INSTITUTE
FOR
REGIONAL SECURITY

KOKODA PAPER NO. 21

BUILDING A RESILIENT CYBER ECO-SYSTEM: NATIONAL AND REGIONAL CONSIDERATIONS

Gary Waters, Brett Biddington and Craig Valli

November 2016

GOLD
SPONSOR

nuix

SILVER
SPONSOR

AUSTRALIA
ECU
EDITH COWAN
UNIVERSITY

BRONZE
SPONSORS

BAE SYSTEMS
INSPIRED WORK

accenture
High performance. Delivered.

About the Institute For Regional Security

The Institute for Regional Security is a registered charity and not-for-profit organisation. Its research is independent and non-partisan. The Institute For Regional Security does not take institutional positions on policy issues nor do sponsors have editorial influence. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the authors.

Published in Australia by the Institute for Regional Security, November 2016

Publication Management: QOTE Canberra (02) 6162 1258

Published and distributed by:
The Institute For Regional Security
2/10 Kennedy Street
(PO Box 4060), Kingston ACT 2604
T: +61 2 6295 1555
F: +61 2 6169 3019
Email: info@ifrs.org.au
Web: www.regionalsecurity.org.au

INSTITUTE FOR REGIONAL SECURITY

KOKODA PAPER NO. 21

BUILDING A RESILIENT CYBER ECO-SYSTEM: NATIONAL AND REGIONAL CONSIDERATIONS

Gary Waters, Brett Biddington and Craig Valli

November 2016

INSIGHTS
IDEAS
IMPACT

Institute for Regional Security
www.regionalsecurity.org.au

Sponsor Acknowledgment

GOLD SPONSOR	SILVER SPONSOR	BRONZE SPONSORS
nuix	ECU EDITH COWAN UNIVERSITY AUSTRALIA	BAE SYSTEMS INSPIRED WORK accenture High performance. Delivered.

The Institute For Regional Security thanks our Gold Sponsor NUIX, our silver sponsor, Edith Cowan University, and our Bronze sponsors Accenture and BAE Systems for supporting this study and for their commitment to fostering research and thinking about the challenges that will need to be met if a more secure, resilient and trustworthy internet is to be delivered to Australia and to the region.

National Library of Australia Cataloguing-in-Publication entry

Creator:	Waters, Gary, 1951- author.
Title:	Building a resilient cyber eco-system: : national and regional considerations / Gary Waters, Brett Biddington, Craig Valli.
ISBN:	9780992571245 (paperback)
Series:	Kokoda papers ; no. 21.
Notes:	Includes bibliographical references.
Subjects:	Internet--Security measures. Cyberinfrastructure--Australia. Computer security--Australia.
Other Creators/ Contributors:	Biddington, Brett, author. Valli, Craig, author. Institute For Regional Security, issuing body.

ABOUT THE AUTHORS

Gary Waters

Dr Gary Waters served in the Royal Australian Air Force (leaving as an Air Commodore); served as a senior public servant in Defence; and worked in the private sector as Head of Strategy for Jacobs Australia. He retired in 2013 and now works part-time as an independent consultant.

He has written fifteen books on doctrine, strategy, cyber security, and military history. His latest two books are ‘Getting it Right: Integrating the Intelligence, Surveillance and Reconnaissance Enterprise’ in 2014; and ‘Australian Defence Logistics: The Need to Enable and Equip Logistics Transformation’ (with Air Vice-Marshal John Blackburn) in 2014.

He is a Fellow of the Royal Melbourne Institute of Technology (graduating with majors in accounting and economics); a graduate of the United Kingdom's Royal Air Force Staff College; a graduate of the University of New South Wales, with an MA (Hons) in history; a graduate of the Australian Institute of Company Directors; and a graduate of the Australian National University with a PhD in political science and international relations.

Mr Brett Biddington AM

Brett Biddington consults to governments and the private sector on space matters and has more general interests in community resilience, notably in the electronic and communications and cyberspace domains. He maintains strong linkages to all elements of the Australian space community including the national security, space science, astronomy and education sectors. Previously he was a member of the Cisco Systems Space Team, in the vanguard of activities which are transforming global space communications and before that was an officer in the Royal Australian Air Force specialising in intelligence, security and capability development.

Craig Valli

Professor Valli has over 30 years experience in the ICT Industry and consults to industry and government on cyber security and digital forensics issues. He is the Director of Edith Cowan University Security Research Institute and Professor of Digital Forensics.

Craig has over 100 peer reviewed academic publications in cyber security and digital forensics. Craig is also the founder and Chair of the Australian Digital Forensics Conference. His main research and consultancy is focussed on securing networks and critical infrastructures, detection of network borne threats and forensic analysis of cyber security incidents.

Craig is also a Fellow of the Australian Computer Society. Craig is the Director of the Australian Computer Society Centre of Expertise in Security at ECU. He is also the current research director of the Australian Cyber Security Research Institute. Craig is also current Vice President of the High Tech Crime Investigators Association (Australian Chapter) and a Member of the INTERPOL Cyber Crime Experts Group.

TABLE OF CONTENTS

PREFACE

This publication would not have been possible without the support and assistance of several government departments and industry representatives. The senior public officials and industry leaders who participated in this cyber project provided exceptional insight and assistance. A number of interviews and meetings and two major workshops were conducted from March to August 2016; the Institute for Regional Security (IFRS) would like to thank all of those involved in these activities.

The cyber project would not have been possible without the generous support of our sponsors – Nuix, Edith Cowan University, BAE Systems, and Accenture – who also provided sterling assistance in several briefings and discussions on key aspects of cyber security.

This Report aims to highlight that the pace of change of technology including that of the threat landscape is going to continue to accelerate, which demands greater adaptation of both individuals and institutions. This acceleration also means that policy must adapt more responsively in future, necessitating the appropriate structures and processes to enable this to occur.

Given the complexity of the cyber security domain, this Report can only provide a high-level overview of the nature of the technology challenges and the potential areas for policy responses. Readers who wish to discuss and debate aspects of this Report are encouraged to do by preparing a short commentary or longer article for IFRS's professional journal, Security Challenges.

Gary Waters, Brett Biddington, Craig Valli

THE 2016 CENSUS: COMMUNICATIONS DISASTER OR CYBER SECURITY FAILURE?

On 9 August 2016 the Australian Bureau of Statistics (ABS) conducted its five-yearly census. The aim was to have every household in the nation provide some basic information about every person who was in the household (home, flat, hotel, etc.) on the night of 9 August.

An extensive media campaign was run in the weeks before the census informing Australians that the census was going to occur and of their obligations to complete the form on pain of a fine if they did not.

The media campaign also encouraged as many respondents as possible to complete the census on-line and assurances were given that the census website would handle the load.

Finally, the campaign informed Australians that they were obliged to give their names and that the ABS planned to keep these names on a file distinct from the aggregated census data for more than four years, instead of the 18 month period that had been the norm for previous censuses.

In the days immediately before the census, privacy advocates questioned the need, legality and legitimacy of the ABS collecting and keeping names of respondents for an extended period. The ABS said that the names were needed for two reasons:

- to, in effect, mark the roll to ensure that all who could complete the census had done so; and

- to permit, through an assigned unique statistical identifier, data from other government databases, to be added to the census data to make for a richer and more granular dataset overall.

Privacy advocates raised concern about the implications of the latter process. It seems to offer the possibility of moving the census away from being a snapshot of the nation at a point in time to be the basis for continuous data collection and data comparison from other sources such as the Australian Taxation Office and the Department of Human Services. Several Senators said that they would not provide their names, which put them potentially in breach of the law and liable to a fine.

SEVERAL SENATORS SAID THAT THEY WOULD NOT PROVIDE THEIR NAMES, WHICH PUT THEM POTENTIALLY IN BREACH OF THE LAW AND LIABLE TO A FINE.

The ABS response to these criticisms and critics was confused and unconvincing.

On the day of the census, according to media reports, several Denial of Service (DoS) attacks against the census website were detected and defeated. However, in the evening when the load on the website was greatest, it collapsed and was taken down by ABS staff. Whether this was the result of a massive Distributed Denial of Service (DDoS) attack or simply a reflection that the system was not able to cope with the numbers of Australians seeking to access the website remains, at time of writing, unknown.

Once again the response from the ABS, this time with the responsible Minister involved, was still confused. A failed router was blamed at one point with no explanation given as to what a router is or how the failure of this device placed the entire census in jeopardy.

In the immediate aftermath political opportunism took over. One senior Minister, for example, accused the Chinese of having orchestrated the attack. As the enormity of the failure of the IT system that Australians had been assured would handle the load on census night became apparent, the Prime Minister promised an inquiry and said that heads would roll.

At time of writing, the speculation notwithstanding, the cause or causes for the collapse of the website are either not known or, if known inside government, have not been made public. Three observations are in order:

- Irrespective of the cause(s), the failure of the ABS website on census night has focused public debate on the cyber domain and cyber security in a way not previously experienced.

- The failure of the census, and more especially the repeated failures in communications, have damaged the social contract between the government and the people which points to the urgent need for the development of a national narrative that defines the rights, obligations and duties of citizens in the cyber age.

- Much of the political and media commentary was ill-informed, implying a lack of knowledge about cyber security principles and concepts by many politicians, media and other opinion leaders.

The failure of the census website, combined with the communications failures, reinforce the importance of the Australian Cyber Security Strategy and of the need to implement its numerous initiatives. If this Report leads to better-informed opinion leaders, journalists and the wider public, which provides further impetus to implementing the Strategy, it will have achieved its purpose.

EXECUTIVE SUMMARY

All societies are struggling to create language and terminology that describes and explains how the Internet works and how it relates to the human experiences and daily lives of ordinary people. Three concepts or ideas, in particular, have gained currency that are unhelpful and, indeed, misleading, and need to be called out as such – the digital economy, the hacker, and limits to the utility of analogies.

ALL SOCIETIES ARE STRUGGLING TO CREATE LANGUAGE AND TERMINOLOGY THAT DESCRIBES AND EXPLAINS HOW THE INTERNET WORKS AND HOW IT RELATES TO THE HUMAN EXPERIENCES AND DAILY LIVES OF ORDINARY PEOPLE.

Cyber challenges are as much organisational as they are technical. A resilient cyber security eco-system must address, therefore, (1) security capabilities - the people, infrastructure, and technology that is security focused - and (2) security processes - the culture, structure, policies, and other organisational elements that address how capabilities are used to achieve a desired security outcome. Cyber security is both a business in itself and an enabler to most other activities and enterprises. The responsibility of all working in the cyber security domain is to ensure that broader enterprise and business objectives are not hamstrung by a security system that is unduly restrictive and limiting.

One of the most immediate cyber security challenges is to address cyber security for the Internet of Things (IoT) that provides flexibility, adaptability and resilience, and that can be codified into security best practices. More broadly, Australia needs to define standards/ guidelines for Information Technology (IT) and information systems interoperability; understand the potential security, performance, and reliability implications when extending functionality of legacy systems; develop clear responsibilities for all the participants in the cyber ecosystem; and know the data – its quantity, variety, and what is held by third parties and where it is held – so that a baseline of access and usage can be established that will allow possible abnormalities to be readily and reliably identified and investigated.

In Australia the nature of the current threat landscape, from both technical and human perspectives, is reasonably well understood. There is good awareness of the potential damage that can be caused by 'trusted insiders' who make a mistake or who act with malicious intent. Less well understood is the magnitude of the changes that are coming and the implications of these changes for the security of cyber enabled systems. Incremental approaches to security in future will not be able to deal with the increase in the number of addresses available and devices connected and connecting to the Internet.

The confluence of IPv6 and IoT will create a threat landscape that demands new policy, organisational and technical responses to ensure that Australia's cyber defences remain strong enough to deter attackers and sufficiently resilient to deal with those that persist. The pace of change in the cyber threat landscape and the technologies means that the Australian Cyber Security Strategy needs to be dynamic and subject to review and update.

A major implementation challenge now is to take the words of the 2016 Cyber Security Strategy and roll them out into tangible and valuable outcomes through the initiatives in the Strategy and others suggested in this Report. This challenge is all about execution – giving effect to the good intentions of the Strategy and feeding back lessons learnt, in an iterative and dynamic process. The whole strategy-to-execution process must be dynamic with feedback loops valued and made explicit. The imperative is to make a start on all of the initiatives outlined in the Strategy document, seizing those that take root quickly and accelerating their development. Some may not take root and should be left to the side.

Developing partnerships, sharing information, building trust, educating society, encouraging innovation, and developing the professional skills in the cyber workforce form the foundation for a successful cyber security ecosystem. All require hard work. Success across these domains will not be even and is likely to occur over different timescales.

INCREMENTAL APPROACHES TO SECURITY IN FUTURE WILL NOT BE ABLE TO DEAL WITH THE INCREASE IN THE NUMBER OF ADDRESSES AVAILABLE AND DEVICES CONNECTED AND CONNECTING TO THE INTERNET.

The timing is right for Australia to take a more prominent collaborative role in building a more resilient cyber ecosystem in the Asia Pacific region. There are practical co-operative measures that can be addressed immediately, such as dealing with cyber enabled crime and cyber crime. Australia should work with regional partners to establish a permanent mechanism for regional co-ordination and information sharing on the ubiquitous impacts of ICT systems on local, national and regional economies. A regional Cyber Security Action Task Force, in like vein to the international Financial Action Task Force, could be set up.

Remotely Piloted Aircraft Systems (RPASs) provide a case study that exemplifies the key aspects of the tempo of technological change and the need for adaptation and appropriate policy responses. The case study is presented at Annex A to this Report. The Report makes a significant number of important observations, which are consolidated and presented in Annex B.

Workshop participants accepted as read the fundamental dependence of economies on resilient and adaptable cyber security systems. From this broad acceptance emerged various proposals to strengthen cyber security policy development and implementation. These are expressed as a series of recommendations or actions listed below. Although responsibility for leading these various initiatives was not assigned, there is a clear inference that collaboration between governments, the private sector and research organisations will be an essential ingredient of success. The study participants acknowledged that government already is implementing a number of the initiatives proposed and, in these cases, the participants simply encouraged government to keep working as expeditiously as practicable.

The proposals and initiatives have been grouped below under five headings: domestic policy and legislative initiatives, measures to stimulate growth of an Australian cyber security industry; education, and regional initiatives. Time limitations prevented an evaluation of the relative merit or priority of these initiatives and, with one exception, no attempt was made to assign responsibility for leadership or implementation. There was, however, wide agreement, that collaboration between governments, the private sector and research organisations will be an essential ingredient of success.

Policy and Legislative Initiatives

- **Map**, measure and baseline the Australian and regional cyber eco-system and cyber security eco-system.
- **Determine** a cyber security model for the IoT that is flexible, adaptable and resilient, and that can be codified into guidelines of best practice.
- **Ensure** the strategy-to-execution process is dynamic - take the words of the new Strategy and roll them out into tangible and valuable outcomes through the initiatives in the Strategy and others suggested in this IFRS Report - feeding back the lessons learnt, and adjusting the Strategy.
- **Overhaul** domestic legislation and contribute to international legislative change.

- **Address** the increased autonomy in cyber physical systems (cars, appliances, and remotely piloted aircraft systems) for liabilities, responsibilities, and policy (and financial incentives) for in-built cyber security and resilience.
- **Ensure** stronger authentication and digital identity management.
- **Address** the policy challenge of maintaining freedom of the Internet, while lifting cyber security protections.

Stimulate growth of Australian Cyber Security Industry

- **Provide** greater support for Australian Industry, including through buying locally, and encouraging innovation and exports through practical actions.

Education

- **Provide** the underpinning policies, structures and funding to support a more holistic approach to cyber security education at all levels - primary, secondary and tertiary - that extends into life-long learning programs for cyber security, producing a stable, safe cyber security eco-system for the economy and society more broadly.
- **Ensure** greater cyber co-ordination across federal and state authorities in Australia, including by addressing cyber security as a Council of Australian Governments (COAG) agenda item, preferably through a dedicated Working Group. Australia could then leverage that strengthened domestic cyber security situation into greater regional collaboration.

Regional Initiatives

- **Use** law enforcement as the principal vector for greater domestic and regional collaboration and co-ordination.

A Practical Next Step

- IFRS AiGroup (AiG) and the Australian Cyber Security Research Institute (ACSRI) will explore the possibility of jointly developing a proposal for submssion to Government to pursue 1.5 track mechanisms for improving collaboration in regional cyber security. A first step could be to survey AiGroup members on their approach and concerns with respect to cyber security. The 1.5 track mechanisms would be tailored to address three sub-groupings of regional nations that broadly reflect their cyber maturity:
    - the strong cyber-aware nations (to include Singapore);
    - the ASEAN states; and
    - PNG and the Pacific Island states.

INTRODUCTION

The Prime Minister released *Australia's Cyber Security Strategy* on 21 April 2016, making clear that effective cyber security was integral to economic activity at the global, regional, and national levels. The Prime Minister also announced several new positions and appointments including:

- an Assistant Minister for Cyber Security;
- a Special Adviser to the Prime Minister on Cyber Security;
- a Cyber Ambassador within the Department of Foreign affairs and Trade; and
- the creation of a Cyber Security Growth Centre with nodes across all Australian States, the intention of which is to:
    - improve engagement between research and business;
    - improve management and workforce skills;
    - improve access to international markets; and
    - lead to regulatory reform.

Cyber resilience is a key component of cyber security and involves a great deal more than technical approaches to the security of data, networks and devices. Nevertheless, technology is at the heart of the challenge and its tempo and requirement for adaptation demand appropriate policy responses.

Purpose

The Institute for Regional Security (IFRS) conducted a cyber security research project from March to August 2016 to examine the cyber technology challenge and possible policy responses for Australia. The project sought to address three related questions:

- Is the pace of change of technology going to continue to accelerate or is it likely to plateau? And related to that, how does Australia deal with the increasing pace of change in the threat landscape?
- How does the pace of technological change affect the ability of people to adapt – individually and institutionally?
- How does policy adapt and what structures and processes might be put in place to support policy?

In addressing these three questions, it was important to identify what levers exist, or need to be created, to allow a mature cyber security posture to be achieved through strategy and policy-led direction rather than technology-led responses. The new Cyber Security Strategy argued that emergent technologies and concepts such as the Internet of Things (IoT), Big Data, mobiles, automation of knowledge work, and cloud offer tremendous opportunities but the technologies and infrastructure on which they operate must be able to be trusted [or assumed to be insecure from the outset].

Report Structure

This report starts with a discussion on language, and then explores the technology challenges posed by cyber developments and possible policy responses by:

- Addressing the evolving cyber security landscape.
- Developing an Australian cyber eco-system, and setting the new Cyber Security Strategy within that context.
- Introducing the Internet of Things and identifying the associated risk.
- Addressing the tempo of technological change and the need for adaptation and appropriate policy responses, focusing primarily on the Internet of Things.
- Highlighting areas for policy improvement, such as legal and regulatory, innovation, education, and workforce.
- Examining the contributions that Australia might make in building a more resilient regional cyber eco-system.

The Report presents brief concluding comment and a list of major recommendations.

Annex A presents an examination of Remotely Piloted Aircraft Systems (RPASs) as a case study that exemplifies the aspects of the tempo of technological change and the need for adaptation and appropriate policy responses.

Annex B presents a comprehensive summary of the Report's observations.

A NOTE ABOUT LANGUAGE

All societies are struggling to create language that describes and explains how the Internet works and how it relates to the human experiences and daily lives of ordinary people. Three concepts or ideas, in particular, have gained currency that are unhelpful and, indeed, misleading – the digital economy, the hacker, and limits to the utility of analogies.

The digital economy concept. Use of the word “digital” as an adjective before the noun “economy”, implies that there might be other economies that are not digital. Examples of any supply chain, from the most advanced to the most primitive, that are not structured around electronic information systems are almost impossible to find anywhere on Earth. Today, personal, regional, national and global economies are all digital by definition. The “digital” adjective needs to be dropped.

The concept of the ‘hacker’. The term ‘Hacker’ was initially used to describe someone who found novel solutions to a technical problem (and this is still the case within the hacker community). However, its contemporary use by the media and some commentators now refers to someone that breaks into computer systems as a hacker. Thus, the term now conjures up an image of a young man, somewhat isolated from his peers, spending hours in front of his computer in his bedroom at home, breaking into the networks of intelligence agencies and other government departments and generally causing a good deal of strife and disruption. “Hackers”, in the minds of many are misguided and maladjusted people who attract a degree of sympathy and who need help. This Report makes the uncompromising point that hackers are, in fact, criminals who are involved in criminal acts. Gaining unauthorised access to a computer system in the cyber world is no different in principle, to ‘breaking and entering’ in the physical world. Removing data from a computer system in the cyber world is no different, in principle, to stealing or theft in the physical world. Defacing a website in the cyber world is akin to vandalism in the physical world. The word “hacker” must be removed from the lexicon and replaced with the accurate description “cyber criminal”. Illegal activity needs to be called out for what it is.

Limits to the use of analogies from biology to explain the Internet. The use of concepts from biology to explain the workings of the Internet are commonplace. Computer “viruses” and the need for “computer hygiene” are common expressions that, by analogy, are attempts to bring the arcane world and language of computing into common reach. There is, however, a downside. An inference from these and similar analogies is that disruption of the services provided by the Internet is to be anticipated and dealt with as an element of the natural order. Such attitudes often mask underlying criminal behaviour and activity, which can lead to values of complacency and forgiveness being more prominent than values of lawful behaviour with clearly understood and socially expected consequences for transgression.

THE WORD “HACKER” MUST BE REMOVED FROM THE LEXICON AND REPLACED WITH THE ACCURATE DESCRIPTION “CYBER CRIMINAL”. ILLEGAL ACTIVITY NEEDS TO BE CALLED OUT FOR WHAT IT IS.

Humans use language to construct and describe reality, and how that reality is conceived and shared directly influences perceptions of risk and reward, opportunity and constraint, action and restraint. A deep responsibility of all who are working to make cyberspace more safe, secure and resilient is to use language that notes the ubiquity of the cyber eco-system and calls out unacceptable, indeed illegal, behaviour when and where it occurs.

THE EVOLVING CYBER THREAT LANDSCAPE

The cyber threat landscape has evolved significantly with respect to the frequency, maliciousness and sophistication of attacks. Breaches are becoming more targeted and attackers are more effective at breaking through defences, principally because of the continuing poor IT hygiene and legacy systems, and the new, technologically-advanced attacks.

Furthermore, enterprises themselves are complicating and growing security issues by moving critical functions to the cloud, adopting social media and allowing a bring-your-own-device (BYOD) policy and practice for their personnel. While each of these offers operating efficiencies and enhanced productivity, the combined practices also expand the number and complexity of devices and connections (end-points) that require monitoring, as well as the number of places where critical-value data is stored, processed, and transmitted. These vulnerable end-points and critical-value data points are potential entry areas for attackers to sensitive data and cyber physical IT assets. They are also points of leakage and attack for insiders, malicious or benign. Regardless of the intent, the results are the same.

Traditional network security solutions are not applied consistently and effectively, and thus, many organisations are not keeping pace with increasingly complex IT environments and a rapidly evolving threat landscape. The threat environment is characterised by:

- In 2012, 9 billion devices were connected to the Internet; Cisco estimates that by 2020, that figure will be 50 billion.

- Traditional software applications have increased from 83 million in 2012 to over 141 million in 2016.
- In 2009, it took on average 4.5 months to create an application; by 2015 that was down to 1.5 days.

Australia's new Cyber Security Strategy made the observations that the average Australian household will have 24 devices connected on-line in 2019, and that the market for connected home devices is expected to grow eleven-fold to 2019. Furthermore, the Strategy argued that Australia is experiencing an increasing number of cyber security incidents and number of targets, and greater sophistication of attacks. The Strategy did not say, however, whether the increase is due to more incidents and targets, or whether the increase is as a result of more reporting. Nor did the Strategy attempt to classify the attacks - whether basic or sophisticated.

THE CYBER THREAT LANDSCAPE HAS EVOLVED SIGNIFICANTLY WITH RESPECT TO THE FREQUENCY, MALICIOUSNESS AND SOPHISTICATION OF ATTACKS.

The confluence of the following factors has impacted cyber security:

- Technology is enabling greater frequency, sophistication and maliciousness of attacks.
- Attack methods that have been successful for almost four decades are still not being remediated with any consistency or collective defensive approach across government and industry.
- Growth of cloud workloads, and migration of data to, and greater concentration of data in, the cloud.
- A strong, lucrative black market for personally identifiable information, corporate data, payment card data, healthcare information, and intellectual property.

- Expansion and porosity of the network perimeter to incorporate a greater number of connected devices with access to sensitive data.
- The increasing ability as a result of this connectedness to manifest cyber physical attacks.
- Lack of preparedness and insufficient testing and training by enterprises in protecting systems and data, both legacy and emergent.

DEVELOPING AN AUSTRALIAN CYBER ECO-SYSTEM

The extensive reach and complex nature of the emerging cyber threat environment suggests the need to think of cyber as an 'eco-system'. Indeed, this notion of an eco-system is reflected in the 2016 Cyber Security Strategy in that the major themes and substantial number of initiatives extend across such a broad front. However, Government can only influence part of the cyber eco-system as most of the technology is outside the direct ownership and control of Federal and State Governments, and the bulk of the end-users are outside Government's direct control as well. Almost all of Australia's critical infrastructure in the following sectors is held privately - energy, telecommunications, transport, water, food and agriculture, finance and banking. Health infrastructures (mainly hospitals) are a mix of private and public ownership.

ALL ELEMENTS OF THE NATION'S CRITICAL INFRASTRUCTURE ARE FUNDAMENTALLY DEPENDENT ON ASSURED, SECURE AND RELIABLE ACCESS TO UNDERPINNING INFORMATION SYSTEMS TO PERFORM THE MYRIAD OF TRANSACTIONAL PROCESSES UP AND DOWN THE VARIOUS SUPPLY CHAINS.

All elements of the nation's critical infrastructure are fundamentally dependent on assured, secure and reliable access to underpinning information systems to perform the myriad of transactional processes up and down the various supply chains. Billing, stock orders, payments, production orders, consignment notes, salaries and wages, movement schedules, the list is endless, are performed with less and less human intervention as systems become more tightly integrated, coupled together and dependent. Networks do not merely carry data from one place to another; increasingly, they sense, assess the data gathered and respond.

This is how the modern economy works – underpinned by the cyber eco-system.

A key sub-text of the new Cyber Security Strategy is an open, free and secure Internet. However, the threats are multiplying as technology advances and more and more people and devices become connected – both externally and internally - thereby increasing the attack surfaces. The Strategy's basic premise is that: *Strong cyber security is a fundamental element of our growth and prosperity in a global economy. It is also vital for our national security.*

The first theme of the Cyber Security Strategy is that strong cyber security requires partnership involving governments, the private sector and the community, and the dialogue between government and business must be a daily occurrence, which is a significant challenge as there are cultural differences, and differences in needs and wants that must be addressed. It would be valuable to examine the true cost of cyber-enabled crime as a start in this theme.

The second theme is that Australia's cyber security is built on a solid foundation but the Cyber Security Strategy calls for cyber defences to be strengthened so that Australia's networks and systems are hardened against compromise and resilient to cyber attacks. It acknowledges the need to provide additional staff for the Australian Cyber Security Centre (ACSC) and Computer Emergency Response Team (CERT) Australia, as well as other organisations charged with the 'protect' dimension. It also highlights the need to improve information sharing, particularly developing joint threat intelligence sharing centres in the States and with the Federal Government that involve industry and government.

The third theme acknowledges that to grow, Australia needs to innovate and further diversify its economy to access new markets and new forms of wealth creation, which demands innovation in cyber security to enable secure platforms on which to achieve this diversification. Encouraging an export industry in Australia is important, and the nation needs to stop being self-limiting, be more willing to celebrate success, and be less risk averse. Israel, for example, has codified its cyber export licensing policy that now supports Industry, and has seen cyber-related exports increase significantly (doubling from 2014 to 2015).

The fourth theme is that, globally, Australia needs to actively develop and promote an open, free and secure cyberspace in which to interact. It needs to be more proactive in regional capacity building, and the role of the new cyber ambassador will be instrumental in this. Australia needs to ensure that there is no safe-haven anywhere in the world for cyber criminals, and actually moving out into the world is important in this respect (as exemplified by Australian Federal Police officers operating overseas, in conjunction with their international counterparts).

The fifth and final theme is that, domestically, Australia and Australians need to have the cyber security skills and knowledge to thrive in the digital age. Being a cyber-smart nation means building a common cyber security narrative and culture that emerges from Australia's core educational institutions. It is not sufficient to simply say “We will do this”. It must be done; it is an imperative. This imperative means starting at primary and secondary schools and extending ongoing education into life-learning programs. Education is also important in changing end-user behaviour; and mechanisms for measuring this change will need to be devised. A well-educated workforce and population of end-users can build a great human firewall for the future.

STRONG CYBER SECURITY IS A FUNDAMENTAL ELEMENT OF OUR GROWTH AND PROSPERITY IN A GLOBAL ECONOMY. IT IS ALSO VITAL FOR OUR NATIONAL SECURITY.

Appointment of an Assistant Minister for Cyber Security, the Special Adviser to the Prime Minister on Cyber Security, and the Cyber Ambassador within the Department of Foreign Affairs and Trade, together with the creation of a nationally co-ordinated Cyber Security Growth Centre, provides a once-in-a-generation opportunity to improve cyber security and to enable a secure cyber eco-system for Australia. However, the Strategy itself has to be implemented and everything must be done to ensure the agencies tasked with the action items are provided with the right funding, right structures and right policies to succeed. In this, the Special Adviser to the Prime Minister on Cyber Security can help set the priorities against the objectives of the operational agencies, but this must be done as a partnership. It would be useful to set up an independent expert advisory group to support the Special Adviser.

A whole-of-nation approach is needed to lift Australia's cyber security capacity. Thus, there must be a public-facing aspect where the Special Adviser interacts regularly with the community, industry and government. Monthly bulletins and quarterly meetings would be a useful way forward in this regard. Only in this way can a cultural shift be realised across Government, industry and the community. Development of a shared narrative is essential – one that explains the challenges and potential solutions as information technology now affects every person every day. Law enforcement also needs to change, from after-event investigations to being much more proactive, which has significant resourcing issues.

Government cannot hope to control the totality of the cyber eco-system, so all components need to be encouraged to come together in a true spirit of co-operation, collaboration and co-ordination. The Internet is a series of public places – some really good, some not so good, and some really bad. Government can play a role in helping these public places to be safer, highlighting that cyber breaches are caused by human actions and failures, and encouraging people to take cyber threats seriously. Thus, by Government acknowledging that it cannot control all of these public places, it can at least seek to influence them, knowing about the bad things and working with industry and society to remedy them.

There is a need to make products safer, ensuring security is embedded by design. While it is beguiling to think that Government can and should do this, the power really is in the hands of the consumer, underlining the importance of a public education campaign and consumer advocacy.

The high rate of growth of technologies and the role of government and institutions globally (which is less effective) are the two dynamics that need to be considered together. This demands increased attention to digital identities and trust in others as the porosity, penetration and pervasiveness of cyber continues to expand. Behaviour of individuals, institutions, commercial businesses, and governments needs to be considered as a whole. It is time to consider different digital identities for different roles, which demands more of a hardware orientation (at the device level for example) than a software orientation. Secure digital identities and trusted behaviours can start to bridge the gap between technological advances and government/industry responses.

IT IS CRITICAL THAT INFORMATION FEEDS COMING FROM THE SYSTEMS AND DEVICES THAT ARE INCREASINGLY BEING DEPLOYED AS PART OF THE MODERN LANDSCAPE CAN BE VALIDATED AND TRUSTED.

Identity management strategies must include system-to-system communications and system-to-device communications. It is critical that information feeds coming from the systems and devices that are increasingly being deployed as part of the modern landscape can be validated and trusted.

There has been a lack of focus on the cross-over between public policy and industry developments; however, this has been addressed in the Strategy, with a number of the detailed initiatives coming from the private sector. There is a private sector expectation that Government has a role in the ‘protect’ dimension beyond itself and that it actively pursues that role and encourages industry responses and public behaviours. This supports the point made above about influencing the eco-system through culture change, rather than controlling it.

The new Strategy seeks to apply a ‘light-touch’, but it does have the potential for influencing the right cyber security outcomes in a profound way through the detailed initiatives, provided the policy implications of the technology changes identified in this IFRS Report are also addressed.

Achieving consensus on the need to address cyber as an eco-system is important for it permits the possibility of mapping the cyber eco-system and the cyber security eco-system. This mapping could be broken down into mapping cyber crime and the Australian Federal Police (AFP) response; mapping the reporting from the Australian Cybercrime Online Reporting Network (ACORN); mapping infrastructure attacks; mapping Australia's interaction in the international eco-system; and so on. Australia cannot afford to wait for a major cyber threat to materialise before acting. It is now time to do the mapping, involving academia, think tanks, and other research institutions. However, it would be important to fund the mapping task itself, not one or two particular institutions to do the mapping.

In examining the actors in the eco-system, it will be important to clearly identify and understand their motivations. For example, the actors – governments, corporations, individuals/consumers, and organised cyber criminal gangs – have different motivations. Cyber security becomes a significant consequence to government when it has physical manifestations (e.g., the Ukraine power grid failure on 23 December 2015). Increasingly, corporations are losing more money through cyber-enabled crime than through physical crime (theft of goods). Such losses have a negative impact on reputation and consumer confidence. Individuals also suffer more from cyber criminal intrusions than from physical robberies. Understanding and dealing with the different actors presents substantial challenges. These difficulties, however, are not a reason not to try.

The Australian economy is digitally dependent and effective cyber security is essential for the economy's sustainability and resilience. Achieving an acceptable level of resilience, however defined, can only be achieved by all participants in the economy – governments, the private sector and individual citizens developing, sharing and enacting a set of behaviours derived from shared and commonly held values about the importance of cyber security. Cyber security becomes a shared pillar of strength from which national good is achieved. Effective cyber security demands different forms of collaborative behaviour across government, industry, academia and individuals/consumers. There will be failures along the way; these need to be dealt with as they arise, and lessons learnt and applied. The key is to start now, using the new Cyber Security Strategy as the trigger, and its initiatives and the issues identified in this Report as the vectors for priority effort.

ACHIEVING CONSENSUS ON THE NEED TO ADDRESS CYBER AS AN ECO-SYSTEM IS IMPORTANT FOR IT PERMITS THE POSSIBILITY OF MAPPING THE CYBER ECO-SYSTEM AND THE CYBER SECURITY ECO-SYSTEM.

There are sensitivities and conflicting priorities between government (protecting intelligence sources) and industry (when it comes to monetisation) so totally open information sharing is not a realistic goal. However, more information does need to be shared and trust is intrinsic in this. On a positive note, Australia is probably transforming more quickly than other nations as it builds and strengthens this trusted environment across the cyber ecosystem, particularly between government agencies and industry. The financial technology (fintech) industry and venture capital industry are two examples of this successful trusted partnership in Australia.

The opportunity exists now for industry developments to progress in synchronisation with Government imperatives and priorities. Furthermore, this tighter collaboration can lead to exports for industry and regional leadership opportunities for Government, as well as an opportunity to contribute more effectively to the international good.

Securing Australia in cyberspace cannot occur in isolation – Australia can only be secure in a global and regional cyber-secure environment. In cyberspace, the strategic advantages conferred on Australia by its geographic isolation from the rest of the world are negated. All nations have a role in securing themselves and contributing to the security of others. On the national front, the Government cannot just look after itself and Australian industry cannot just look after itself – both need to be working together to look after all players, for the national good. From that position of strength, Australia can then contribute to the regional and international good.

Government needs to look closely at how it classifies data as industry and academia need to be able to access information if there is to be a genuine and effective partnership. This means that sharing the information widely and classifying only a small amount should be the default position, rather than classifying everything by default. Secrecy in some part is challenged by the *modus operandii* of the Internet protocols in that any individual or organisation with sufficient means can readily intercept network transmissions in transit. Government also needs to determine how secret information from law enforcement and intelligence agencies can be declassified (removing any reference to the sources or methods of its collection) within 24 hours, for timely distribution to the private sector when required.

Government and the private sector need to be operating together – sharing information – which must start with operating at the unclassified or protected levels. In this respect, Israel has a strong government/military and industry relationship, which could be emulated to a degree. The relationship is supported through a comprehensive national strategy that involves three distinct layers – robustness, resilience and defence.[1]

THE CHALLENGE IS A NEVER-ENDING ONE, BALANCING THE NEED TO KEEP UP WITH THE THREAT (AND PREFERABLY AHEAD OF IT) AND TO KEEP UP WITH THE FUNCTIONALITY OF THE INFORMATION SYSTEMS.

Two of the principal challenges facing the Australian cyber eco-system and the global cyber eco-system are system assurance and user behaviours. Entities within the eco-system rely on multiple players for their cyber security so there is already a symbiotic relationship between them. The challenge is a never-ending one, balancing the need to keep up with the threat (and preferably ahead of it) and to keep up with the functionality of the information systems.

Technical defences can be excellent; however, ill-discipline, curiosity and other poor behaviours can bring these excellent technical defences undone. In addition, the increasing sophistication of cyber-criminal attacks demands renewed

[1] Robustness is everything needed to maintain sound organisational operations. It involves government working with the private sector on regulations, organisational processes, risk assessment, technical measures, human procedures, corporate norms, etc. Resilience is event-driven and enables an organisation to snap back to good health. It involves information sharing, analysis of attacks, means of containing attacks and a recovery plan.

attention on user behaviour and continuing education of users. A related issue is the propensity of people to put so much personal information in the cyber realm through social media that simply helps the criminals. Better education in this respect – what is referred to as operational security - is needed.

Policy sequencing against the contours of the emerging situation for Australia is a challenge as it is not just the cyber security strategy calling for resources, but also an infrastructure strategy, an education strategy, an innovation strategy, a research and development strategy, and so on – all good strategies that need resourcing. A national security strategy would help in establishing priorities across these competing areas.

In this context, there is a need to bring focus and priority to cyber security to attract more investment dollars. This entails getting better at telling the cyber security story – the public narrative. Australian success stories need to be better publicised, including getting the message out across the region. This leads to ensuring that successes are celebrated as the Cyber Security Strategy initiatives take effect. The Cyber Security Growth Centre will be a pivotal tool in achieving this outcome.

Within the Cyber Security Strategy itself, there is the question of policy/time trade-offs, which add to the challenges for setting priorities that suggest the need for greater support to the Special Adviser to the Prime Minister on Cyber Security, such as a review group or advisory group that examines how the initiatives are progressing. The notion of a cyber security college that focuses education warrants examination – it could also contribute to assessing and re-assessing progress in the Strategy's implementation. While the Strategy is being implemented across a number of agencies, and each is particularly effective in their individual contributions, the need for tight co-ordination and synchronisation is vital for the Strategy to be executed optimally.

THERE IS A NEED FOR THE COMMUNITY TO BECOME BETTER EDUCATED ABOUT RISK TO ALLOW THE PRESENT DEFAULT SETTING OF RISK AVOIDANCE TO BE REPLACED WITH A MORE POSITIVE AND ACCEPTING APPROACH TO RISK.

The new Cyber Security Strategy achieves helpful balances between threat and risk, and trust and opportunity. The utility of these balances will be demonstrated if they reflect in the way in which the initiatives outlined in the strategy are implemented. A related issue concerns the way in which different sorts of risk are valued. In broad terms there are two types of risk. Type 1 risk may be characterised by the phrase 'if this fails then I will be in trouble'. Type 2 risk is characterised by the phrase 'if I don't do this, what are the consequences'. The former is focussed on the individual (person, company, other entity) whereas the latter has a broader system or ecosystem focus. The focus needs to move more to type 2 risk and away from type 1. Furthermore, there is a need for the community to become better educated about risk to allow the present default setting of risk avoidance to be replaced with a more positive and accepting approach to risk. A community that understands that failure sometimes occurs and can provide opportunities for learning is resilient and forward looking. A corollary is that success should be celebrated.

A major implementation challenge now is to take the words of the new Strategy and roll them out into tangible and valuable outcomes through the initiatives in the Strategy and others suggested in this Report. This is all about execution – moving from the good Strategy through the strong initiatives, executing the associated actions and outcomes, feeding back the lessons learnt, and adjusting the Strategy. The whole strategy-to-execution process must be a dynamic one, with feedback loops. A start needs to be made on all the initiatives and those that take root quickly should be subject to accelerated development. Some initiatives may not take root and they should be shelved or even discarded. The question is one of having the right idea at the right time and moving quickly on those 'right' ideas.

THE INTERNET OF THINGS

The Internet of Things (IoT) sometimes referred to as the Internet of Everything (IoE) is perhaps the biggest challenge for policy-makers, and is defined as network interconnectivity in which everyday objects such as machines, appliances, sensors and compute hardware are able to communicate with one another without the need for human-to-computer interaction to perform required tasks. The IoT offers real opportunities for value creation and capture, but these opportunities also introduce significant risks, both new and existing, that demand new strategies for protection. Every new device adds a new attack vector or opportunity for malicious or criminal activity, potentially against devices, data, and users. Furthermore, data aggregation presents an increasingly attractive target for the execution of both cyber-enabled and traditional crime types.

The IoT concept is made possible by the cheap embedded compute devices, ubiquity in connectivity, digital analytics and automation. The IoT has been embraced as a way to improve operations, using it to monitor machines, track supply chains, automate business and industrial processes, automate sensing and monitoring of our environment and interactions with same.

IoT applications typically depend on the closely co-ordinated actions of multiple intersecting layers along the cyber supply chain that interact with infrastructure, clients, and customers. Vulnerabilities exist within each node, and, perhaps more importantly, between nodes in the cyber supply chain. Connections and interfaces in any system are invariably the weakest element of that system. The challenge is to engender necessary and sufficient trust in the system overall to permit the potential and possibilities of the IoT to be realised safely and securely. Consistently robust mechanisms that maintain data confidentiality and integrity and that guard against breaches across the multitude of connected points are most unlikely to be created without some form of policy intervention.

It will, therefore, be important for policy-makers to define standards for interoperability; understand the potential security, performance, and reliability implications when extending functionality of legacy systems; develop clear responsibilities for all the players in the diffuse cyber eco-system; and know the data – its quantity, composition, and what is held by third parties and where it is held – so that a baseline of access and usage can be established that will allow possible abnormalities to be readily and reliably identified and further investigated.

MANY OF THESE CONSUMER DEVICES OR INTELLIGENT CONSUMER GOODS HAVE LITTLE OR NO SECURITY BUILT IN TO THEM, YET ALL HAVE THE ABILITY TO GATHER INFORMATION AND SHARE IT AT AN EXPONENTIAL RATE.

The Information Security Forum (ISF) in their *Threat Horizon 2018* report identified three themes for which organisations should be preparing now: technology adoption dramatically expands the threat landscape; the ability to protect is progressively compromised; and governments are becoming increasingly interventionist. In a formal release of the report, Steve Durbin, managing director of the ISF, argued that IoT is significant because of the increasing impact of more and more devices on the daily lives of people, as well as companies and other organisations. Many of these consumer devices or intelligent consumer goods have little or no security built in to them, yet all have the ability to gather information and share it at an exponential rate, making the job of securing personal data all the more challenging. Furthermore, it should be noted the emergent IoT devices in of themselves can become a vector by which to pivot an attack.

The *Threat Horizon 2018* report doesn't sound positive. After all, the opening of the report warns that organisations are losing their way when it comes to security, struggling with a maze of uncertainty as they grapple with complex technology, proliferation of data, increased regulation, and a serious skills shortage. On a positive note, this report is a prediction of what the future of the threat landscape could – and probably will – look like. It means that organisations can address today's security problems with an eye to the future and begin putting together a proactive approach, rather than waiting to react as specific problems arise.

Managing IoT Risk [2]

Most IoT devices will not typically perform critical functions, nor will they individually store or generate critical data, so at worst if they are attacked, it can reasonably be argued that there will be a degree of annoyance but not much else. Mass effect from compromising IoT devices is determined by the ability to compromise a single/master device that controls many others (single point of failure) or the ability to propagate the attack across many devices simultaneously using distributed methods. Given the distributed nature of much IoT technology, a mass-scale attack can be launched with little effort; i.e., releasing an attack can be accomplished by purchasing, downloading and running the code. Capabilities such as these are possessed by some nation states, but increasingly, also by professional, multi-national cyber criminal organisations such as Anonymous. This observation moves the challenge from cyber crime to national security.

[2] See James Andrew Lewis, 'Managing Risk for the Internet of Things', Centre for Strategic and International Studies, February 2016, for further discussion on managing IoT risk.

Some IoT functions will require data and commands to be encrypted for security. Public Key Infrastructure (PKI) and secure transport layers (SSL and TLS, often designated by HTTPS) can securely exchange encryption keys, and thus larger industrial IoT devices with sufficient compute power may be able to use these existing encryption products. However, simple devices may require new lightweight encryption products that require less memory and processing power as IoT devices are typically low cost with relatively low compute and memory power.

GIVEN THE DISTRIBUTED NATURE OF MUCH IOT TECHNOLOGY, A MASS-SCALE ATTACK CAN BE LAUNCHED WITH LITTLE EFFORT.

Authentication technologies are likely to continue to improve and do so more rapidly than on-board IoT authentication technologies. These technologies will use various combinations of smart phones, cloud-based data analytics, behavioural patterns, and biometrics to securely identify those accessing IoT devices and seeking to issue commands. That said, the challenge to encryption that will come with quantum computing looms large, and is discussed in more detail later in this Report.

Progress in IoT security will be slowed for the same reasons that making cyberspace more secure has been slow – technological uncertainty, limited international co-operation, lack of incentives for improvement, limited regulatory authority for safety, weak on-line identities, and an Internet business model based on exploitation of personal data. However, the same approaches being used to reduce cyber risk can be used to manage IoT risk – research, incentives and regulation. It is worth noting that, experience shows that regulation if poorly designed can impose a significant cost and technological restriction that reduces the opportunity for growth and innovation.

Decision-making about IoT can be improved if three metrics are used to assess risk – the value of data, the criticality of a function, and scalability of failure. These help policy-makers, regulators and legislators to identify where government intervention is needed to secure the IT supply chain and where such actions are not needed. Those IoT devices providing sensitive functions require a higher degree of scrutiny and effort for security. IoT creates risk when the function it performs is critical for life and safety, when the data it generates is highly sensitive, and when the effects of disruption are significantly scalable. Devices that do these things will need to be held to higher standards through government action. Those that do not can be left to market forces and legal action to correct.

Decisions about autonomy will be a key determinant for the efficiency of IoT devices: if human operators intervene in an IoT operation, this will typically decrease efficiency. This also decreases benefits, so decisions will be needed as to when device autonomy is acceptable and when the capability for human intervention must be maintained in the interests of security or where the environment is not well understood and relatively entropic.

IoT will require a graduated scale of protections and security measures that reflect the actual degree of risk, determined not just by potential vulnerability but also by the value and sensitivity of both data and functions in the total IT supply chain. All data is not of equal value. It is critical that data produced from these devices is assessed by examining provenance in supply chains, its privacy impacts and commercial worth within that chain and also when combined with other source data for commercial or strategic gain. Essentially determining the risk of disclosure of that data to the cyber space.

TEMPO, ADAPTATION AND POLICY

The IoT certainly introduces vulnerabilities and challenges that require policy responses. However, it is not the IoT *per se* that is driving this demand for a policy response, as Internet Protocol version 6 (IPv6) is about to become more broadly adopted. Indeed, the confluence of IPv6 and IoT will create a landscape that allows cyber criminals to launch potent distributed denial of service (DDoS) attacks that bridge the cyber and physical domains and that cause economic and social disruption, the likes of which has not been seen before, as well as introducing other challenges as discussed below.

The sheer number of IPv6 addresses on offer is almost incomprehensible - 2^{128} versus 2^{32} for IPv4. [That is approximately 340,282,366,920,938,463,463,374,607,431,768,211,456 for IPv6 versus approximately 4,294,967,296 for IPv4]. To set this in some form of comparative context, the lifetime heartbeats of the sum of the world's population of 8 billion people, living to 80 years of age, with 80 heartbeats per minute would still be well short of the number of IPv6 addresses. It is this extraordinary size that enables the Internet of Things for the future, but it also enables the Internet of Threats as end user devices have direct accessibility to the Internet.

THE SHEER NUMBER OF IPV6 ADDRESSES ON OFFER IS ALMOST INCOMPREHENSIBLE - 2^{128} VERSUS 2^{32} FOR IPV4.

The move from IPv4 to IPv6 has been going on for so long that it is becoming more like a tradition than a transition. It is vital to understand IPv6 so as to prevent the introduction of security vulnerabilities through configuration mistakes on both endpoint devices (e.g., laptops and mobile devices) and network infrastructure (e.g., routers and switches). IPv6 is being added to networks while IPv4 remains. The two will run in parallel for some time, which doubles the possible problems as network providers will have to monitor and secure both routed protocols.

To take just one subset of the IoT – Industrial Control Systems (ICS) more formally known as Supervisory Control and Data Acquisition (SCADA) systems – these are not managed well currently, and the security community has been dealing with challenges to them for many years. If sensors and actuators can be manipulated, the outcomes can be catastrophic (as Stuxnet showed; which was discovered in 2010 after having targeted Programmable Logic Controllers in Iran's nuclear program centrifuges). Potential outcomes include disruptions to operations, sabotage to the infrastructure, loss of life from damaged infrastructure, cyber attacks, data theft by cyber criminals, cyber espionage by foreign governments, and malicious acts by disgruntled employees or other insiders.

If there is a struggle today to scan addresses used by legacy SCADA devices, how will devices using IPv6 addresses be dealt with in future? IoT wearables (fitness bands, heart trackers) are increasing significantly, and so too is the data being transmitted, and wearables are only a small part of the IoT, for which policy responses are still lacking.

It is this sheer number of devices and possible spaces in the new IPv6 Internet that could provide the trigger for 'Balkanisation' of the Internet (breaking up into separate enclaves) if policy responses are not forthcoming.

Many IoT devices will be small, low-power, embedded devices that use wireless communication, which will, over time, lead to challenges in burgeoning cyber junk and limited wireless spectrum, including in a congested and contested environment. Limited spectrum will conspire against effective communication, as has been the case in Iraq already. A related observation is that the rush to the cloud is creating a bandwidth issue, which indirectly creates a spectrum issue as latency for high-demand applications is not being addressed.

IF THERE IS A STRUGGLE TODAY TO SCAN ADDRESSES USED BY LEGACY SCADA DEVICES, HOW WILL DEVICES USING IPV6 ADDRESSES BE DEALT WITH IN FUTURE?

Decaying technology is a major issue in long term pieces of critical infrastructure for example power and gas networks, water and sewage distribution. The foundation for Australian energy smart grids today is already approaching a decade old, and as the IoT accelerates, such grids and data and devices will proliferate, leading to a lot of data and devices that will no longer be used – leading to a mass and mess of cyber junk. There is a related issue, and that is the potential for any unknown (zero day) defect in a device that was not found at time of manufacture, to become a vector for mass disruption or destruction. These zero days can be and have been found many years after installation of the legacy device. A stark example of this was the recent attacks against the Secure Sockets Layer (SSL) technology that provides secure transmission of data. The previously unknown attacks broke any legacy system that was vulnerable, requiring significant patching or complete refits to occur.

Zero day exploits of devices and indeed known vulnerabilities can allow malevolent actors to move in and out of the device and in and out of the network of similar devices referred to as a grid. Alternatively, such actors can stay and persist in the grid and it may not be possible to remove the threat even once it is known. The only alternative for removal of the threat is the complete removal and replacement of the compromised equipment, a not inexpensive undertaking.

This notion of cyber junk will be an issue across several vectors:

- *Junk in terms of bulk*: how are redundant or legacy elements removed from the environments into which they have been embedded once their useful life is over? (Current examples include plastic in the world's oceans, coffee cups and coffee pods in the physical environment, and the smart grid and SCADA devices in the cyber environment).
- *Junk as a radio spectrum disruptor or sinkhole*: many IoT models/designs currently involve the use of wireless spectrum to provide links for command and control and collection/dissemination of data. How or what is being done to remove elements from the environment so that there is not white ghost noise in the signal space? (As an analogy, 1 cicada can be nice to listen to; however, 1 million cicadas all chirping at once is a nightmare).
- *Junk as a disruptive platform*: using network-enabled devices to pivot off or from which to launch large denial of service attacks, or using them for covert collection of intelligence.
- *Junk as a covert channel*: use of the spare 'memory' in these devices to hide and store illegal artefacts, which has been found already to occur in some operational systems. Or use of the existing communications channels for covert communication.
- *Junk as a disruptor of kinetic energy*: flicking off and on a 1 watt device is not much of a problem; however, switching off and on 10 million devices would produce a 10 megawatt surge.

Quantum computing is another issue – the rapid advance in 'compute' power (Moore's Law) is tapering off, and something like quantum computing will be needed to continue the advances in 'compute' power. Quantum computing is still some way off, but when realised, will mean all current systems become legacy systems because of the ability for quantum computing to break current encryption technologies.

Encryption of electronic content is an essential best practice, despite the fact that many organisations and individual users do not encrypt email or files stored behind their corporate firewalls, files stored in the cloud, and in other venues. However, most IT administrators understand the benefits of encrypting content to protect sensitive or confidential information; to protect their organisations against, and reduce the impact of, data breaches; to satisfy regulatory obligations; and to protect against various types of legal liabilities.

A RELATED ISSUE IS THAT THE AMOUNT OF ELECTRONIC EVIDENCE OF CYBER CRIME BEING PROCESSED HAS INCREASED BY A MAGNITUDE OF THREE FROM 2010 TO 2015.

There is no question that transnational crime is one of the biggest threats confronting Australia. For example, ‘ransomware’ (which encrypts storages on a targeted computer/system and demands a ransom to unlock it) is becoming sophisticated and can be purchased on-line relatively inexpensively. A version of ‘ransomware’, known as ‘jackware’ is on the cusp of being rolled out, which locks up a car or other device until payment is received. ‘Exploits’ are fungible things and are readily available for sale in digital marketplaces and can be purchased via credit card, virtual currency or exchanged for precious metals and minerals.

A related issue is that the amount of electronic evidence of cyber crime being processed has increased by a magnitude of three from 2010 to 2015, based on Western Australian police statistics provided to Edith Cowan University. The costs associated with this data – retention, power requirements, provision of facilities, etc. – are not quantified currently but need to be for the future. Some Australian laws still insist that such data must be retained for 99 years, and much of that data is high-definition imagery, needing significant storage capacity. There are clearly policy and resource implications around data retention for criminal prosecution that need to be addressed urgently.

Cyber security is a highly entropic area in which to develop policy. The pace of technological change is accelerating, as is the pace of change in the threat landscape, and institutions and individuals are struggling to keep up. For example, the Apple i-Phone is less than a decade old, starting at a time when social media was in its infancy. This relatively new technology and new human behaviours for socialising on-line, coupled with the breadth of IoT and corresponding threats, begs the question of how often should a national cyber security strategy be updated and released. It certainly needs to be dynamic and the gap from 2009 to 2016 has been far too long. An annual or bi-annual review is necessary.

In short, there is a need to know where technology is going, know where the threat actors are going, and to get out in front to prevent the more advanced attacks as well as the less-sophisticated traditional attacks. Incentives are needed to start early, such as initiating pilot projects that can gain momentum and demonstrate success. Market incentives can achieve short-term wins, while education and skills development, together with legislation, can be longer-term solutions. Incentivising companies to come forward with breaches and show that in more of a positive light would be a useful step forward.

Binary solutions must be avoided as any tendency for polarisation will simply exacerbate the situation. Cyber security is a multi-faceted challenge and solutions must be multi-faceted, and accommodate significant degrees of interdependence.

One of the major cyber security challenges is to determine a cyber security model for the Internet of Things that is flexible, adaptable and resilient, and that can be codified into standards. As mentioned earlier, the Internet of Things brings with it the Internet of Threats. IoT represents a constant threat and a constant risk that needs to be carefully managed, as discussed earlier.

LEGAL AND REGULATORY ASPECTS

Enforceable mandatory disclosure laws in some overseas countries have made industry take notice as a result of the exposures of the breaches to private data. Without mandatory disclosure laws organisations will continue to hide or deny exposures and loss of data. The current Australian Privacy Principles address information security of personal information, particularly APP11, well. The Privacy Commissioner, however, needs better resourcing to enforce these given the scale of Australia's use of cyber-based systems. It is about end-state trust but to get there, unpleasant and unnerving issues need to be faced and dealt with. The creative tension between threat and trust needs to be better understood and more effectively managed.

THE LEGAL FRAMEWORK FOR CYBER SECURITY IS WELL BEHIND AND HAS PROVEN UNABLE TO KEEP UP WITH THE PACE OF TECHNOLOGICAL CHANGE.

The legal framework for cyber security is well behind and has proven unable to keep up with the pace of technological change. Furthermore, different State laws pertaining to the movement of data (personal data and data for prosecution of criminals) compound the problem.

The biggest legislative policy questions for cyber today that require urgent attention are related to cryptology: (1) To surrender or not surrender crypto keys (current legislation is totally inadequate)? (2) Encryption algorithms are currently treated as a digital munition in terms of exports, but what will happen when quantum computing arrives and what will be Australia's policy framework for exporting quantum solutions and dealing with quantum computing? There are other areas that require policy attention as well – such as manufacturers installing backdoors to enable law enforcement to bypass security mechanisms, and the collection and non-disclosure of methods of bypassing security mechanisms that are maintained by the Australian Signals Directorate.

When information is requested that crosses different legislative jurisdictions, a decision needs to be made quickly and if there is agreement, the data needs to be provided quickly. Anecdotally, it seems that such data currently can take three to six years to be passed across Australia's State jurisdictions. There also needs to be mutual respect for legal positions and legal processes from country to country, which is currently problematic, particularly as there is a general lack of willingness to abide by the legal framework of other countries – exacerbated by out-of-date legislation.

Jurisdictional challenges arise with data flowing across international borders because the data and the person generating it may be subject to different countries' laws. These challenges also lead to international tensions as law enforcement seeks evidence stored on foreign servers to support domestic criminal investigations and as individuals expect domestic privacy protections for data hosted overseas. Increasingly, countries have responded by imposing new requirements to store data locally, thereby threatening cross-border data flows.

A common approach is needed through regional agreements, such as those emerging from the Asia-Pacific Economic Cooperation (APEC) forum, that address privacy issues and that legitimise legal methods for obtaining cross-border access to evidence in criminal investigations. Such an approach to agree on international norms for the free flow of information would also reduce diplomatic tensions between national sovereignty and the borderless Internet, on which the Australian economy increasingly relies.

INNOVATION

An immediate challenge for Australia is to determine how to codify what a free, open and secure Internet means in order to attract investment from industry. This needs to be resolved in the immediate term, especially for entrepreneurs in cryptographic solutions. There is little point in government encouraging innovation, only to lose the innovators through inadequate and out-of-date legislation or regulation (that results in the innovators moving their business overseas). Export control is often about who the customer is, more so than what the technology is, so that will always be a challenge. That said, development of a quantum resistant key will force legislation to change. More responsive structures and mechanisms are needed to ensure legislation can change dynamically and meet the rapidly changing threat.

SERIOUS INVESTIGATION IS NEEDED INTO HOW AUSTRALIAN INNOVATION CAN BE ENCOURAGED AND INTO THE CONCOMITANT INVESTMENT AND SUPPORTING POLICIES AND STRUCTURES THAT ARE LIKELY TO DELIVER SUCCESS.

Australia's regulatory framework needs to accommodate innovative companies that are trying to solve cyber problems and issues. This raises two fundamental questions. How are Australian-owned businesses to grow? And how is confidence grown in the Australian community and government around the concept that Australian-made can be best-of-breed? Serious investigation is needed into how Australian innovation can be encouraged and into the concomitant investment and supporting policies and structures that are likely to deliver success. Government agencies must also be encouraged to procure from Australian companies. Lack of such support for Australian companies carries across to lack of support for Australian research and innovation.

There is also a significant challenge around the export of intangibles, especially for the research community, which needs to be addressed and clarified at a policy level. The Australian Government introduced the Defence Trade Controls Act (DTCA) in 2012. The Act was subject to immediate review and amendments were passed into law in April 2016. The provisions of the Act with respect to intangibles such as the content of a Powerpoint presentation or an email, if applied with undue rigour, may hamper international research collaborations. Australian scientists researching projects of interest to military or intelligence services must seek approval from the Defence Export Control Office before sharing their research results with foreign colleagues. Legal uncertainties have been created and risks have filtered through to risk-averse university bureaucracies. The intent and application of the DTCA has been misunderstood by some universities, leading to unnecessary administrative burdens being imposed on academic staff.

EDUCATION

Strategic investment in education by Australia is crucial, otherwise the supply of talent will be the undoing of the Cyber Security Strategy's execution. Threats and their counters need to be better explained to the community without engendering unnecessary concern or fear. This points to the need for better user/consumer education.

Engagement between industry and academia needs to be bolstered to attract more funding for research. When compared to the comparable investments being made by allies and regional nations, Australia is a noticeable laggard. TAFEs and primary and secondary schools need far more attention and resourcing. Not all cyber security occupations will require a university degree.

WHEN COMPARED TO THE COMPARABLE INVESTMENTS BEING MADE BY ALLIES AND REGIONAL NATIONS, AUSTRALIA IS A NOTICEABLE LAGGARD.

Children from Grade Three onwards need to be ‘captured’ and excited by vocational opportunities that cyber security presents throughout their lives. This means Government, industry and academia need to be working collaboratively in providing the opportunities for education at all levels. The USA CyberPatriot Program (*https://www.uscyberpatriot.org/*) is an example of a successful cyber education program that could be adapted and introduced into Australia.

Currently, the appetite for universities to lead in cyber research and education is driven more by numbers of students than the pursuit of research itself. Greater priority needs to be placed on research by university leaders and a more proactive stance needs to be taken by universities to allow focus to be brought to bear on cyber security, which needs to be encouraged by Government and industry. There is not even a research/study code for cyber security – it is still a subset of computer science.

A national cyber security education curriculum is sorely needed and is being looked at by academia; however, any curriculum will need to be linked to education funding. State-based growth centres can help to accelerate this move, particularly if they are joined up in pursuit of a common good, but funding and political priority are needed if education is to become a powerhouse of change for cyber security. A related challenge is the need for greater support for computer science academics who have disproportionate teaching loads when compared to academics in other disciplines.

CYBER WORKFORCE

There are five forces shaping the workforce of tomorrow:

- Education, training and continual learning in the workplace.
- Collaborative, flexible, innovative, diverse and inclusive behaviours.
- Soft skills as well as technical skills, with feedback and open communication.
- Culture of innovation that harnesses ideas and celebrates successes and failures.
- Opportunities for global engagement and exposure to world's best practice.

Levels of automation need to be increased for greater efficiency, but also to deal with the lack of skilled cyber security specialists. Chris Pogue (the Chief Information Security Officer for Nuix) argues that trained people are the most important component of any organisation's cyber defensive posture, and in that respect, the blending of human intelligence and technology is key to success. He argues the need to engineer out as many human intersection points as possible to reduce the opportunity for errors. In those areas where automation cannot replace human interaction, the people in those positions should be extensively trained and equipped with software that will act as an intelligence multiplier.[3]

[3] See Chris Pogue, 'The Human Vulnerability', Nuix White Paper, 2016.

There is currently too much ambiguity around cyber security training programs and skills. Many organisations are investing in cyber security training programs; however, the content of those training programs is not clear and there is no way of knowing how relevant these programs are to real-world cyber security challenges. Organisations claim they have IT security professionals on-board. However, how well such internal IT security teams are trained, tested and augmented by external experts is not known.

There is a global shortage of talent, with the most acute deficiencies being: cloud security specialists, network security specialists, security analysts (i.e. threat analysts, Security Operations Centre (SOC) personnel, incident responders), and data security specialists. Cyber security education tends to follow an extremely broad curriculum, with cyber security often being treated as a subset of computer science, rather than as a stand-alone subject. While cyber security generalists are needed, specialisation does matter. Employers need specific skills to fill gaps while cyber security professionals can accelerate their careers with training and skills development in high-demand areas. This is the conundrum the Australian cyber security industry faces. Until a strategic plan is developed to greatly improve the supply side of cyber security skills, the demand side will become increasingly chaotic.[4]

[4] See Jon Oltsik, 'High-demand cybersecurity skill sets', *Network World*, 10 May 2016.

A RESILIENT REGIONAL CYBER ECO-SYSTEM

Most Asia-Pacific States now recognise that they are increasingly vulnerable through their greater connectivity and dependence on cyberspace, with the Internet now an integral part of the everyday lives of people in the Asia-Pacific region. Business and banking are increasingly being conducted on-line, which supports national and regional productivity and improved social well-being. The enormous attraction of social networking is resulting in the sharing of a lot of personal information on-line.

Cyber intrusions are occurring daily, in which intellectual property, sensitive government and commercial information, and the identities of individuals are all being stolen. One of the most common attacks currently is ransomware, which does not involve theft. There are also many other crimes that are enabled by the Internet, such as cyber bullying, child pornography, stalking and fraud. In addition, secure communications are enabling organised crime and terrorism, and the ability of terrorists to distribute propaganda and conduct recruitment campaigns from well beyond Australia's jurisdiction. Law enforcement agencies in all countries are ill-equipped to respond to and investigate these crimes. The threat from cyberspace will only worsen as it becomes more tightly enmeshed across regional societies and within their economies.

THE THREAT FROM CYBERSPACE WILL ONLY WORSEN AS IT BECOMES MORE TIGHTLY ENMESHED ACROSS REGIONAL SOCIETIES AND WITHIN THEIR ECONOMIES.

Australia should take a more prominent collaborative role in helping the Asia-Pacific region improve cyber security and build a more resilient regional cyber eco-system. There is an increasing political desire and there are strengthening trade and investment ties across the region, as well as a growing sense of urgency to identify cyber challenges and deal with cyber risks that are critical to the interests of all regional nations. Thus, it is time for regional dialogue and action on cyber policy and practice that focuses on dealing with the shared cyber challenges and risks, and promoting economic growth while ensuring regional stability.

There are practical co-operative measures that can be addressed immediately, such as dealing with cyber crime. Over the longer term and building on the trust established in implementing immediate measures, other measures could be introduced, such as identifying red lines on State-based cyber attacks that could damage critical economic infrastructure, or stopping economic cyber theft.

There are some immediate challenges, however. Regional countries are looking at cyber challenges individually and in piecemeal fashion rather than collectively and holistically, and many have set up their cyber security centres within their intelligence organisations, which makes closer collaboration difficult. Moreover, any collective view on cyber security tends to be driven by the Association of South East Asian Nations (ASEAN) agenda, with cyber discussion forums being built entirely around that much broader agenda.

Language and trust will continue to pose substantial barriers to real progress. However, if practical progress in cyber security cannot be achieved to ensure that trust is solidified, then ‘Balkanisation’ of the Internet becomes a real possibility, as mentioned earlier in this Report. Such a development would not be in Australia's interest.

Another challenge in moving regional cyber security collaboration forward is in terms of CERT to CERT engagement; for example, Indonesia and China each have three different CERTs.

On a more positive note, the Asia-Pacific CERT (APCERT) has achieved a degree of progress and established a solid reputation, proving to be a good model for bringing together multiple countries. APCERT has made a start in addressing general operating policies, procedures and guidelines for regional Internet security. Communication protocols, technical capabilities and incident response mechanisms are all being improved; however, APCERT runs on a low budget.

Thus, APCERT does provide a basis; however, there would need to be a lot more give and take in APCERT forums for real progress to be made in future. The involvement of APCERT with Australia's most important 500 companies is applauded. A more richly resourced APCERT would be able to engage smaller companies and to develop, eventually, a robust and inclusive national cyber resilience eco-system with regional links as well. The joint threat centres proposed in the 2016 Cyber Security Strategy promise to be a vital step in strengthening relationships between APCERT and industry nationally.

THE ASIA-PACIFIC CERT (APCERT) HAS ACHIEVED A DEGREE OF PROGRESS AND ESTABLISHED A SOLID REPUTATION, PROVING TO BE A GOOD MODEL FOR BRINGING TOGETHER MULTIPLE COUNTRIES.

Regionally, ASEAN Regional Forum (ARF) workshops have been conducted on measures to enhance cyber security, including cyber confidence building measures. And the Asia-Pacific Economic Cooperation (APEC) Telecommunications and Information Working Group has recently addressed cyber crime, the dependence of economies on the Internet, mobile security, Domain Name System Security Extensions, and IPv6. Again, these are positive trends, but more can be done at the policy level.

Yet another challenge across the region is convincing companies and operators of critical infrastructure to report data breaches. While the attitude of some businesses is one of accepting the fact that they have been compromised, fixing the breach and learning from it, most tend to cover up breaches.

The real challenge here is overcoming the short-term focus that some regional countries tend to take; evidenced by the smaller countries struggling with their e-crime and data breach investigations. This challenge is being exacerbated as e-crime and data breaches increase across the board, and while these increases force attention to be focussed on the problem, the sheer magnitude overwhelms the local ability to respond.

A Role for Australia

Australia should be proactively involved in developing closer co-operation across the region on information sharing, threat assessments, transnational investigations and domestic legislation development. Furthermore, Australia should advocate for a permanent mechanism for regional co-ordination and information sharing, and offer to co-chair a regional industry forum that addresses the impacts of cyber on the various economies, to discuss: joint research and development projects; transparent global standards; education and training on information security; cyber security mitigation strategies and public awareness; and confidence building through sharing information and best practice. Because of the natural organisational tendency to avoid co-ordinating and collaborating with others, a formal mechanism is needed to make this happen.

In building a more resilient regional cyber eco-system, Australia should be arguing for a sustainable way to promote certainty and stability in cyberspace. There exists an opportunity and perhaps even a responsibility to help create a shared vision and sense of shared mission. There are four crucial areas in this respect: deterrence, mutual restraint, established norms of behaviour, and measures to prevent a crisis arising from misinterpretation or miscommunication. Regional cyber security discussion on these crucial areas needs policy engagement, transparent and respectful dialogue, and an optimistic sense of regional partnership. By promoting such a substantive cyber dialogue, Australia can help promote regional certainty and stability in Asia-Pacific relationships and help create policy settings that are conducive to economic prosperity of all regional nations.

AN INITIAL STEP IN IMPROVING REGIONAL CYBER SECURITY COLLABORATION COULD BE TO BRING THE NATIONAL CYBER SECURITY CENTRES TOGETHER.

An initial step in improving regional cyber security collaboration could be to bring the national cyber security centres together. IFRS could have a leadership role in that regard, but would have to do so in partnership with the Australian Government and others. And, as mentioned above, it would need to address the challenges of language, trust and the dominance of the intelligence communities. In respect of this last challenge, Australia could adopt a brokering role to re-define just what ‘intelligence’ means in cyber discussions to better support policy direction and traction for the region.

Australia's contribution to institutional development and strengthening of whole-of-government approaches in many regional countries has been successful to date and this could be leveraged to address cyber security, noting that PM&C and DFAT have the lead on policy development with regional countries. There is strong support for 1.5 track dialogue (with government and non-government discussions occurring in parallel), discussing cyber issues and challenges and looking for practical areas of collaboration, such as in cyber crime. Extending those discussions to cyber espionage would probably be a step too far at this stage. It would be important to set realistic expectations from the outset.

In partnering with others to project 1.5 track cyber security forums into the region, IFRS would probably have to do so through three separate avenues:

- The cyber-aware nations such as Japan, South Korea, Taiwan, Singapore, New Zealand, India, and China. IFRS could partner with other organisations, such as the Observer Research Foundation in India, to pursue this avenue.
- The ASEAN states minus Singapore. It would probably be necessary to conduct discussions in Singapore, perhaps in partnership with one of the Singaporean think-tanks, such as the Singapore Institute of International Affairs (SIIA), the Institute of Southeast Asian Studies (ISEAS), the Asia Research Institute (ARI), or the Cyber Security Agency (CSA) Singapore.
- PNG and the Pacific Island states, whose focus would be on CERT issues such as technical matters, although some of the more strategic aspects would also need to be addressed. This could be carried out in conjunction with the Australian Cyber Security Research Institute.

Another concrete mechanism that could be used in furthering co-ordination and collaboration in regional cyber security would be to set up a regional Cyber Security Action Task Force, in like vein to the international Financial Action Task Force. This would ensure that Governments and businesses in all Asia-Pacific states were able to work more closely together in partnership to identify, monitor, and manage risks; deal with the vulnerabilities; enforce domestic law; strengthen international law and norms; and improve resilience. This would, of course, demand collaboration to anticipate future threats through all-source assessment, continuous scanning and early warning, and feeding that into regional policy-making through periodic risk assessments and reviews.

Police forces are advancing in the digital forensics area and in some countries they are collaborating domestically better than in Australia. There are strong law enforcement links across regional countries, which open up the channels for dialogue in far better ways than could be achieved through security and intelligence channels.

Law enforcement is the obvious candidate to initiate a common regional approach to cyber security – to build trust, to leverage existing relationships, and to address a common and shared problem. However, Australia must ensure it is doing enough in bringing the Federal and State law enforcement agencies together nationally in the first instance, before expecting to be able to gain traction in contributing to a regional approach. Hong Kong and Singapore have leapfrogged other countries in this respect because they have only the one law enforcement agency. Australia must also ensure that State law enforcement agencies have appropriate resources and training to respond constructively to cyber incidents.

ANOTHER CONCRETE MECHANISM THAT COULD BE USED IN FURTHERING CO-ORDINATION AND COLLABORATION IN REGIONAL CYBER SECURITY WOULD BE TO SET UP A REGIONAL CYBER SECURITY ACTION TASK FORCE.

There are no real policy barriers as such for a regional cyber security approach, apart from restrictions to sharing encryption and on sharing some privacy-related information. It is just that technological developments and commercial responses are moving ahead much faster than policy settings and policy development. The use of mobile phones in banking and finance is a case in point. Thus, the real challenge for Government is in playing catch-up with the technology and the commercial applications of the technology. Meanwhile, the banks and major telecommunications carriers are also being sidelined as these developments gain momentum.

There is also the question of norms. Norms considered legitimate and worthy in Australia are not shared or equally valued by all countries in the region. For example, possession of child pornography is a crime in Australia but it is not in other nation states. Furthermore, regulations are often put in place for specific domestic reasons that do not always translate to the domestic circumstances of other nations. However, geopolitically, Australia is well placed to nurture a cyber security capability regionally, drawing upon the national capability presently being developed.

Complicating the challenge for Government is the fact that Australian commercial entities are moving into the region and adopting a regional perspective for promoting their products (including cyber security products) into each of the countries of the region. Non-Government Organisations (NGOs) are also having a stronger presence and proliferating.

Thus, it is important for the Australian Government to also leverage Australian industry (and NGOs) in developing a regional cyber eco-system. Australian Industry Group (AiG) has many Australian businesses as members that are linked individually to the region, especially in terms of their supply chains. For example, Australian transport and construction companies have established strong commercial links into the region. The Business Council of Australia (BCA) and AiG could be strong brokers with IFRS in reaching into the region through commercial links and joining commercial developments up with government actions.

The Need for Australia to Strengthen Specific Areas

In a commercial sense, Australia is lagging countries such as Singapore, South Korea, China, and the United States, and the technological developments and pace of commercialisation are progressing much faster in these countries that have now gained a critical mass and sense of vision that have them on the crest of a wave that Australia has missed. It is clear that Australia is not doing enough in terms of leadership from either an academic, government or industry perspective. Exports control policy is an important area in this respect that needs a lot of work. Furthermore, if Australian industry is to play a more dominant role in regional cyber security, from an economic perspective, then Australian organisations (both public sector and private) need to be encouraged to buy Australian products first and foremost, as discussed earlier in this Report.

IT IS CLEAR THAT AUSTRALIA IS NOT DOING ENOUGH IN TERMS OF LEADERSHIP FROM EITHER AN ACADEMIC, GOVERNMENT OR INDUSTRY PERSPECTIVE.

Lack of communication from Government and from industry erodes trust; a good example of this is in relation to the 2016 Australian census that was commented on early in this Report. Identity authentication, accreditation and security are the most important technical and policy areas to be addressed in the immediate term to improve trust, both in Government and industry, and in the underpinning systems.

Capable people, capable organisations, the necessary investment funding, innovation and the right government policies to support an Australian cyber security industry need to be found and created. Australia should be able to leverage its collective talent to provide cyber security capabilities; rather than rely on Israel, the US, and other markets. As Data61 CEO Adrian Turner, who was recently appointed as co-chair of the Cyber Security Growth Centre, said in May 2016, there is tremendous opportunity to build a vibrant security industry domestically. He said the new Cyber Security Growth Centre will help bring together industry research and governments to create a national cyber security innovation network; develop a national strategy for Australia to become a global leader and attract investment from multinationals; and co-ordinate cyber security research to reduce overlap. Turner also said that there is a clear economic imperative for cyber security capability in Australia, where the nation has digitally advanced industries, such as banking, that demand comprehensive cyber security capabilities.

Another complicating factor in Australia doing more domestically so as to better influence regional developments is that culturally, Australia has a low tolerance for risk, which is not the case for some regional neighbours. Countries such as Singapore, Hong Kong and Malaysia are moving ahead more quickly in joining up their domestic responses to cyber challenges as they are less risk averse than Australia.

Australia needs to address this broader domestic issue by setting up a Commonwealth of Australian Governments (COAG) Working Group on cyber security to address the national scale of the challenge first before leveraging that into the region. Australia cannot expect to promote a whole-of-region approach to cyber security until it has secured its own whole-of-nation approach. Indeed, this observation suggests that it is not just law enforcement but also Justice and Attorney-General's Departments that should be brought together and use the common ground achieved there to lift the whole cyber issue up to a political and broader policy level.

CONCLUDING COMMENT

Cyber challenges are as much organisational as they are technical, the implications of which include the following:

- There must be a healthy partnership between the public and private sectors to share information and best practices.
- Trust relationships become paramount at every level.
- A focus on IT hygiene is needed, which is day-to-day maintenance and monitoring of devices and IT systems using widely accepted security best practices.
- Resources should not only be focused on defending against cyber attacks, but also on being able to detect vulnerabilities, and limit the damage of a breach. Some cyber security teams refer to the need to: Deflect, Detect, React, Respond, and Recover.
- Emphasis must continue to be placed on upgrading Australia's cyber incident response capabilities, as well as cyber security forensics, in order to quickly identify the perpetrators of attacks and to successfully prosecute them.
- More research and development is needed on new technology for preventing and responding to cyber attacks.
- Further effort is needed to educate and train a cyber security workforce, as demand for cyber security professionals is expected to rise to 6 million globally by 2019, with a projected shortfall of 1.5 million.
- Cyber security needs to be included in all education programs.

- Leaders in government and the private sector must create a culture that ensures everyone treats cyber security as a high priority.

- The cyber world calls for balances to be struck between privacy, freedom of speech, and free flow of information on digital infrastructures on the one hand, while on the other, this has to be balanced with the safety of the public and society as a whole. And all of this needs to occur in a context that allows the economy and innovation to flourish.

- Sovereignty considerations need to be balanced against international obligations in a cyberspace environment that does not respect sovereignty or individual rights, knows no borders, and operates at the speed of light.

- Policy needs to consider incentives for compliance to evolving best practice, provide clarity on responsibility for consequences, and offer guidance on how to deal with future scenarios that the technology explosion will bring, rather than on the individual technologies themselves.

- Regular and realistic threat training needs to be a feature of Australia's cyber security eco-system.

A resilient cyber security ecosystem must address, therefore, (1) security capabilities - the people, infrastructure, and technology that is security focused - and (2) security processes - the culture, structure, policies, and other organisational elements that address how capabilities are used to achieve a desired security outcome. Cyber security is both a business in itself and an enabler to all other activities and enterprises. The responsibility of all working in the cyber security domain is to ensure that broader enterprise and business objectives are not hamstrung by a security system that is unduly restrictive and limiting.

Major Recommendations

The workshops concluded that the priority areas for cyber security policy development and implementation in order to protect and strengthen the economy are:

- Map the cyber eco-system and cyber security eco-system.
- Determine a cyber security model for the deployment of IoT that is flexible, adaptable and resilient, and that can be codified into guidelines of best practice.
- Ensure the strategy-to-execution process is dynamic - take the words of the new Strategy and roll them out into tangible and valuable outcomes through the initiatives in the Strategy and others suggested in this IFRS Report - feeding back the lessons learnt, and adjusting the Strategy.
- Overhaul domestic legislation and contribute to international legislative change.
- Provide greater support for Australian industry, including through buying locally, and encouraging innovation and exports through practical actions. As well as increasing proactive support in cyber defence.
- Provide the underpinning policies, structures and funding to support a more holistic approach to cyber security education at all levels - primary, secondary and tertiary - that extends into life-long learning programs for cyber security, producing a stable, safe cyber security eco-system for the economy.
- Address the increased autonomy in cyber physical systems (cars, appliances, and remotely piloted aircraft systems) for liabilities, responsibilities, and policy (and financial incentives) for in-built cyber security and resilience.

- Ensure stronger authentication and digital identity management.
- Address the policy challenge of maintaining freedom of the Internet, while lifting cyber security protections.
- Ensure greater cyber co-ordination across federal and state authorities in Australia, including by addressing cyber security as a COAG agenda item, preferably through a dedicated Working Group. Australia could then leverage that strengthened domestic cyber security situation into greater regional collaboration.
- Use law enforcement as the principal vector for greater domestic and regional collaboration and co-ordination.
- IFRS, AiG and ACSRI should partner with Government to pursue 1.5 track mechanisms for improving collaboration in regional cyber security. One initial step might be to survey AiG members on their approach and concerns with respect to cyber security. The 1.5 track mechanisms should tailor their approaches to the cyber maturity of regional countries across three different groupings:
    - the strong cyber-aware nations (including Singapore);
    - the ASEAN states; and
    - PNG and the Pacific Island states.

ANNEX A

REMOTELY PILOTED AIRCRAFT SYSTEMS AS A CASE STUDY

Society, industry and commerce are in a period of rapid transformation as the digital revolution becomes more pervasive. Most, if not all, of the technologies that are emerging as a result of this revolution are especially vulnerable to cyber attack. These new capabilities include nano-technology, bio-technology, genetic engineering, autonomous systems, artificial intelligence, and unmanned vehicles, to name only a few.

THERE MUST BE CLOSE CO-ORDINATION DOMESTICALLY, REGIONALLY AND INTERNATIONALLY FOR RPASS TO TAKE THEIR PLACE IN SUPPLY CHAINS.

The second workshop devoted some time to a case study of Remotely Piloted Aircraft Systems (RPASs) as an exemplar of an emerging set of capabilities that are vulnerable to cyber attack from numerous vectors. More commonly known as Unmanned Aerial Vehicles (UAVs) or drones, these aircraft have applications across many industries and sectors of the economy. There is an evolving RPAS industry in Australia that is seeking to develop systems for sale domestically and for export as well, notably into regional markets.

Safety of operations is of paramount concern to operators, users, insurers, flight certification, and air traffic management and control agencies. There must be close co-ordination domestically, regionally and internationally for RPASs to take their place in supply chains.

Community concern about RPASs has been confined largely to the physical risks that smaller, readily purchased devices present to commercial and military aircraft, especially near airports and to the risks to privacy when camera-equipped RPASs are flown above private property without permission. RPASs are basically flying computers, and there is significant potential for cyber security related flaws and vulnerabilities to be exposed and exploited.

Typically, RPASs are controlled by a computer on the ground. Signals are sent on several frequencies from the ground to the RPAS and vice versa. Commands, video signals and information such as speed, altitude or range are examples of the types of data passed. Malware can disrupt any or all of these signals. One strain of malware has already been found to directly affect RPASs; it allows attackers to remotely take control the system and is known as Maldrone.

RPAS operators must consider malware as a threat as RPASs become more involved in commercial enterprises, and as they become commonplace in performing missions in support of agriculture, infrastructure and environmental monitoring, and first response. Military UAVs have already been attacked, and there has been at least one incident of keylogger malware infecting a US UAV fleet, supposedly when an operator used the control PC of a UAV to play a video game.

Building cyber resilience into RPASs is complicated by the diverse threats and vulnerabilities faced by these systems. In addition to these current challenges, policy responses must account for the pace of technological change and the need for rapid adaptation in response to future applications of RPASs, some of which will be innovative and disruptive. Some threats will be malicious, while others will be unintentional. They sum to challenges for programmers, lawmakers and the general public, all of whom need to address RPAS security without reducing the utility of these systems.

For programmers, the most pressing security concern is to develop code that always works whilst avoiding vulnerabilities that criminals can compromise. Privacy is the issue that the general public tends to worry about most as many RPASs carry cameras. However, RPASs can also pose a threat to physical security for the general public as well, as the systems can be modified to carry weapons (typically kinetic, chemical or biological in nature) or to cause physical damage themselves if they crash either accidentally or deliberately.

As regulators and lawmakers examine ways to handle the broader security threats that RPASs in the wrong hands can represent, greater focus is needed on the cyber security aspects associated with malware. The RPAS is emerging technology and the cyber security vulnerabilities and risks inherent in these systems are expected to increase substantially. Perhaps the most worrying immediate security concern for RPASs is their ability to carry explosives and be used in a targeted terrorist attack. Currently, organisations that want to operate an RPAS must have a qualified pilot on staff; yet, hobbyists can fly an RPAS without a licence.

MILITARY UAVS HAVE ALREADY BEEN ATTACKED, AND THERE HAS BEEN AT LEAST ONE INCIDENT OF KEYLOGGER MALWARE INFECTING A US UAV FLEET, SUPPOSEDLY WHEN AN OPERATOR USED THE CONTROL PC OF A UAV TO PLAY A VIDEO GAME.

There needs to be strong assurance regimes around the use of emerging and disruptive technology, such as RPAS, and the potential second- and third-order effects that may result, in particular from their misuse.

To decrease potential security risks involving RPASs additional investment in anti-RPAS research is necessary and there is evidence that this is starting to happen. Terrorist threats, security breaches and cyber security issues are expected to be important drivers of this expanded research. Additionally, countermeasures developed by criminals and other malevolent actors will, themselves, need to be countered. Legislation and regulation is needed to facilitate and not impede this much-needed research.

The RPAS industry is already well ahead of the regulations and moving faster. The nexus between technical complexity and regulation is a difficult issue and how regulators, policy makers and legislators will obtain the requisite knowledge of the technical state-of-play is an enormous challenge; one that may contribute significantly to a lack of willingness to regulate.

Currently, some areas of experimentation that involve cyber attacks against the control systems of RPASs are illegal in Australia under the Telecommunications Interception Act. Modelling and simulation and experimentation inside Faraday cages can only go so far in understanding the behaviour of these increasingly autonomous systems when they are under logical attack.

One RPAS manufacturer has programmed no-fly zones into the systems being offered to the market. The effect is to prevent the operator from flying the RPAS in the vicinity of airports and airfields. But this is just one manufacturer and there is no regulation that insists on such in-built limitations.

Radio communications are the Achilles heel of RPASs. Spectrum allocations, transmitter power levels, receive sensitivities, coding schemes and encryption standards are among the topics to be addressed in order to meet the overriding necessary premise of RPASs, which is that they must be safe. The Civil Aviation Safety Authority (CASA) is aware of the cyber threat to RPAS operations and is working to capture these concerns in policy and regulations; always, and rightly, from a perspective of safety. The RPAS challenge demonstrates the need to build cross-domain information sharing, to use a common language, and to adopt a common approach that acknowledges the breadth and depth of the

THE CIVIL AVIATION SAFETY AUTHORITY (CASA) IS AWARE OF THE CYBER THREAT TO RPAS OPERATIONS AND IS WORKING TO CAPTURE THESE CONCERNS IN POLICY AND REGULATIONS; ALWAYS, AND RIGHTLY, FROM A PERSPECTIVE OF SAFETY.

challenge of addressing the cyber threat in emerging technologies. Clearly, more flexible policy settings are needed, of which responsive regulation is but one lever.

Time is of the essence. The RPAS industry is estimated to be worth $82 billion globally in 2025, with civilian use being driven by advances in power, fuel consumption, communications, encryption, interoperability, ease of use, and new levels of autonomy. If Australian RPAS manufacturers and operators are to benefit from this market nationally, regionally and globally, they need designated test areas and regulatory support to conduct tests that will ultimately demonstrate the resilience of the systems being developed to jamming and cyber attacks whether caused intentionally or unintentionally.

At a higher level of abstraction the notion of a ‘technological singularity’ is gaining traction. This involves the convergence of bio-technology, genetics, advanced materials, nano-technology, autonomous systems, and artificial intelligence, all being mediated by ICT/cyber systems. Using different language, this means that, at their moment of conception, these new technology products are by definition enmeshed in the cyber domain; they are elements of the Internet of Things (IoT).

ANNEX B

SUMMARY OBSERVATIONS

The major observations from this Report are summarised in this Annex.

One of the most immediate cyber security challenges is to address cyber security for the Internet of Things (IoT) that provides flexibility, adaptability and resilience, and that can be codified into security best practices. More broadly, Australia needs to define standards for IT and information systems interoperability; understand the potential security, performance, and reliability implications when extending functionality of legacy systems; develop clear responsibilities for all the players in the diffuse cyber eco-system; and know the data – its quantity, variety, and what is held by third parties and where it is held – so that a baseline of access and usage can be established that will allow possible abnormalities to be readily and reliably identified and investigated.

In Australia the nature of the current threat landscape, from both technical and human perspectives, is reasonably well understood. There is good awareness of the potential damage that can be caused by ‘trusted insiders’ who make a mistake or who act with malicious intent. Less well understood is the magnitude of the changes that are coming and the implications of these changes for cyber security systems. Incremental approaches to security in future will not be able to deal with the exponential increase in the number of addresses available and devices connected and connecting to the Internet.

The confluence of IPv6 and IoT will create a threat landscape that demands new policy, organisational and technical responses to ensure that Australia's cyber defences remain strong enough to deter some attackers and sufficiently resilient to deal with those which persist. The pace of change in the cyber threat landscape and the technologies means that the Australian Cyber Security Strategy needs to be dynamic and subject to continuous review and update.

The challenge of increasing and intense competition for access to the finite resource of the electromagnetic spectrum needs to be addressed as billions of new devices, which define the IoT, are connected wirelessly. As a consequence, policies and other response mechanisms need to be developed for dealing with cyber junk and the increasingly latent defects in much of the old and degrading smart grid equipment, existing Operational Technology (OT) and SCADA networks.

THE PACE OF CHANGE IN THE CYBER THREAT LANDSCAPE AND THE TECHNOLOGIES MEANS THAT THE AUSTRALIAN CYBER SECURITY STRATEGY NEEDS TO BE DYNAMIC AND SUBJECT TO CONTINUOUS REVIEW AND UPDATE.

Quantum computing and the ready availability of 'exploit' technologies, such as ransomware kits are other challenges that need policy responses.

A national security strategy would help in establishing priorities for funding across the competing strategies such as those for cyber security, infrastructure, education, innovation, research and development, and so on.

A cogent national narrative on cyber security is needed to explain the challenges and potential solutions. Government cannot hope to control the totality of the cyber eco-system, so all components need to be encouraged to come together in a true spirit of co-operation, collaboration and co-ordination. The Cyber Security

Growth Centre would be an ideal pivot for this. Furthermore, such a compelling public narrative and celebrating Australian success stories are prerequisites to attracting investment dollars.

Cyber security is an issue of the national good. IT and cyber systems are ubiquitous across all supply chains of the Australian economy today and the nation is increasingly catastrophically dependent on IT's secure operation. The security of IT in supply chains requires a different form of collaborative behaviour across Government, industry, and individuals/consumers, where initiatives can be launched quickly and successes celebrated, accepting that there will be failures which need to be dealt with as they arise.

Government needs to look closely at how it classifies and shares data as industry and academia need to be able to access information if there is to be a genuine and effective partnership. All need to be operating together – sharing information – and this must challenge existing paradigms and move to a need to share rather than the need to know.

A baseline map of the cyber security eco-system should be produced. A cyber security body of knowledge (CSBOK), with agreed lexicon and grammar needs to be generated to provide a common shared understanding of the language of cyber security.

Products must be safer, ensuring security by design; however, while Government has a role, the power really is in the hands of the consumer, further underlining the importance of a public education campaign. However, the need to keep up with the threat (and preferably ahead of it) and the need to keep up with the economic functionality of the information systems must be balanced.

More responsive structures and mechanisms are needed to ensure legislation can change dynamically and meet the rapidly changing threat. Thus, the legal framework needs to be overhauled, State laws need to be harmonised, data retention laws need to be modernised, surrender of crypto keys needs to be addressed, and export of quantum computing needs to be articulated. Indeed, the policy and resource implications around data retention requirements, particularly for prosecuting criminals, need to be addressed urgently. Understanding the true cost of cyber crime and cyber enabled crime would help to bring focus and priority.

Australia needs to better support exports and innovation, which demands legislative change and more government support for Australian technologies and companies. A review of overall regimes around dual use needs to occur to ensure innovation and export potential are not being stifled. Australia needs to stop being self-limiting, be more willing to celebrate success, and be less risk averse if it wants to encourage innovation and an export industry.

A CYBER SECURITY BODY OF KNOWLEDGE (CSBOK), WITH AGREED LEXICON AND GRAMMAR NEEDS TO BE GENERATED TO PROVIDE A COMMON SHARED UNDERSTANDING OF THE LANGUAGE OF CYBER SECURITY.

Greater priority needs to be placed on research by university leaders and a more proactive stance needs to be taken by universities to allow focus to be brought to bear on cyber security, which needs to be encouraged by Government and industry. Government must ensure that cyber security effort can be effectively measured and the provision of specific cyber security field of research codes are a rudiment that are absent. Sustainable funding and continued political priority are needed if education is to become a powerhouse of change for Australia's cyber security eco-system, noting that education is also important in changing end-user behaviour.

A major implementation challenge now is to take the words of the 2016 Cyber Security Strategy and roll them out into tangible and valuable outcomes through the initiatives in the Strategy and others suggested in this Report. This is all about execution – giving effect to the good intentions of the Strategy and feeding back lessons learnt, in an iterative and dynamic process. The whole strategy-to-execution process must be dynamic with feedback loops valued and made explicit. The imperative is to make a start on all of the initiatives outlined in the Strategy document, seizing those that take root quickly and accelerating their development. Some may not take root and should be left to the side.

Developing partnerships, sharing information, building trust, educating society, encouraging innovation, and developing the professional skills in the cyber workforce form the foundation for successful cyber security. All require hard work. Success across these domains will not be even and is likely to occur over different timescales.

The timing is right for Australia to take a more prominent collaborative role in building a more resilient cyber eco-system in the Asia Pacific region. There are practical co-operative measures that can be addressed immediately, such as dealing with cyber crime. Australia should work with regional partners to establish a permanent mechanism for regional co-ordination and information sharing on the ubiquitous impacts of ICT systems on local, national and regional economies. A regional Cyber Security Action Task Force, in like vein to the international Financial Action Task Force, could be set up.

An initial step in improving regional cyber security collaboration could be to bring the national cyber security centres together. IFRS could have a leadership role in that regard, but would have to do so in partnership with the Australian Government and others. IFRS and AiG should partner with Government to pursue 1.5 track mechanisms for improving collaboration in regional cyber security. One initial step might be to survey AiG members on their approach and concerns with respect to cyber security. The 1.5 track mechanisms should tailor their approaches to the cyber maturity of regional countries.

Australia needs to ensure greater cyber co-ordination across its own federal and state authorities, including by addressing cyber security as a COAG agenda item, preferably through a dedicated Working Group, before it can hope to influence greater regional cyber security collaboration. It is also important for the Australian Government to leverage Australian industry (and NGOs) in developing a regional cyber eco-system.

The global economy is a complex cyber ecosystem. The movement of goods and services across cities, nations and the world assumes secure and assured access to the internet. Many processes are becoming automated and all manner of devices are being connected to the internet at an accelerating rate, a phenomenon known as the Internet of Things (IoT).

In March 2016 the Australian Government released its Cyber Security Strategy and this document provided important context for this IFRS study. The study also sought to understand the implications for Australia of regional approaches to cyber security and the roles that Australia might play to strengthen the cyber resilience of regional nations to their benefit and to Australia's as well.

This short report seeks to use plain English to explain concepts that have been for too long relegated by political and business leaders to technical staff who, their best efforts notwithstanding, have struggled to articulate the policy and legislative challenges that the internet, and cyberspace more generally presents to national and global society.

The report, based on the individual contributions and collective judgments of a group of well-informed individuals from diverse backgrounds, makes some recommendations and suggestions that, if implemented, we think will deliver a more secure, resilient and trustworthy internet to Australia and to the region.

INSTITUTE FOR REGIONAL SECURITY

INSIGHTS
IDEAS
IMPACT

Promoting regional
stability and prosperity

www.regionalsecurity.org.au