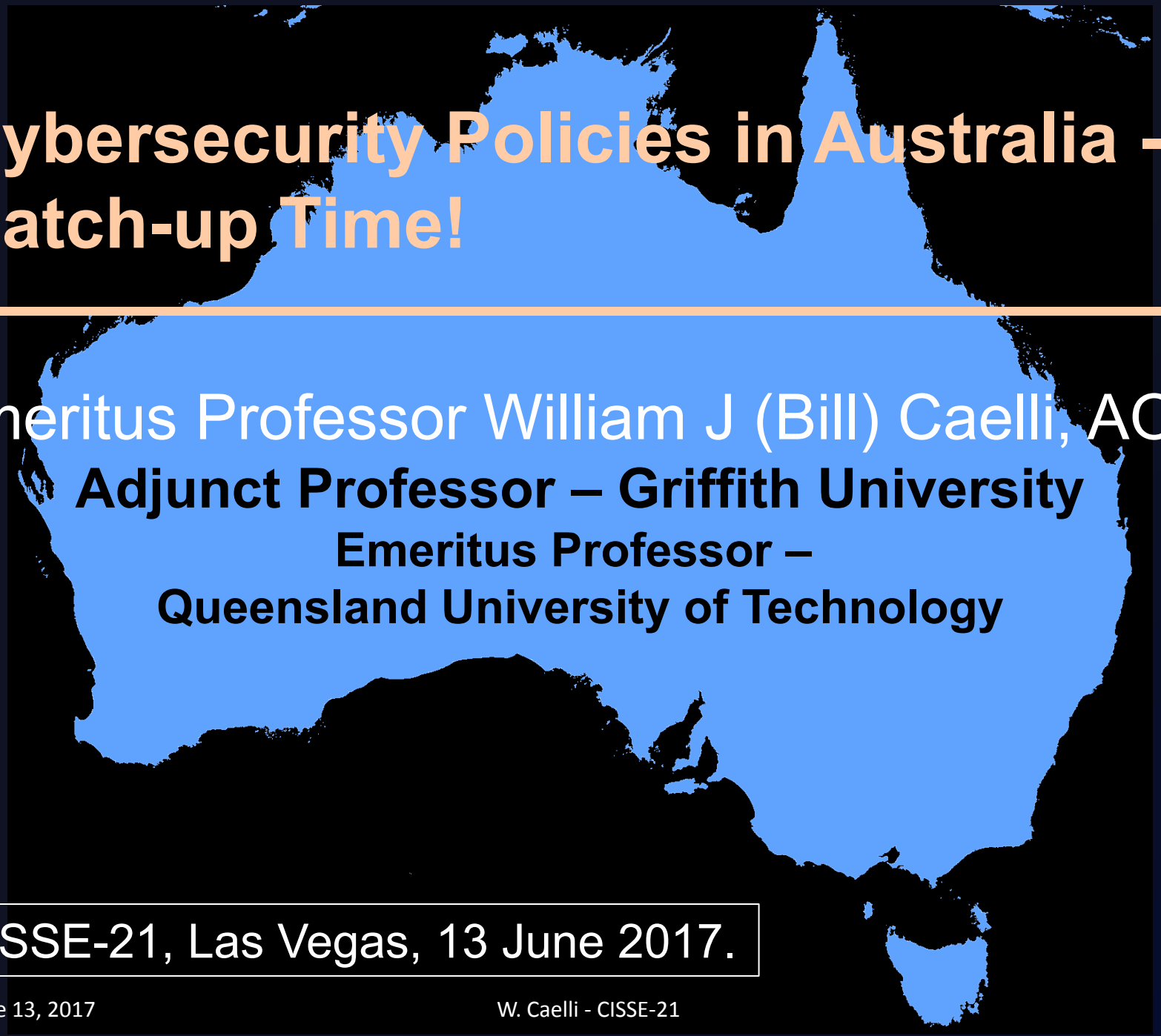
Cybersecurity Policies in Australia - Catch-up Time!



Emeritus Professor William J (Bill) Caelli, AO :

Adjunct Professor – Griffith University

Emeritus Professor –

Queensland University of Technology

CISSE-21, Las Vegas, 13 June 2017.

Agenda:

1. Some background and history.
2. Who's who in Australian Federal Government Cyber Policy – 2017
3. Policy frameworks – 2017
4. Real initiatives – real $$ (?)
5. Cyber training, education and research
6. Cyber business development
7. What's next?

Agenda:

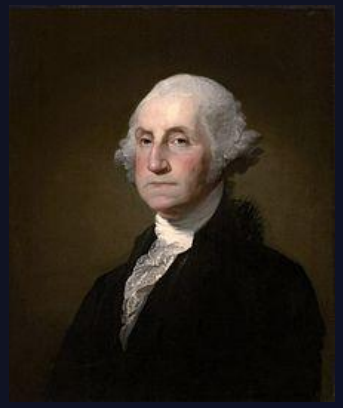
1. **Some background and history.**
2. Who's who in Australian Federal Government Cyber Policy – 2017
3. Policy frameworks – 2017
4. Real initiatives – real $$ (?)
5. Cyber training, education and research
6. Cyber business development
7. What's next?

3A

Speech

of the President of the United States to both Houses of Congress.

January. 8th 1790.



Among the many interesting objects, which will engage your attention, that of providing for the common defence will merit particular regard.— To be prepared for War is one of the most effectual means of preserving peace.

Si vis pacem, para bellum

If you wish for peace,
prepare for war

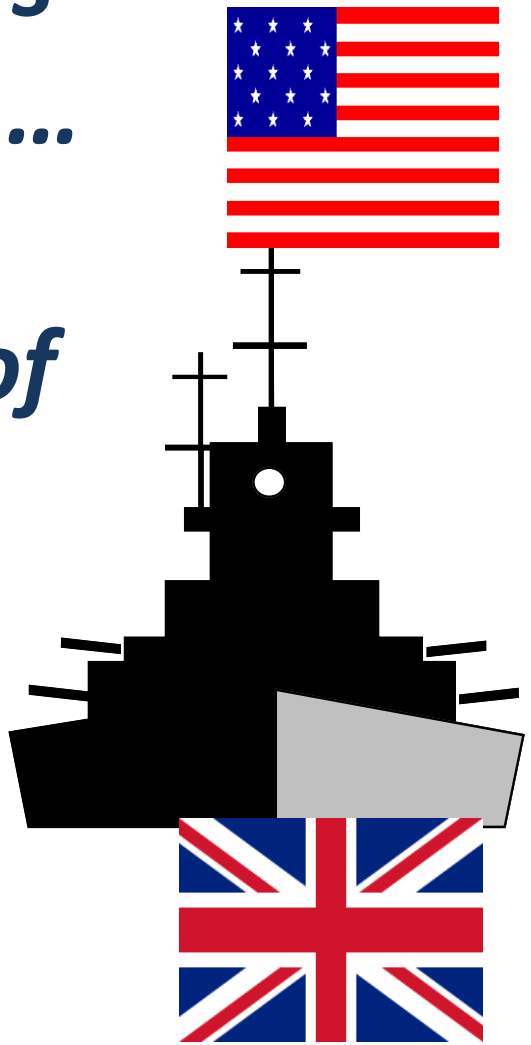
USN
Electronic Attack Squadron
VAQ-139
“Cougars”

UK
Royal Navy

++

“ … in order that His Majesty’s Subjects may do their utmost … to.. capture .. the Ships and Vessels belonging to citizens of the United States,

*and to **destroy their commerce**…”*



18 June 1812 - **USA declares war on Britain –**
(until 24 December 1814)

Circular despatch from
Earl Bathurst to
Governor Macquarie,
New South Wales,
13 October 1812.

Acknowledged by
Governor Macquarie,
28th June 1813.

Battle of the Coral Sea – 4 – 8 May 1942 (75th Anniversary)

Battle of Midway 4 – 7 June 1942

Central Bureau

HYPO SigInt Station – Hawaii
3 April 1942
Japanese Navy JN25 code broken
- Japanese offensive to Port Moresby / Solomon Islands planned.

EDUCATION AND RESEARCH

1987

- Discussion/plan re formation of
- *"Information Security Research Centre (ISRC)"*
- Queensland Institute of Technology
  - University 1989

1988

- ISRC formed (July 1)
- Founding Director – Dr William J Caelli (ERACOM Pty Ltd.)

~2003

- Information Security Institute (Now disbanded)

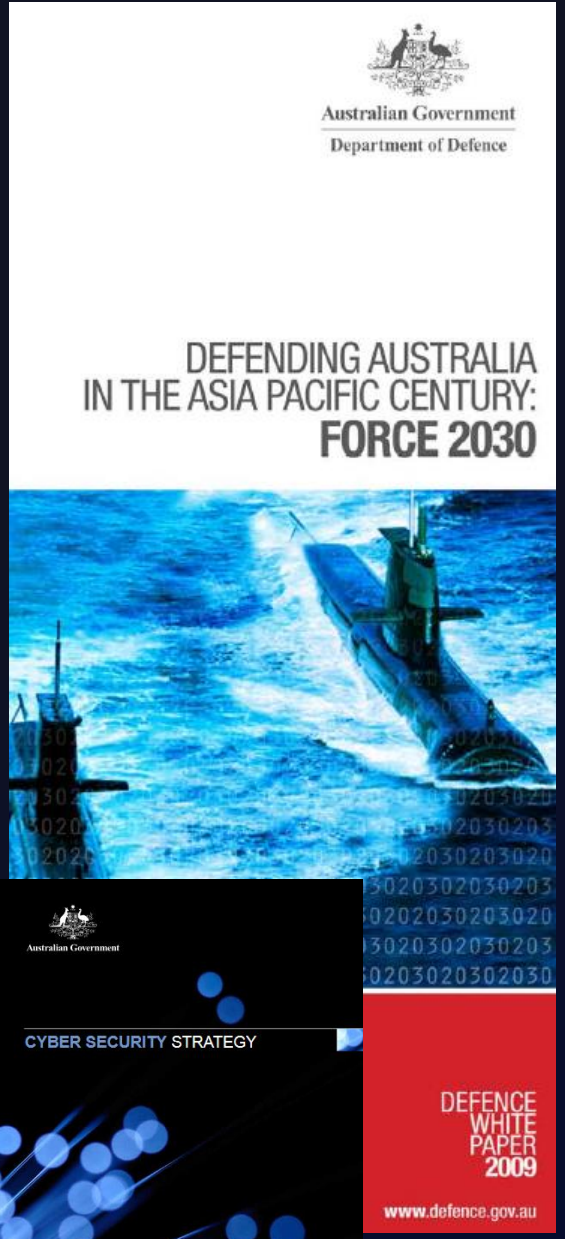
2009:

2009 Cyber Security Strategy – Attorney-General's Dep't

2009 Defence White Paper

Real delays until 2016 !

- **ASPI** View 2017 – catchup!:
  - clarity on national cyber governance,
  - boost confidence in cyber defences,
  - stimulate cyber industry,
  - need to engage Australian private/ public sectors in conversation about cyber policy and security
  - vital for national prosperity



The Hon Kevin Rudd MP
Former Minister for Foreign Affairs

2011

Cooperation on Cyber – a new dimension of the US Alliance

Joint media release : The Hon Kevin Rudd MP, Minister for Foreign Affairs & The Hon Stephen Smith MP, Minister for Defence, 15 September 2011

*The US and Australian Governments agreed today that a **cyber attack** on either of them would trigger the mechanisms of the **ANZUS** Treaty.*

26th Australia-United States Ministerial Consultations (AUSMIN) September 15, 2011

Agenda:

1. Some background and history.
2. **Who's who in Australian Federal Government Cyber Policy – 2017**
3. Policy frameworks – 2017
4. Real initiatives – real $$ (?)
5. Cyber training, education and research
6. Cyber business development
7. What's next?

AUSTRALIA'S
CYBER SECURITY STRATEGY

Enabling innovation, growth & prosperity


Policy
Special Adviser on Cyber Security
(Department of the Prime Minister and Cabinet)
Governance arrangements
(overseen by Special Adviser on Cyber Security)
International Engagement
Cyber Ambassador
(Department of Foreign Affairs and Trade)
Operations
Australian Cyber Security Centre Coordinator
(Department of Defence)

POLICY

Department of Prime Minister & Cabinet (Special Advisor on Cyber Security)

Prime Minister
The Hon. Malcolm Turnbull, MP

Minister Assisting the PM on Cyber Security
The Hon Dan Tehan, MP

Special Advisor on Cyber Security
Mr Alaister McGibbon

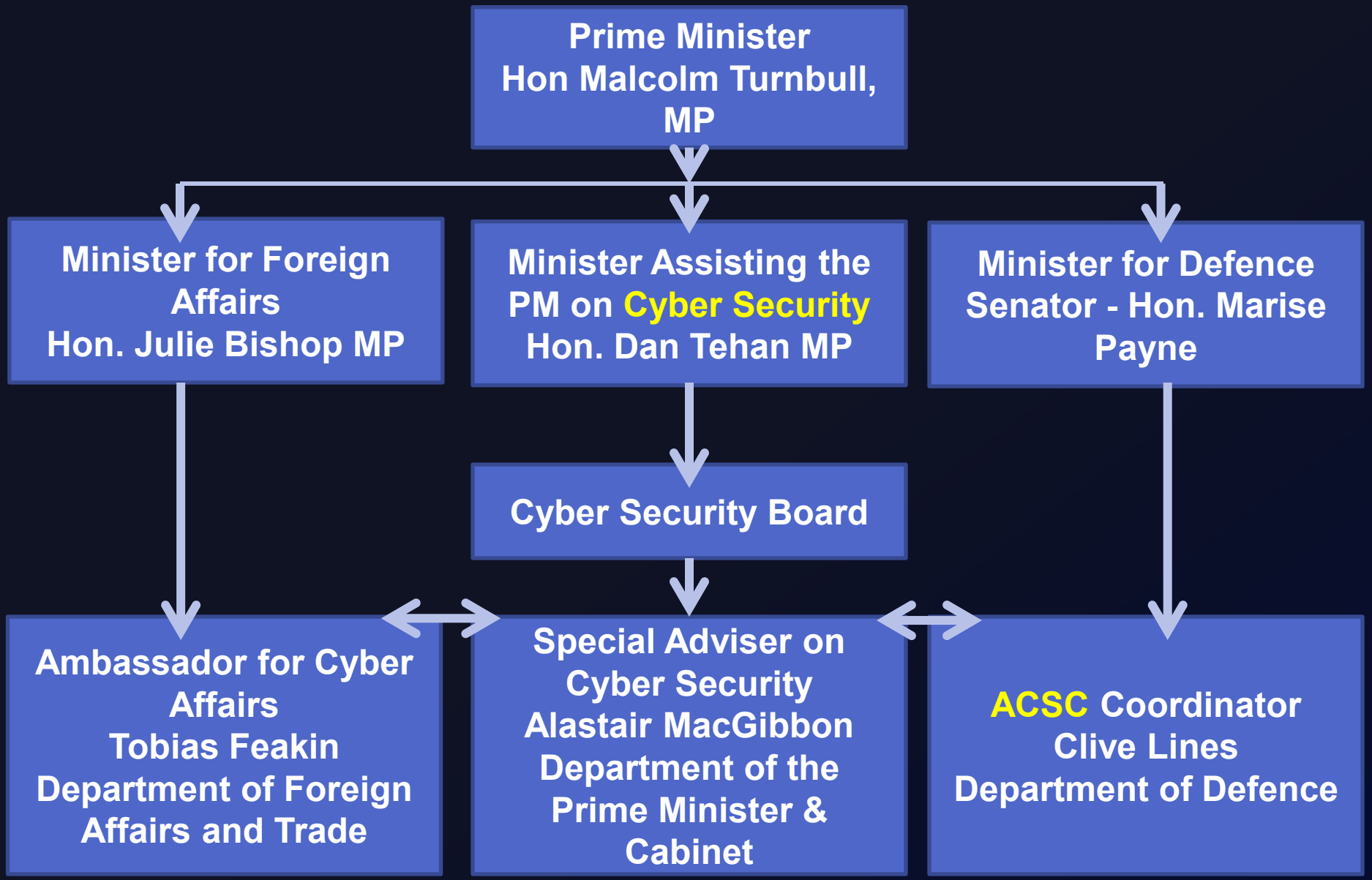
Front Page – The Weekend Australian May 6, 2017.

Minister Assisting the Prime Minister for Cyber Security, Dan Tehan, Prime Minister Malcolm Turnbull and the Prime Minister's Special Adviser for Cyber Security, Alastair MacGibbon at the roundtable on **19 April**.
URL https://www.dpmc.gov.au/news-centre/cyber-security/cybersecurity-roundtable-looks-future

INTERNATIONAL ENGAGEMENT

Department of Foreign Affairs and Trade
Ambassador for Cyber Affairs
Dr Tobias Feakin
(formerly ASPI –
Australian Strategic Policy Institute)

2017 STRUCTURE:

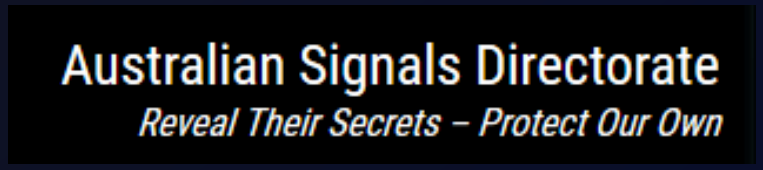


Agenda:

1. Some background and history.
2. Who's who in Australian Federal Government Cyber Policy – 2017
3. **Policy frameworks – 2017**
4. Real initiatives – real $$ (?)
5. Cyber training, education and research
6. Cyber business development
7. What's next?

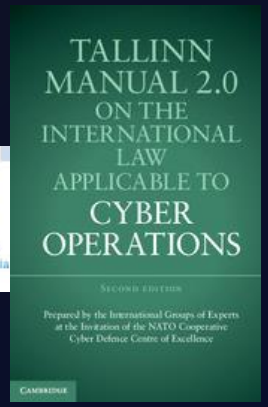
POLICY FRAMEWORKS

- Cyber Security 2016
  - One year Update 2017
- Defence White Paper 2016
- AISEP - Australasian Information Security Evaluation Program
- DECO - Defence Export Controls
  - DSGL - The Defence and Strategic Goods List
  - Wassenaar Arrangement



- UKUSA - 1946
- ANZUS (AUSMIN) – 1951

- NATO - "Tallin Manual"



DEFENCE WHITE PAPER - 2016

*The Government's highest priority will continue to be our alliance with the United States…… Australia's security is underpinned by the **ANZUS Treaty**, United States extended deterrence and access to advanced United States technology and information.* (ANZUS Treaty – 1951)

*The Government is committed to continuing the development of Australia's defence relations with **China**, and working to enhance mutual understanding, facilitate transparency and build trust.*

Reservists: ….technical skills…not readily available in Permanent ADF.

DEFENCE WHITE PAPER - 2016

- New/complex non-geographic threats
  - Cyberspace / space
- Cyber attacks- real/present threat to ADF/Australia
- Defence- contribute to cyber efforts
- Better coordinated cyber security capabilities
  - Industry/academia
- No separate “CYBERCOM”

Senator the Hon Marise Payne Minister for Defence

The Hon Christopher Pyne MP Minister for Defence Industry

The Hon Dan Tehan MP … Minister Assisting the Prime Minister for Cyber Security ++

Agenda:

1. Some background and history.
2. Who's who in Australian Federal Government Cyber Policy – 2017
3. Policy frameworks – 2017
4. **Real initiatives – real $$ (?)**
5. Cyber training, education and research
6. Cyber business development
7. What's next?

CYBERSECURITY 2016 – UPDATE 2017

Proposed Solutions

- Technology – important
  - Cultural change – more effective (blame the victim??)
- Australia – lead in cybersecurity industry
  - Industry-relative infancy (ERACOM 1979!) $$$???
- Innovation & Science agenda
- Defence industry plan
- Fed Gov't - $230M over 4 years
- Address shortage of cybersecurity professionals (Hiring)
- Develop national "stock" of cybersecurity skills
- Deploy defensive & offensive cyber capabilities
- Boost defence cybersecurity

CONTRADICTIONS – CHALLENGES - HISTORY

- Support use of encryption
  - Challenges for law enforcement & security agencies
  - Access data "essential for investigations" (again!)
- Gov't agencies "address challenges" – after 30 years!
- Harden networks and systems
- ASX-100 - voluntary governance = "health checks"
- Support CREST

BUT –

- **"Common Criteria" / AISEP – no mention???**
- **Obligations on suppliers – no mention???**
- **"Blame the user" – implied???**
- **Crypto policy ??**

AUSTRALIA - DIRECTIONS

INDUSTRY

- Cyber – 1 of 9 national science & tech research priorities
- Venture capital ("Angel" vs Rounds ??)
- Support entrepreneurs
  - Visas
- Tax treatment – "angels"
- Concessional tax treatment for investors
- Incubator support
- $36M – 5 year – innovation strategy
- Commercialisation of public research
- $30M "industry led" cyber security growth centres

BUT second round funding?

Agenda:

1. Some background and history.
2. Who's who in Australian Federal Government Cyber Policy – 2017
3. Policy frameworks – 2017
4. Real initiatives – real $$ (?)
5. **Cyber training, education and research**
6. Cyber business development
7. What's next?

AUSTRALIA - DIRECTIONS

EDUCATION & RESEARCH

- Academic Centres of Excellence **(CAEs?)**
- Enhance quality of courses, teachers & professionals
- Undergrad & postgrad education
- Consistent curriculum
- "Superior" teaching
- Skills via TAFE & RTOs

BUT – SFS (Scholarship for Service) ???

- Traditional university vs MOOCs

vs NFP (SANS, ISC^2 , etc)

vs Commercial ???

- Academic staff ??

AUSTRALIA - DIRECTIONS

2017 UPDATE

- $3.45M address education shortage
- Declaration of *"offensive cyber capability"* & deployment
  - Against Islamic State
- More support for SMEs (access to CREST in 2018?)
- Policy on supply chain security
- >40 PhD students
- Oceania Cyber Security Centre – Melbourne
  - 8 Victorian Unis
  - Oxford global cyber security capacity centre (GCSCC)
  - Defence Science Institute
- *"Cyber Boot Camp"* – Ministers & Senior Public Servants

Global Cyber Security Capacity Centre

BUT – expert/experienced academic staff ???

(Accessed May 10, 2017)

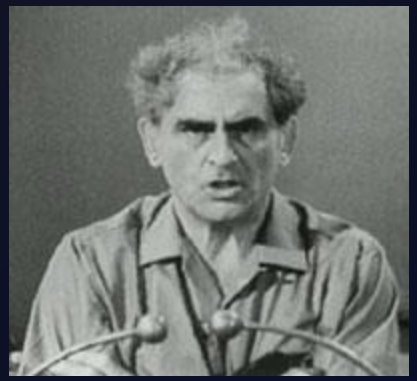
Agenda:

1. Some background and history.
2. Who's who in Australian Federal Government Cyber Policy – 2017
3. Policy frameworks – 2017
4. Real initiatives – real $$ (?)
5. Cyber training, education and research
6. **Cyber business development**
7. What's next?

AUSTRALIA - ACSGN

The global cyber security market is currently worth more than $100 billion and is expected to more than double by 2020.

BUT
WHY IS IT SO ?



Prof Julius Sumner Miller
1959, *"Why Is It So?"*
KNXT Channel 2
Los Angeles.

AUSTRALIA - LIMITATIONS

- Limited local manufacture
- Little control over products
- Services from domestic & international organisations
- Risk – diverse global supply chain
- Guidance for agencies – manage supply chain
- Founding partner – Global Forum on Cyber Expertise – The Hague - 2015

BUT DECO/DSGL/Wassenaar ???

THE WASSENAAR ARRANGEMENT

On Export Controls for Conventional Arms and Dual-Use Goods and Technologies

AUSTRALIA

Defence and Strategic Goods List

made under paragraph 112(2A)(aa) of the

Customs Act 1901

Compilation No. 7

Compilation date: 10 November 2016

Includes amendments up to: F2016L01727

Registered: 15 November 2016

Wassenaar Arrangement
on
Export Controls for Conventional Arms and Dual-Use Goods and Technologies

ICT - DUAL-USE TECHNOLOGY & ARTEFACTS

2001: A Space Odyssey (1968)

https://www.tripwire.com/solutions/industrial-control-systems/ics-for-dummies/?referredby=mailchimp/&utm_source=The+State+of+Security+Newsletter&utm_campaign=0d6001e968-EMAIL_CAMPAIGN_2017_05_08&utm_medium=email&utm_term=0_a2892d69fb-0d6001e968-271313485

tripwire

PRODUCTS SOLUTIC

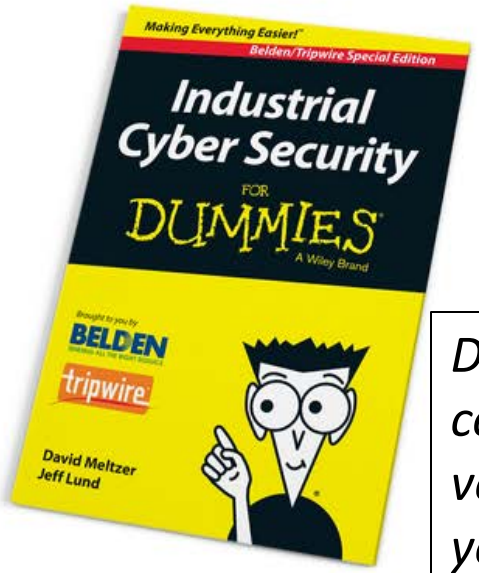
Industrial Cyber Security For Dummies

IT'S SURPRISINGLY GENIUS

Your go-to guide for getting started with industrial cyber security, this Special Belden/Tripwire Edition e-book is packed with security insights specific to industrial control systems and operations environments — you'll have smart answers when "those" questions come up.

LEARN

- IT and OT convergence impact on ICS security
- "Lessons Learned" from real world industrial scenarios
- Use foundational security controls to get 80% security "bang" for your 20% security effort



Thank You

Thank you for your interest in this resource.

Due to the United States export controls, additional verification of the information you submitted is required.We will notify you via email once the verification process is complete.

Due to United States export controls, additional verification of the information you submitted is required. We will notify you via email once the verification process is complete.

May 11, 2017.

Bloomberg – May 4, 2017.

Australian Trade - 2016

Aust – China 117,286.70 #1

Aust – USA 32,652.31 #3

(by $M)

Parameters defining an ICT Dependent "Technology Colony"

- supply chain trust (hardware, software, comms)
  - limited education / training
  - inability to assess chain
  - no alternate supply (?)
- inability to analyse/evaluate products
- inability to assess risk
- total dependence
- ICT *"cargo cult"*

Agenda:

1. Some background and history.
2. Who's who in Australian Federal Government Cyber Policy – 2017
3. Policy frameworks – 2017
4. Real initiatives – real $$ (?)
5. Cyber training, education and research
6. Cyber business development
7. **What's next?**

WHAT'S NEXT?

PROBLEMS:

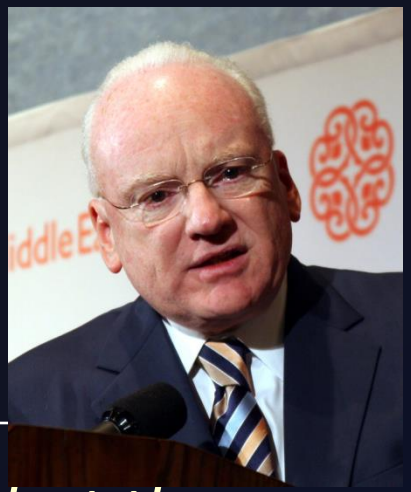
- Responsibility / obligations on suppliers – not just purchasers
  - End-user/application developers capacity ?
    - No application can be any more secure than the hardware facilities/OS/library/sub-systems!
- Independent assessment
  - (Common Criteria – IS15408)
  - Hardening servers - support for CC/OSPP – Labelled / MAC (SELinux)

- Program to "teach the teachers" – PhD programs
- SFS style program to boost supply of professionals ???

A START BUT MUCH MORE NEEDED!

Richard A Clarke - USA

National Coordinator for Security, Infrastructure Protection and Counter-terrorism



".. the conclusion by the Administration is that the nation IS at risk because over the last decade we have made the nation, the economy and national defense dependent upon computer networks. We have designed, ad hoc, a ***national information infrastructure without any thought of including security."***

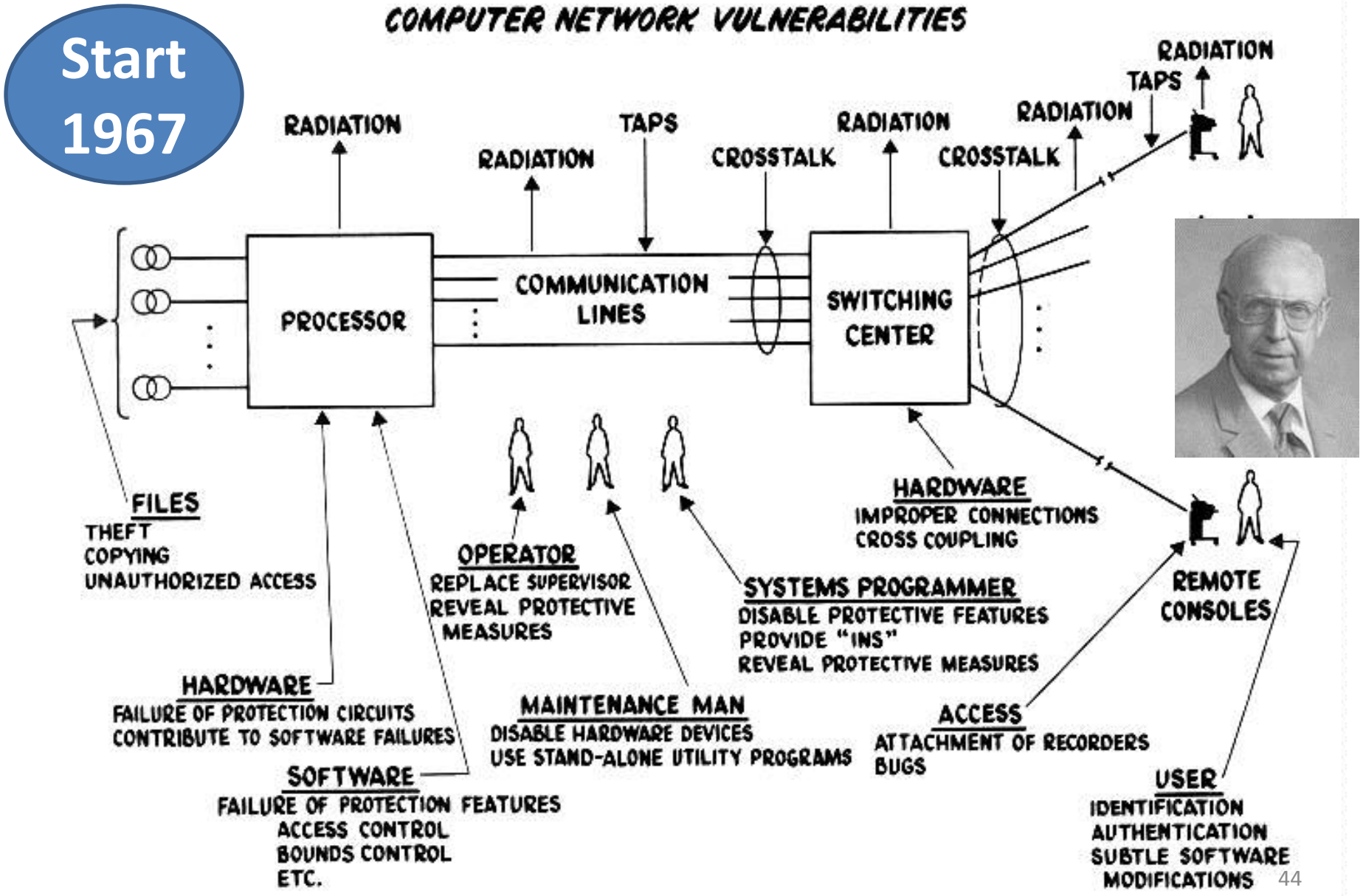
Source: 3rd NCISSE, New York

(Clarke, May 1999)

20th NISSC
October 7-10, 1997

Baltimore Convention Center Baltimore, MD

Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security - RAND Report R-609-1 (Feb 1970, Declassified 10 Oct 1975)



THANK YOU!


Questions & Discussion..
(Courtesy Gay & David Epstein, New Zealand.)