UNSW AUSTRALIA | Australian Centre for Cyber Security
UNSW Canberra

AUSTRALIA’S RESPONSE TO ADVANCED TECHNOLOGY THREATS:

AN AGENDA FOR THE NEXT GOVERNMENT

ACCS Discussion Paper No. 3

MEDIA-BRIEFING PRE-PUBLICATION VERSION:
CAN BE CITED

(SUBJECT TO COPY-EDITING
AND REFERENCES BEING EDITED)

Greg Austin and Jill Slay

Australian Centre for Cyber Security
University of New South Wales Canberra
May 2016

ABSTRACT

Australia's take up of advanced technologies has been highest in consumer applications, commerce, science, mining and health. The response has been moderate in most industrial and defence applications. It has been poor in education and a range of social management, policing 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 those advanced technologies, 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. Almost all countries are in the same position of lag facing advanced technology threats but that is small cause for comfort.

As the threats from advanced technologies escalate rapidly at the global level, Australia will need new policies, 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. The main actors are making important new corner-stone contributions in security policy related to advanced technologies. Planned budget growth at the federal level to 2020 is impressive, including for the establishment of thousands of new positions in government agencies and large increases in defence-funded research. But 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 of Australians. There are unrevealed time/policy trade-offs in the federal government's positions. The country's education and training policy needs to make giant steps not currently planned. An enhanced STEM approach will have no strong pay-offs in the next decade for security against advanced technology threats.

This paper lays out a policy agenda for the next government in the country's response to advanced technology threats. It does so largely through the lens of cyber security (or perhaps as aptly, "defence in cyber space"). Since advanced information and communications technologies (ICT) underpin all modern science and most industrial and consumer activities, security of or against those technologies would, one might think, be of the highest priority for the most developed countries.

Looking at current and future threats, Australia's key allies -- the United States and the United Kingdom -- take this view. Australia does not. The paper proposes several recommendations to overcome the country's lagging posture in three areas of policy: countering cyber crime, critical infrastructure protection, and provision of world class policy research and education relevant to Australia's specific needs.

The paper suggests the creation of a Cyber Defence League on the Estonian model, a National Cyber Security College, and a Cyber Scientific Advisory Board. It calls for immediate action to better protect individual Australians from cyber crime. It recommends a new approach to civil defence in cyber space to protect the economy.

AUTHOR NOTES

Professor Greg Austin is a Professor in the Australian Centre for Cyber Security. He also serves as a Professorial Fellow at the EastWest 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 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 has collaborated with the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, including in its recently published book, *International Cyber Norms: Legal, Policy & Industry Perspectives*. Greg's most recent book, *Cyber Policy in China* (Wiley 2014) offers the first comprehensive analysis (military, economic and political) of China's leadership responses to the information society. Greg has a Ph D in International Relations and a Master's degree in international law.

Professor Jill Slay AM is the Director of the Australian Centre for Cyber Security. Professor Slay's research has focused on Forensic Computing for the last ten years although she has a well-established international research reputation in a range of aspects of cyber security including critical infrastructure protection and cyber terrorism. With a variety of collaborators, she has instigated cross-disciplinary research that draws on social science, anthropology, law, drugs and crime, police and justice studies, as well as systems and communications engineering and IT, to achieve its aims. She advises industry and government on strategy and policy in this research domain. Jill has published one book and more than 120 refereed book chapters, journal articles or research papers in forensic computing, information assurance, critical infrastructure protection, complex systems and education. She has been awarded approximately $2 million in grant funding since 2005. Jill is a Fellow of the International Information Systems Security Certification Consortium (ISC^2) and a member of its Board. She was made a member of the Order of Australia (AM) in 2011 for contributions to forensic computer science, security, protection of infrastructure and cyber-terrorism.

ACCS DISCUSSION PAPER SERIES

The ACCS Discussion Paper Series is a vehicle to subject the research of scholars affiliated with the Centre to further review and debate prior to the finalisation of research findings in more formal scholarly outlets, such as journals or books.

ABOUT ACCS

The Australian Centre for Cyber Security (ACCS) at the University of New South Wales Canberra is two things. First, it is 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 that provides both advanced research as well as undergraduate and graduate education on cyber security. ACCS brings together 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/

Introduction

On 27 May 2016, seven world leaders endorsed G7 Principles and Actions on Cyber at their annual summit in Japan.[1] They called on all countries to join the Budapest Convention on Cyber Crime, a Council of Europe Treaty signed in 2001, and to support the G7 High Tech Crime Working Group[2] set up in 1997. Australia joined the Budapest Convention in 2013. There appears to be little sign in public documents in Australia of the country's participation in the work of high tech crime working group, beyond some links with its 24/7 hotline and posting of AFP liaison officers to Interpol headquarters in Lyon. In 2007, Australia joined the Strategic Alliance Cyber Crime Working Group (SACCWG), which brings together national law enforcement of the Five Eyes intelligence alliance.[3] Australia set up a National Cyber Crime Working Group in 2010 which called for national statistics on cyber crime. Six years later, Australia has no official statistics on many forms of cyber crime from its law enforcement agencies,[4] though some jurisdictions have statistics on certain types of cyber crime, usually those on child protection. Authoritative data on convictions for most forms of cyber crime in Australia, as well as for unsolved and uninvestigated cases, is not readily available. It is therefore possible to suggest that Australia has a ten to twenty year time lag in understanding and responding to advanced technology threats from criminals.

These criminals include terrorists. In January 2016, Prime Minister Malcolm Turnbull observed in Washington DC that the coalition against Islamic State was losing the battle in cyber space.[5] He said: "There is one element of our campaign, however, that needs considerable improvement". He added: "The cybersphere demands reactions as rapid as the kinetic battlefield". On another front, in April 2015, an independent evaluation on terrorist financing found a lack of engagement by police forces in most jurisdictions in Australia with using high quality nationally available data.[6] Yet terrorist use of advanced technologies, including in cyber space, has been a preoccupation of law enforcement officials since at least 1997. In the 2016-17 budget paper, the Attorney General's Department reported that the Australian Security Intelligence Organisation (ASIO) saw "growing hostile cyber activity" (from terrorists and states) as an important target of its work. ASIO assessed that "The gap is likely widening between the scale and scope of harm experienced to Australia's sovereignty, government systems, and commercial and intellectual property, and the ability of ASIO and partner agencies to successfully mitigate that harm."[7]

When it comes to addressing threats from advanced technologies, Australia has been behind the pace compared with leading countries. This is the conclusion of two papers released by the Australian Centre for Cyber Security (ACCS) in January 2016 focussing on the defence

[1] See http://www.mofa.go.jp/files/000160279.pdf.
[2] Formally called the Roma-Lyon Group's High-Tech Crime Subgroup.
[3] Australia, Canada, New Zealand, United Kingdom, United States.
[4] ACORN is a public reporting system supported by the many police jurisdictions in Australia and New Zealand. Its website notes: "due to the nature of cybercrime not all reports can be investigated, however reports are taken seriously and will help to contribute to the national intelligence database". See https://www.acorn.gov.au/sites/g/files/net1061/f/acorn-fact-sheet_2.pdf.
[5] Malcolm Turnbull, "Australia and the United States: New Responsibilities for an Enduring Partnership", Speech at CSIS Washington 18 January 2016, https://www.pm.gov.au/media/2016-01-18/australia-and-united-states-new-responsibilities-enduring-partnership.
[6] Financial Action Task Force, "Anti-money laundering and counter-terrorist financing measures: Australia Mutual Evaluation Report", April 2015, http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/Mutual-Evaluation-Report-Australia-2015.pdf.
[7] p. 166.

portfolio.[8] It is also the conclusion of a briefing note about other aspects of cyber security policy released in April 2016 on the eve of the release by the Prime Minister of the most recent "Cyber Security Strategy".[9] As noted in a recent UK study based on a consultation between industry, policy practitioners and scholars, "there is a common perception that the actual cost of cyber attacks is not so high that expensive countermeasures are justified."[10]

That situation of 10-20 years' time lag in Australia is the case now. In order to understand what the future may bring, this paper aims to identify a policy agenda for the next government in the country's response to advanced technology threats. It does so largely through the lens of cyber security (or perhaps as aptly, "defence in cyber space"). As the current government has so correctly observed, our security against or relying on advanced technologies in cyber space is a direct function of the country's overall capacities to deal with those technologies in all walks of life. Since advanced information and communications technologies (ICT) underpin all other advanced technologies, all modern science and most industrial and consumer activities, security of or against those technologies would, one might think, be of the highest priority for the most developed countries.

The paper begins with an overview of future global threats. It then looks at the policy legacy up to September 2016 in very brief terms as a foundation for discussion of the new foundations laid since then by Prime Minister Malcolm Turnbull. The paper then takes three areas of policy both to sketch out in more detail where Australia is at, and also to open up discussion of a policy agenda for the next government. These areas are:

- countering cyber crime
- critical infrastructure protection
- research, education and knowledge transfer.

Australia's Cyber Security Scene

In a Briefing Note released on the eve of the publication of the 2016 Cyber Security Review, we proposed a check list for evaluating the sum of Australian policies in this field. It is reproduced in Box 1. The briefing highlighted:

- the US$19 billion emergency spend in just one year by the United States for additional civil sector cyber security measures announced in February 2016 (400 times Australia's new annualized spend)
- the UK announcement of an additional five-year spend of £1.9 billion (ten times Australia's annualized new spend) for roughly comparable measures
- relative lack of attention by Australia, at least in public, to planning for extreme cyber emergencies

[8] See Greg Austin, "Australia Rearmed: Future Needs for Cyber Enabled Warfare", ACCS Discussion Paper No. 1, UNSW Canberra, January 2016, https://www.unsw.adfa.edu.au/australian-centre-for-cyber-security/sites/accs/files/uploads/DISCUSSION%20PAPER%20AUSTRALIA%20REARMED.pdf and Keith Joiner, "Integrating Cyber Survivability into ADF Platform Development", ACCS Discussion Paper No. 2, January 2016, https://www.unsw.adfa.edu.au/australian-centre-for-cyber-security/sites/accs/files/uploads/DISCUSSION%20PAPER%20CYBER%20SURVIVABILITY.pdf.
[9] Australia. Department of Prime Minister and Cabinet, "Cyber Security Strategy", Canberra, 2016, https://cybersecuritystrategy.dpmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf.
[10] Knowledge Transfer Network, "Innovation Challenges in Cyber Security@, 2016, pre-publication version.

- underdeveloped strategies and structures for resilience of critical cyber-dependent infrastructure
- some institutional gaps in the "whole of nation" approach.

Box 1: The Checklist

Setting

1. Consistent articulation of the different domains of cyber security (crime, harassment and bullying, espionage, warfare); of the many dimensions of cyber security (technical, human, social and legal); and how different sections of the society must bear differentiated responsibilities.

2. Consistent and comprehensive articulation of the threat environment and variegated response options.

3. A comprehensive suite of governmental, cross-sector, private-public, professional and civic organisations active in cyber security.

4. National consensus on where to draw the line between sovereign capabilities and the global communities of practice (including R&D)

Response

5. Effective monitoring of business and economic threats and rapid response capabilities at the enterprise level, including large corporations and SMEs.

6. Nation-wide preparedness for the unlikely but credible threat of an extreme cyber emergency affecting the civil economy or national security interests (including international aspects).

7. Effective response capabilities for social threats (crimes) against individuals, including children and other vulnerable groups.

A national cyber security strategy in a liberal democracy and free market economy is not exclusively or even primarily a government-led effort. In many respects, the government can only facilitate and inspire within the constraints of tight budgets. Moreover, Australia sits in a global community of cyber security practice, technologies, policies, public education and research on which it can draw (we do not need to do everything ourselves from scratch). One example of this is the country’s “five eyes” intelligence relationship and the larger set of our strategic relationships with the “five eyes” partners. Another example of this is our openness to enabling factors for cyber security, such as foreign investment, trade and movement of specialists. The Australian government has a good news story to tell on some of the enabling factors for cyber security that has not been as well articulated as it might be. But Australia also faces a rapidly evolving and more serious constellation of threats, most of which originate outside the country though some are home-grown and often very localized, often where police have zero capacity in investigating cyber crime.

The tone and sense of urgency of the national debate in Australia does not rise to the level of intensity as it does in the United States, the United Kingdom, France, China and several other countries.

Table 1 sets out an overview of the many places where one must look to find Australia's cyber security policies and the myriad of actors involved.

TABE 1: PUTATIVE AUSTRALIAN POLICY SOURCES AND ACTORS

Security Need	Putative Policy Sources	Primary sub-Cabinet Actors
Warfare	Defence White Paper 2016 Information Operations 2013 (ADF)	Defence, ADF, ASD,[11] ASIS,[12] DFAT, ONA, DIO, private contractors
Espionage/ Counter-espionage	Defence White Paper 2016 ASIO Strategic Plan 2013-16[13] ASIO Counter-Espionage Strategy[14]	Defence, ASD, ASIO, ASIS, AFP, Courts, DPP, private contractors
Counter-Terrorism	Australia's Counter-Terrorism Strategy 2015[15] Review of Australia's Counter-Terrorism Machinery 2015[16] ASIO Strategic Plan 2013-16	ASIO, Attorney General's Dept, ASD, AFP, State Attorneys General, Police, Courts, DPP Defence, ASIS, private contractors
Combating cyber theft	National Plan to Combat Cyber Crime 2013	Attorney General's Department, ACSC, AFP, State Police, Courts, DPP, Defence, ASIS, private contractors
Combating Cyber Harassment, Bullying, Stalking, Grooming (crimes)	National Plan to Combat Cyber Crime 2013	Attorney General, ACSC, AFP, State Attorneys General, Police, Courts, DPP, Defence, ASIS, private contractors
Combating Reputation Damage (criminal defamation)	National Plan to Combat Cyber Crime 2013	Attorney General, ACSC, AFP, State Attorneys General, Police, Courts, DPP, Defence, ASIS, private contractors
Combating Data Corruption (crime)	National Plan to Combat Cyber Crime 2013	Attorney General, ACSC, AFP, State Attorneys General, Police, Courts, DPP, Defence, ASIS, private contractors
Protecting Critical National Systems	Critical Infrastructure Resilience Strategy: Policy Statement 2015 Critical Infrastructure Resilience Strategy: Plan 2015 Defence White Paper 2016	Attorney General, ASD, AFP, State Attorneys General, Police, Courts, DPP Defence, ASIO, ASIS, private contractors
Privacy	Australian Law Reform Commission Inquiry #123[17]	Australian Information Commissioner, Human Rights Commission, Attorneys General
Combating Data Manipulation and Corruption	National Plan to Combat Cyber Crime 2013	

[11] ASD is called out as a separate actor though it is institutionally part of Defence.
[12] ASIS is called out as a separate actor though it is administered by the Minister of Foreign Affairs and Trade.
[13] http://www.asio.gov.au/img/files/ASIO-Strategic-Plan_2013-16_A4_web.pdf.
[14] Presumed to exist and to be classified.
[15] https://www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/Australias-Counter-Terrorism-Strategy-2015.pdf.
[16] https://www.dpmc.gov.au/sites/default/files/publications/190215_CT_Review_0.pdf.
[17] http://www.alrc.gov.au/publications/serious-invasions-privacy-digital-era-alrc-report-123/recommendations.

Policy Research	No national research strategy for cyber security policy	Universities, thinks tanks, governments, police, security forces, private sector
Technical research	DSTG (Defence) Research Plan for military aspects	DSTG, Data61, ARC
Education	No national curriculum standards for cyber security education (tertiary, secondary or primary)	

Future Threats

Each year, leading figures in the United States intelligence, security and justice community report to Congress in public on cyber threats in a consistent, comprehensive and detailed fashion. In 2015, the Director of National Intelligence reported: "we must be prepared for a catastrophic large scale strike – a so-called cyber Armageddon", even though he said that was considered a low likelihood.[18] In 2016, the mood was as grim. Clapper reported that "The increased reliance on AI [artificial intelligence] for autonomous decisionmaking is creating new vulnerabilities to cyberattacks and influence operations. As we have already seen, false data and unanticipated algorithm behaviors have caused significant fluctuations in the stock market because of the reliance on automated trading of financial instruments".[19] Clapper also reported: "2014 saw, for the first time, destructive cyber attacks carried out on US soil by nation state entities" … "unpredictable instability is the new normal".[20] This last assessment was shared in large part by Georgia Tech in 2014: "Low-intensity online nation-state conflicts become the rule, not the exception".[21]

One sentence in Clapper's 2016 statement has enormous implications for defenders in cyber space in terms of training, priorities and costs. He warned of an "an increased emphasis on changing or manipulating data to compromise its integrity (i.e., accuracy and reliability) to affect decisionmaking, reduce trust in systems, or cause adverse physical effects". This will shift the defense requirements from securing a system to having advanced techniques for information assurance across a massive trove of data.

But the scale of threat as perceived in the United States is equally demonstrated by the declaration of a national emergency in cyber space two years running in April 2015 and 2016. The language of President Obama in March this year captures the reasoning and the threat assessment behind it: "Significant malicious cyber-enabled activities" from outside the country "continue to pose an unusual and extraordinary threat to the national security, foreign

[18] Director of National Intelligence, "Worldwide Threat Assessment", 2015, http://www.dni.gov/index.php/newsroom/testimonies/209-congressional-testimonies-2015/1175-dni-clapper-opening-statement-on-the-worldwide-threat-assessment-before-the-senate-armed-services-committee.

[19] P. 1, https://www.dni.gov/files/documents/SSCI_Unclassified_2016_ATA_SFR%20_FINAL.pdf.

[20] Director of National Intelligence**,** Remarks as delivered by The Honorable James R. Clapper, Director of National Intelligence, Opening Statement to the Worldwide Threat Assessment Hearing, Senate Armed Services Committee, Thursday, Feb. 26, 2015, http://www.dni.gov/index.php/newsroom/testimonies/209-congressional-testimonies-2015/1175-dni-clapper-opening-statement-on-the-worldwide-threat-assessment-before-the-senate-armed-services-committee**.**

[21] Georgia Tech information Security Centre and the Georgia Tech Research Institute, "Emerging Cyber Threats Report 2015", 2014, p. 13, https://www.gtisc.gatech.edu/pdf/Threats_Report_2015.pdf.

policy, and economy of the United States".[22] He made this statement in formally declaring the continuance of a national security emergency in cyber space that he had declared for the first time one year earlier. This is his admission that the most powerful country on the planet has consistently failed to secure its main cyber space assets in the face of specific rampaging and escalating threats.

Trends in technologies for cyber attack and defence have been described in many places: from government agencies, scholars, vendors, netizens and hackers. Those of special significance for benchmarking national cyber security needs are those that cut across and combine different vectors of attack. These might be called "systems of systems" technologies. The first thing that strikes a policy analyst coming to the question from a neutral position is the immense diversity of estimations about future technologies of attack and defence systems. There is also the consideration that novel (disruptive) cyber technologies will emerge and be deployable at short notice, in time periods as short as a matter of days.

Complex Cyber Attacks

If one takes a selection of the more authoritative assessments from security specialists, the characterization of threat development around complex cyber attacks is a useful place to start. In 2015, a U.S. based analyst, Carl Herberger, the Vice President of Security Solutions at Radware, reported that in 2013 the average cyber attack he had observed involved seven attack vectors (though some had reached over 25 attack vectors), different phases (each with several waves), with successive phases relying on methods that worked in the previous phase but adding new attack vectors.[23] This was rather well captured in a FireEye presentation in 2013 which listed four characteristics of the emerging threat landscape: coordinated persistent threat actors, dynamic polymorphic malware, multi-vector attacks and multi-phase attacks.[24]

These characterisations are very important benchmarks. But even they don't take us as far as we need to look. They address only a narrow slice of the threat picture.

As one leading guidepoint for understanding emerging threats, we might look at the topic of critical infrastructure protection and the acknowledged world leader in cyberspace defence of it, the Idaho National Laboratory (INL). The case of electric power supply, which is controlled by digital assets, is was the subject of testimony of an Associate Director of INL, M Brent Stacey, on 21 October 2015, which is extracted verbatim below:

> - The presumption that a control system is "air-gapped" is not an effective cyber security strategy. This has been demonstrated by over 600 assessments.
> - Intrusion detection technology is not well developed for control system networks; the average length of time for detection of a malware intrusion is four months and typically identified by a third party.

[22] Barack Obama, "Letter -- Cyber-Enabled Activities Emergency Continuation", White House, Washington DC, 29 March 2016, https://www.whitehouse.gov/the-press-office/2016/03/29/letter-cyber-enabled-activities-emergency-continuation.

[23] See more at: http://inspiratron.org/blog/2015/05/29/the-art-of-cyber-war/#sthash.LxJiSSIc.dpuf.

[24] See http://www.exclusive-networks.be/wp-content/uploads/2013/11/FireEye-breakout-session.pdf.

- As the complexity and “interconnectedness ” of control systems increase, the probability increases for unintended system failures of high consequence - independent of malicious intent.
- The dynamic threat is evolving faster than the cycle of measure and countermeasure, and far faster than the evolution of policy.
- The demand for trained cyber defenders with control systems knowledge vastly exceeds the supply.[25]

As far as Australia’ public threat assessments are concerned, one key reference point is the 2015 “Threat Report” of the Australian Cyber Security Centre (ACSC). It says: “Australia has not yet been subjected to any activities that could be considered a cyber attack”, one “seriously compromising national security, stability or prosperity”.[26] It says that “Robust cyber defences will continue to allow a high degree of confidence in network and information security.” The ACSC seems to be saying that since Australia has not been attacked, the country can be confident that it is secure in cyber space. The other two assessments from U.S. sources paint a very different picture: Australia has probably been attacked and does not know it and it is no more secure, probably less so, than the United States from imminent and longer term future threats. The document does not describe the menace with the same sense of urgency as the allies do.

In Mr Turnbull’s preface to the 2016 Cyber Security Strategy, he observed: “The scale and reach of malicious cyber activity … is unprecedented. The rate of compromise is increasing and the methods used by malicious actors are rapidly evolving”.[27] It said Australia needed to prepare for a “significant cyber event”, with scale of effect unspecified. The problem with such a statement, and several like it in the body of the Strategy, is that it lacks contours and baselines. This assessment gap is demonstrated vividly in the report when it says that the costs to Australia of cyber attack could be between $1 billion per year and $17 billion per year.[28] The Strategy’s commitment, one of five major undertakings, to ensure “Australia’s networks and systems are hard to compromise and resilient to cyber attacks” is one that will not be achievable for a decade at least because of the threat trends and the low level of global preparedness attested by leading international authorities and Australia’s own ASIO, various Defence Department reports and independent assessments of them.

[25] United States. House of Representatives. Science Subcommittee on Energy And Science Subcommittee On Research And Technology, Written Testimony of Mr. Brent Stacey, Associate Laboratory Director for National & Homeland Security, Idaho National Laboratory, 21 October 2015, p.3, http://docs.house.gov/meetings/SY/SY20/20151021/104072/HHRG-114-SY20-Wstate-StaceyB-20151021.pdf.

[26] Australian Cyber Security Centre (ACSC), “Threat Assessment 2015”, pp.8, 24. Cyber attack is defined by ACSC as follows: “Includes deliberate acts through cyber space to manipulate, destruct, deny, degrade or destroy computers or networks, or the information resident in them, with the effect, in cyber space or the physical world, of seriously compromising national security, stability or prosperity”. See https://www.acsc.gov.au/publications/ACSC_Threat_Report_2015.pdf.

[27] Australia. Department of Prime Minister and Cabinet, “Cyber Security Strategy”, Canberra, 2016, https://cybersecuritystrategy.dpmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf.

[28] “Cyber Security Strategy”, p. 5.]

From a Modest Legacy to a Richer Bequest

When looking for the antecedents to current policy and practice which can today be aggregated as ‘cybersecurity’, the 44th Parliament Briefing (Parliament 2013) reports that cyber threats were first identified as a national security concern 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 resulted in a new mechanism for information exchange but did not meet all its implementation goals. 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 notes its cyber focus as (p18)

> ‘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 laid out five priorities:

- **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.'

Through the 2016 Cyber Security Strategy, the current government has delivered a mature and nuanced cyber security strategy that promises to redress important deficiencies in the country's posture. The plan is an historic achievement, but apart from mentions of terrorism, it does not openly discuss key sources of malicious activity, such as China and Russia. The strategy does not have a spending plan adequate to address the pace and scale of emerging threats to the digital economy or national security.

On the credit side, the strategy's 8-page action plan, along with its indicators of success, is ambitious in its scope. Novel measures include joint public-private threat assessment centres in the states and a series of new appointments, including an Assistant Minister, a Special Adviser (both reporting to the PM) and an ambassador for cyber affairs. There are radical commitments to widen the services of the Australian Signals Directorate in the Department of Defence to meet private sector customer needs.

The inclusion of so many concrete "announceables" in the strategy was a pleasant surprise. On the other hand, many of the new commitments are fairly generalized and lack granularity, such as the intent to increase numbers for cyber security graduates, women in the profession, and school kids "in the know".

In the absence of quantification of such commitments, the strategy is to be applauded for its additional undertaking that the government will report annually on its success, including presumably the numerical expansion of these and other cohorts. In one year's time, we will want to know from the government how many more cyber graduates we have compared with this year. In the medium term, we will need the government to provide some metric on how many graduates in the field we actually need. We also need to see the baseline statistics for this year.

We might ask the government fairly promptly for some elaboration on just what levers it intends to use, in partnership with universities and the corporate sector, to pursue the cohort goals in cyber security and what sort of money it is prepared to put into it.

Most importantly, there are unrevealed time/policy trade-offs in the federal government's positions. The country's education and training policy needs to make giant steps. An enhanced STEM approach is only one and it will have no strong pay-offs in the next decade at least for security against advanced technology threats. The Strategy gives no strong sense of when we might expect to see impacts from the measures announced on the security in cyber space of Australian citizens and enterprises.

Countering Cyber Crime

Criminals in cyber space have very little chance of being brought to justice, unless their victim is the United States government. For almost all other cases and countries, convictions seem to be very small in number. This situation bears out an Italian assessment that "the vast majority of governments addressed cyber security more within the framework of national defense rather than from the point of view of the protection of individual, social, and economic assets."[29] The Australian government did not see cyber crime as an important focus of the recent Cyber Security Strategy, and suggested that it was, in this area of policy, complemented by the National Plan to Combat Cyber Crime released in 2013 by the previous government.

The 2016 Strategy does make a commitment to develop and implement a specialists training plan in the field of countering cyber crime, with no further detail (p. 60). It also commits in the broadest of terms of increasing the capacity of the AFP and the Australian Crime Commission to counter cyber crime (p.59).

The Cyber Security Strategy notes that the cost of cyber crime to Australia is between A$1 billion and A$17 billion. The wide range for this "estimate" is strong evidence of how low a priority this area of policy has been.

The Cyber Crime plan committed states and the Commonwealth to ensuring that responsible agencies "have the capabilities and capacity they need to detect, disrupt, investigate and prosecute cybercrime and manage digital evidence".[30] It said that the National Cyber Crime Working Group would:

- "encourage basic training on cybercrime and digital evidence becoming a mainstream component of police training, including by continuing to support the development of nationally consistent training and education resources
- consider options to increase the pool of knowledge at law enforcement agencies' disposal, including options for accessing expertise from the private and tertiary sectors, such as through secondments
- consider options to coordinate access to specialist expertise across our police forces, including through options for a national centre of excellence or an agreement about the sharing of specialist resources across Australian police agencies
- continue to monitor capability gaps across our police forces to guide capability improvement
- monitor law enforcement powers which relate to the investigation of cybercrime and collection of digital evidence to ensure they remain effective.

[29] P. 708, https://pralab.diee.unica.it/sites/default/files/armin15-fcct.pdf.
[30] P. 30.

It is important for the Working Group and the Commonwealth government to report in outcomes of this work. In the 2016-17 budget and forward estimates, the government has provided almost $15 million over four years to the Australian Crime Commission to improve its capability to combat cyber crime. But beyond that we do not have a clear picture.

As noted in the Introduction, Australia has no official statistics on many forms of cyber crime from its law enforcement agencies,[31] though some jurisdictions have statistics on certain types of cyber crime, usually those on child protection. Authoritative data on convictions for most forms of cyber crime in Australia, as well as for unsolved and uninvestigated cases, is not readily available. Australia has a ten to twenty year time lag in understanding and responding to advanced technology threats from criminals.

To begin to redress this, as the 2013 National Cybercrime Plan suggested, it would definitely be worthwhile to set up a Centre of Excellence in High Tech Crime in Australia. It could leverage off the Interpol centre in Singapore, but we need one in Australia if we are to begin to manage the impacts here. But a more effective pathway may be to move immediately to set up a national cyber crime fighting unit, including research staff, funded to at least $20 million per year for ten years, that is resourced to begin to bring Australia into a starting position to capture and convict cyber criminals.

Critical Infrastructure Protection

Specialists and governments around the world are almost unanimous that a catastrophic cyber emergency is highly unlikely in peacetime but they cannot agree on what priority to accord planning for one in national cyber security strategies. A number of governments, especially the United States and Estonia, view the threat as credible and have accorded such a possibility a high priority in their planning. This approach conforms to the traditional approach that while outright war with major powers, like China and Russia, is highly unlikely, it is still essential to have defence capabilities in place, as well as mobilisation plans, for the eventuality. However, the need to plan for extreme cyber emergencies is not only driven by the common dictates of national defence policy, but the unique characteristics of cyber space and vectors of attack or system failure within advanced systems. The NATO Framework Manual observes that governments "recognise that a disruption in one infrastructure can easily propagate into other infrastructures" with catastrophic consequences.[32] It also observes that highly developed resilience strategies for extreme cyber emergencies are an essential part of military deterrence in the cyber age (p.82). Some leading private sector organisations also accord a high priority to planning for extreme cyber emergencies. In 2013, a global survey by the World Federation of Exchanges (WFE) and the International Organization of Securities Commissions (IOSCO) found that 89 percent of respondent exchanges considered that cyber crime in securities markets can be considered a systemic risk. It continued to develop policy responses and in November 2015 advised its members to plan for "extreme but plausible scenarios" (p. 2).[33]

[31] ACORN is a public reporting system supported by the many police jurisdictions in Australia and New Zealand. Its website notes: "due to the nature of cybercrime not all reports can be investigated, however reports are taken seriously and will help to contribute to the national intelligence database". See https://www.acorn.gov.au/sites/g/files/net1061/f/acorn-fact-sheet_2.pdf.

[32] https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf.

[33] https://www.iosco.org/library/pubdocs/pdf/IOSCOPD513.pdf.

In the United States, since 2006, the USA has conducted biennial exercises in the Cyber Storm series to test responses in national cyber emergency situations.[34] Idaho National Laboratory conducts research on nation resilience in the face of "catastrophic and potentially cascading events that will likely require substantial time to assess, respond to, and recover from."[35] In 2010, Sandia National Laboratory warned of seven structural defects in U.S. decision-making that would undermine its resilience in an extreme cyber emergency.[36] In 2011, President signed PPD 8 on national emergency preparedness, including for nationally significant cyber attack.[37]

The UK sees responsibility for defending critical national infrastructure as sitting "firmly with industry", while the "government works closely with them to provide advice, assurance and expertise", including through "joint exercises to improve preparedness".[38] "On average, CERT-UK supports three exercises per month to test cyber resilience and response" (p.23). The Bank of England lead two Waking Shark table top exercises in 2011 and 2013, to test the financial sector against an extreme and concerted cyber attack by a hostile country.[39] In 2016, the UK and USA will partner in an exercise to test a terrorist cyber-enabled attack on a nuclear power station.[40]

In Australia, the ACSC's 2015 Threat Report says extreme cyber attack is unlikely "outside a period of significant heightened tension or escalation to conflict with another country". In 2011, ANZUS partners agreed that the treaty could be invoked in the event of a serious cyber attack.[41] The government's 2015 resilience strategy for critical infrastructure mentions cyber threats only in general terms.[42] The government runs a program for critical infrastructure modelling and analysis (CIPMA) which in principle connects the government with the best available academic research in the field. It also has a Trusted Information Sharing Network (TISN) which was set up in the 2015 plan made three main commitments in respect of cyber space:

- Increase the exploration of cyber cross-sectoral dependencies through more cyber-focused TISN activities, including in conjunction with CERT Australia and CIPMA.
- Explore opportunities for greater international collaboration on cyber security issues as they relate to critical infrastructure.
- Implement the outcomes of the Australian Government's cyber security review as they relate to critical infrastructure.

[34] https://www.dhs.gov/cyber-storm.

[35] http://docs.house.gov/meetings/SY/SY20/20151021/104072/HHRG-114-SY20-Wstate-StaceyB-20151021.pdf.

[36] http://prod.sandia.gov/techlib/access-control.cgi/2010/104766.pdf http://prod.sandia.gov/techlib/access-control.cgi/2010/104766.pdf.

[37] https://www.dhs.gov/presidential-policy-directive-8-national-preparedness.

[38] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf.

[39] http://www.bankofengland.co.uk/financialstability/fsc/Documents/wakingshark2report.pdf.

[40] http://www.theguardian.com/uk-news/2016/mar/31/uk-us-simulate-cyber-attack-nuclear-plants-test-resilience.

[41] http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22media%2Fpressrel%2F1416907%22.

[42] See "Critical Infrastructure Resilience Strategy: Policy Statement" (2015) and the "Critical Infrastructure Resilience Strategy: Plan" (2015), both available at http://www.tisn.gov.au/Pages/default.aspx.

Unfortunately, the public results of the review, the Cyber Security Strategy, included scant attention to critical infrastructure. In 2013, ASPI assessed that "Australia's cyber policy looks disjointed and lacking in detail".[43] That remains the situation today. Australia has participated in an Asia Pacific cyber exercise and the U.S. Cyber Storm series.[44] In 2013, an officer of the Commonwealth Bank identified 7 extreme cyber scenarios to focus attention on this problem set.[45]

INL has identified a three tier defensive approach, rendered verbatim below:

1. Hygiene: "the foundation of our nation's efforts , composed of the day - to-day measure and countermeasure battle"; "important routine tasks such as standards compliance, patching, and password management"; "primarily the role of industry, with both vendors and asset owners participating".
2. Advanced persistent threat: "the more sophisticated criminal and nation state persistent campaigns"; requiring "a strategic partnership with industry and government"; "these roles are still evolving"; "ICS-CERT provides critical surge response capacity and issues alerts of current vulnerabilities to the government and asset owners"
3. High impact low frequency events: "catastrophic and potentially cascading events that will likely require substantial time to assess, respond to, and recover from. This level is primarily the responsibility of the government."

Research at INL focuses on the two highest priority tiers (#2 and #3 in the list above), aiming for a "two- to four-year research-to-deployment cycle" and to "achieve transformational innovations that improve the security of our power infrastructure by reducing complexity, implementing cyber-informed design, and integrating selected digital enhancements". The laboratory "is pursuing a grand challenge to develop novel and deployable solutions to take a set of high value infrastructure assets off the table as targets". This program assumes pervasive insecurity: It promotes "a paradigm shift in the methods used to historically develop control systems. This paradigm is predicated on the fact the traditional trust relationships in peer communications are no longer a satisfactory assumption. Instead, a resilient control system design expects a malicious actor or actions to be part of normal operation and is designed to mitigate such actions".[46]

Australia has no comprehensive effort that matches the approach adopted by INL, and in fact much of the government's effort is spent on the lowest priority tier (#1 in the list above) identified by INL: the cyber security hygiene of operators and enterprises.

A 2012 UK analysis provides some additional insight into the processes threatening cyber resilience of another aspect of critical infrastructure, the financial services sector.[47] The study was based on consultation with industry. Interviewees identified as one of the top 3

[43] https://www.aspi.org.au/publications/special-report-the-emerging-agenda-for-cybersecurity/SR51_agenda_cybersecurity.pdf.

[44] http://www.smh.com.au/it-pro/security-it/australias-cyber-protection-put-to-the-test-20120215-1t5nl.html.

[45] http://www.rsaconference.com/writable/presentations/file_upload/stu-w21b.pdf.

[46] See website of Idaho National laboratory, https://inlportal.inl.gov/portal/server.pt/community/distinctive_signature__icis/315/grand_challenge.

[47] United Kingdom. Financial Conduct Authority, HM Treasury and the Bank of England, "Technology and Cyber Resilience Benchmarking Report 2012", London 2013, http://www.bankofengland.co.uk/financialstability/fsc/Documents/technologyandcyberresiliencebenchmarkingreport2012.pdf'

technology risks the “development or emergence of new technology and poor change management in relation to new technologies”.[48] A 2013 academic study on a similar subject warned against the danger of estimating risks in isolation from each other: “Estimation of CPS[49] risks by naively aggregating risks due to reliability and security failures does not capture the externalities”. [50] It called out “biased security choices” that “reduce the effectiveness of security defenses”. Looking to future threats, it warned that CPS “are subjected to complex risks, of which very little is known despite the realization of their significance”.

Research, Education and Knowledge: The Missing Link

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.

Table 2: Policy impact on education, training research and workforce needs

Security Need	Putative Policy/ Advice Sources	Education, Research and Training implications
Cybersecurity	ASD Top 4	Cohort of government and industry Staff who are educated or trained in: • Network Security • Information Security • Incident response • Digital Forensics • Software development • Criminology
Warfare	Defence White Paper 2016, 2009	Cohort of government and industry Staff who are educated or trained in: • Network Security • Information Security • Incident response • Digital Forensics • Software development • Reverse engineering • Cyber effects • OS Intelligence

[48] The other two were network and critical system outages, and access management and control of administration privileges.

[49] Cloud Platform Services.

[50] Saurabh Amin, Galina A. Schwartz, Alefiya Hussain, “In Quest of Benchmarking Security Risks to Cyber-Physical Systems”, *IEEE Network*, January/February 2013, 19-24, 24, http://www.eecs.berkeley.edu/~schwartz/IEEEMag2013.pdf.

		• Law • Policy
Espionage/ Counter-espionage	Defence White Paper 2016, 2009 ASIO Report to Parliament 2011/2 ASIO Strategic Plan 2013-16	Cohort of government and industry Staff who are educated or trained in: • Network Security • Information Security • Incident response • Digital Forensics • Software development • Reverse engineering • Cyber effects • OS Intelligence • Law • Policy
Combating theft	National Cyber Crime Strategy 2013	Cohort of government and industry Staff who are educated or trained in: • Network Security • Web Security • Information Security • Incident response • Digital Forensics • Law • Criminology
Combating Harassment, Bullying, Stalking, Grooming (crimes)	National Cyber Crime Strategy 2013	Cohort of government and industry Staff who are trained in: • Network Security • Information Security • Web Security • Incident response • Digital Forensics • Human Factors • Psychology • Law • Criminology
Reputation Damage		• Information Security • Web Security • Psychology • Management • Criminology
Data Corruption (crime)		• Information Security • Web Security • Incident response • Digital Forensics • Criminology
Critical National Systems	Critical Infrastructure Resilience: Policy Statement 2015 Critical Infrastructure Resilience Strategy: Plan 2015 Defence White Paper 2016	• Dependency Analysis • Information Assurance • Web Security • Incident response
Combating Data Manipulation and Corruption	National Cyber Crime Strategy 201	Cohort of government and industry Staff who are educated or trained in: • Network Security • Information Security • Incident response • Digital Forensics • Software development • Reverse engineering

		• Cyber effects • OS Intelligence • Law • Policy • Criminology

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 VCs, 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 (May 2016), there was some small impact in universities in Australia, some of which responded by starting small research groups (usually based in IT) or teaching themes in cybersecurity, digital forensics or critical infrastructure disciplines. These were 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 five attempts to get a CRC 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.

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 3:

Table3: Some Suggested Australian Curriculum Elements

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 ▪ 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	▪ 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 ▪ Advanced Security Risk Management ▪ Advances in Security Technology	• 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 • 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

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.

Conclusion

The Australian government has committed itself to a worthy national development agenda around innovation, but the country as whole appears so far to have been unmoved by the rhetoric. Creativity and innovation continue to bubble away, but there is no sign of a quantum leap. Australia looks like a country-in-waiting for its next innovation revolution.

The phenomenon of quantum leap implies a rapid shift to a different state – the "excited atom". It also implies the application of energy (the introduction of light). The particular atom that experiences the electron transition under the application of the light does so on a random or irregular basis and will return to the ground state near instantaneously. So the metaphor is quite useful as we ponder the political fortunes of "innovation agendas" of this or that government.

The metaphor may most useful simply in that it alerts us to a state of nature. Apply light and energy, produce some excitement and see new sub-atomic particles called photons. No-one owns the state of nature. It happens. But the quantum leap will not happen without the energy stimulus. And if we want to know it is happening, we need science to help us. If we want to see a quantum leap, we need science (a body of knowledge about atomic physics) to tell us what is happening, when and why.

For a quantum leap in innovation, Australia needs a body of knowledge that can help us recognize the excited state of creativity and new production. We also need a social and economic structure that can be geared toward creating the excited state. The country appears to lack a widely-shared body of knowledge about innovation processes and the social and economic structures we need. We also need a body of people who care and who want to see innovation badly enough that will accept structural political and economic change to promote it.

The Australian Council of Learned Academies (ACOLA) has made a massive contribution in the recent past but to benefit from these studies we need to popularize the "knowledge" represented by these studies. We need some champions. But we also need some underlying shifts in the background knowledge, the public narrative, about Australia's "knowledge economy" -- its generals, its foot-soldiers and the history of its victories and defeats. In fact, we need to see history of the country's knowledge economy and knowledge society on a scale with even greater clarity than we see our military history. Australia has an official historian for its wars but not for its knowledge economy.

In 1998, Tim Sherratt observed that the "history of science in Australia is a field intimidated by its subject" He suggested that we "have been too slow to examine the local context of knowledge production and use". In my view, notwithstanding clear advances, historical analysis of Australia's knowledge society is still trapped by what Sherratt called the "antiquarian plod or the celebratory frolic". We do have the journal *Historical Records of Australian Science*, but science is not the same as the "knowledge economy". This term was coined as far back as 1962 by American economist Fritz Machlup. In the intervening 54 years, we have had no shortage of studies on Australia's knowledge economy. The tragedy is that we have moved too slowly to popularize not just the research but the very idea of a knowledge economy.

We cannot regard Australia's cyber policy as mature until the government:

- has had an open and candid conversation in public with key stakeholders about the sort of threat scenarios we face, from military operations to privacy, from cyber crime to extreme cyber emergencies
- has developed policies and agencies, supported by the civil sector, that could perform credibly in all of those scenarios
- has articulated strategies to reduce the risks of future threats
- has articulated a civil defence strategy for the inevitable high impact disruption of our civil economy and communities of an extreme cyber emergency
- has set in place policies for development of our industry base and work force that can support all of the above to the extent that our national economy permits and limitations of alliance support dictate.

Recommendations

Recommendation # 1*:* The Federal Government should consider the establishment of a Cyber Defence League (on the Estonian model), or similar, to stimulate the necessary step changes in awareness and capability for the country that it so badly needs.

Recommendation # 2: Australia should become a member of the NATO Cooperative Cyber Defence Centre of Excellence or build a similar centre here for the Asia Pacific, with the aim of establishing a flourishing epistemic community in cyber policy that Australia and its Southeast Asian neighbours lack.

The current plans for capacity building in the region do not equate to this proposal.

Countering Cyber Crime

Recommendation #3: The States and Commonwealth should honour their commitment made in 2010 to develop reliable and comprehensive statistics on cyber crime, especially of the cases they have investigated and where prosecutions have been brought.

This is not addressed by current proposals for voluntary information sharing or the ACORN database.

Recommendation #4: The States and Commonwealth should commit to a fast track process to set up a national cyber crime fighting unit, including research staff, funded to at least $20 million per year for ten years, that is resourced to begin to bring Australia into a starting position to capture and convict more cyber criminals.

Critical Cyber Infrastructure Protection

Recommendation #5*:* To meet the unique demands of protection of critical cyber space infrastructure, the Government should set up a Working Group with the states and private sector organizations to develop a unique national strategy.

Research, Education and Knowledge Transfer

Recommendation #6: In line with a similar recommendation devised in the UK, Australia should establish a Cyber Scientific Advisory Board, with responsibility for communicating future threats and advising on responses.

Such a Board must be premised on the proposition that "the problem of cybersecurity is essentially a fusion of technology, policy and behaviour, and crosses many disciplines".[51] The Board must be chaired by an academic specialist in cyber public policy or the economics of cyber policy who can work across these disciplines not by a scholar with a narrow technical discipline. The Board should be funded to disburse grants up to $30 million per year for research and university education initiatives. The Board should be funded to disburse grants up to $30 million per year for research and university education initiatives. The Defence Department can easily fund this from its projected budget growth but the Board should not be "captured" by Defence. (This is a very different proposal from the Government's commendable plan to set up an industry-led Cyber Security Growth Centre, which is funded at only $30 million over four years.)

Recommendation #7: Australia needs to consider creation of a National Cyber Security College to get focus and concentrate expertise.

Such a body could help generate the following necessary actions:

- Establish nationally approved 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 upskilled and converted into Cyber Security professionals
- Develop a mechanism whereby the industries which 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
- Devise a dedicated, well-funded plan to 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 developing a private system and sector specific initiatives for hybrid education initiatives around the country.

[51] Knowledge Transfer Network, "Innovation Challenges in Cyber security", 2016 (pre-publication version).