Open Access License Notice

Cybersecurity Education at Formal University Level: An Australian Perspective

William J Caelli
w.caelli@illeac.com

School of Electrical Engineering and Computer Science
Science and Engineering Faculty
Queensland University of Technology, Australia;

Vicky Liu
v.liu@qut.edu.au

School of Information and Communication Technology
Griffith University, Australia

Abstract - Cybersecurity studies at undergraduate / postgraduate level are offered at numerous universities in Australia. The level offered varies from a specifically named undergraduate / postgraduate coursework degree to usual IT or relevant degrees offering cybersecurity as a minor or major theme. A minority of universities do not offer any specific cybersecurity specific course while others offer such courses in association with industry organisations. Based upon an extensive analysis of published course / program data from university websites, chosen as the best data repository that would normally be examined by prospective students, this study submits that in Australia available courses are few and are acknowledged as not meeting market demands for skilled cybersecurity professionals. This has been recently recognised by Australia's Federal Government which has implemented the "Academic Centres of Cyber Security Excellence (ACCSE)" program in its 2016 / 2017 budget to promote the discipline and university support for it. In summary, courses currently available appear quite limited in scope.

Keywords

information security education, cybersecurity education and training, IT education, networking and cybersecurity, cybersecurity courses

1 INTRODUCTION

This study examines the situation in relation to courses of study in cybersecurity offered at the formal university level in Australia at both undergraduate and postgraduate levels. It discusses coursework degree programs only and does not examine postgraduate research programs such as PhD activities, etc. Moreover, Australia, in terms of information and communications technology (ICT), must be regarded as a *"technological colony"* [1] in the sense that it does not have any notable manufacturing capacity in the basic products / artefacts of the sector. This includes microprocessors and allied components, complete computer systems, operating systems, data network components, etc. This emphasizes the growing political and defence policy concerns in relation to cybersecurity education levels in Australia which, in summary, are seen as being inadequate. However, in computer technology terms, it must be noted that Australia built a full computer system, later named "CSIRAC", starting in 1947 which went into full operation in 1949 [2].

Australia does, however, have a notable position and long history in the use of ICT for various application sectors. Tertiary education in the public and private sectors incorporates educational institutions broadly categorised as either universities or *"Technical and Further Education (TAFE)"* institutions although qualifications offered by these two distinct entities now overlap, e.g. a Bachelor's level degree in information technology now available at a TAFE, etc. Until relatively recently, Australia's TAFE sector mainly offered one or two year "Certificate" or "Diploma" programs and associated qualifications.

This study concentrates on the traditional university sector. However, it must be noted that other major education activities in cybersecurity exist in Australia, as

elsewhere, through company specific, e.g. Microsoft, RedHat, CISCO, etc. and dedicated not-for-profit entities such as the SANS Institute, ISACA, ISC^2, etc. offerings. At the same time, some universities offer such industry certified educational programs as an integral part of a tertiary qualification causing difficulty in creating a completely separate set of educational classifications in the cybersecurity area. At the time of this study, early 2017, appropriate courses and their offering institutions are identified and a broad categorisation of an associated offering is made while at the same time acknowledging that government sponsored enhancement to cybersecurity education and training is under active discussion and potential nation-wide implementation. The Australian Computer Society (ACS) normally accredits education programs in the information technology, computer science and related areas, having particular significance for any student wishing to gain work visa or immigration status for Australia through such study at an Australian institution. The paper also addresses the identified cross-disciplinary approaches in cybersecurity education at the accredited tertiary education level in Australia in line with recent Federal Government policy statements in the area. Resulting from the study a number of clear policy questions are identified which need urgent resolution for any new, successful cybersecurity education program to succeed in Australia.

"Massive open on-line courses (MOOCs)" related to most aspects of cybersecurity are widely available in Australia, as elsewhere in the world. However, at the time of this analysis, such cybersecurity courses are offered entirely by overseas entities, including COURSERA, edX, Udacity, Udemy, FutureLearn, and others.

2 CYBERSECURITY EDUCATION / RESEARCH POLICY AT FEDERAL GOVERNMENT LEVEL

Dr. Tobias Feakin, Australia's first *"cyber ambassador"*, [3] has stated that *"The current shortfall in the workforce—and the research and development base which complements it—can only be fixed through investment in sound policy and a long-term education plan that targets high schools and universities to promote careers in the cyber security profession"* [4]

To this end, the Australian Prime Minister announced *"Australia's Cyber Security Strategy: Enabling innovation, growth & prosperity"* in 2016 [5]. The forward to the strategy by the Prime Minister stated as follows:

> *"Most importantly, this Strategy will play a key role in securing Australia in the 21st Century. It also represents a significant investment in cyber security. The Government will invest more than $230 million over four years to enhance Australia's cyber security capability and deliver new initiatives. This complements the significant investment in cyber security outlined in the 2016 Defence White Paper, boosting Defence cyber capabilities by up to $400 million over the next decade."*

That $230 million does not, of course, solely relate to cybersecurity education and training but to overall programs in the area. In addition, in 2015 Australia became a founding partner in the *"Global Forum on Cyber Expertise"* (GFCE) [6] at the *"Global Conference on CyberSpace"* held in The Hague, The Netherlands. This "forum" has the stated policy for its GFCE members and partners to *"develop joint initiatives to strengthen cybersecurity, fight cybercrime, protect online data and support e-governance."* The implication of needs to advance education and training is obvious but is not explicitly stated. However, the statement that *"outcomes of initiatives are practical achievements on cyber capacity building and best practices which are shared with and can be multiplied by other GFCE members"* clearly indicates support in the education and training arena. Australia's participation in this broad program was alluded to in a paper published in the 2nd edition of the GFCE journal via the following statement [7] indicating an intention to build *"A cyber smart nation: improve cyber security awareness, address skills shortages and develop a highly-skilled cyber security workforce."* The 56 members of GFCE include both Australia and the USA as well as a number of private sector corporate entities.

At the same time the Australian Government announced in late 2016 the formation of the *"Australian Cyber Security Growth Network (ACSGN)"* as an *"industry-led and not-for-profit company responsible for delivering the activities of the Cyber Security Growth Centre initiative"* [8]. This is further explained as follows; *"The ACSGN will have a national footprint and will work closely with Australia's cyber security*

sector to take advantage of this growing global market for cyber security products and services. It will operate out of several nodes established across Australia, which will provide a way of connecting the many fragmented cyber security activities and bridge capability and expertise across the country." [9]

This initiative, however, is not solely aimed at education and training but rather industry development.

An emphasis is also being placed on *"developing leaders in cybersecurity"* with an injection of $22 million (Aust) over time from 2016. At early 2017 the exact implication and implementation of this in relation to the funding and further creation of education and training initiatives and in relation to the ACSGN are not known.

However, a separate plan entitled the *"Academic Centres of Cyber Security Excellence (ACCSE)"* is seen to be part of the earlier $230 million *"Cyber Security Strategy"* as announced by Australia's Prime Minister in April 2016. Interestingly, that announcement made out that *"it is expected that ACCSE will be self-sustaining with ongoing operations funded through student course fees and fee-for-service income, including from Australian Government agencies and other external sources."* While in some ways similar to the USA's *"National Centers of Academic Excellence in Cyber Defense (CAE-CD)"* [10] program there appears to be no equivalent to the USA's *"Scholarship-for-Service"* initiative to encourage young people to take up such courses and enter the cybersecurity profession. Similarly, the USA program does not offer any specific financial backing to individual academic institutions participating in the scheme. However, the USA's program does apparently incorporate the overall formal educational ambitions of the Australian program as follows [10]:

> *The CAE-CD program comprises the following designations: Four-Year Baccalaureate / Graduate Education (CAE-CDE), Two-Year Education (CAE2Y) and Research (CAE-R). All regionally accredited two-year, four-year and graduate level institutions in the United States are eligible to apply.*

Financial support in Australia appears very limited as follows; *"the Government has committed $1.9 million over four years (2016-2017 to 2019-2020) for the establishment of ACCSE in Australian universities to address the nation's critical shortage of skilled cyber security professionals."* [8].

In many ways these new Australian programs appears aimed at what may loosely be categorised as engineering / technology / computer science professionals or "IT geeks". However, Australia has had a strong postgraduate position in relation to defence / security policy research for many years particularly at the Australian National University (ANU) and at a number of "think tanks" such as the *"Australian Strategic Policy Institute (ASPI)"* which was established with government support in 2001 [11].

3 RELEVANT CYBERSECURITY EDUCATION / TRAINING POLICIES AT INDIVIDUAL STATE LEVEL

While each State of Australia normally has some form of policy setting in relation to cybersecurity relevant to its own information systems and data networks, these do not appear to address the education and training requirements for appropriate cybersecurity professionals. For example, the State of Queensland has announced the establishment of a *"Cyber Security Unit"* to be funded for around $12.5 million (Aust) and which will be associated with the office of the State Government's Chief Information Officer. However, no indication is given of how required cybersecurity professionals will be educated, trained and retained. [12] Other States of Australia have similar cybersecurity statements or policies / regulatory settings but, in terms of education and training, most emphasis appears to be on general awareness education for the public at large and for children and schools in particular. At the State level, TAFE is essentially a State administered and funded activity and individual TAFEs offer a Bachelor's degree in matters related to cybersecurity, e.g. Bachelor of Information Technology (Network Security) at TAFE New South Wales [13]. However, TAFE education in this area appears new and is not analysed in this paper. TAFE, in many ways, is an analogy of the *"Community College"* activity in the USA with that emphasis on 2 year duration programs.

At the same time, and as a notable exception, the State of Victoria has announced the formation of the *"Oceania Cyber Security Centre (OCSC)"* as a collaboration by Victoria's 8 universities with substantial State level funding [14]. It has the stated ambition of *"engaging with industry to develop research and training opportunities for dealing with cyber security issues."* At the time of this survey senior management appointments have been made but any education/training programs have yet to be detailed.

4 CATEGORIES OF CYBERSECURITY EDUCATION AND TRAINING IN AUSTRALIA

According to Wikipedia [18] there are 43 universities across Australia including 2 international universities and 1 private university, although Universities Australia [15], the main representative body only lists 39 of these as members of that body. This study examines 40 of these. The appropriate website of the Australian Federal Government [16] also lists 43 universities and refers to the appropriate quality assurance agency, namely the *"Tertiary Education Quality and Standards Agency (TEQSA)"* as *"Australia's independent national regulator of the higher education sector"* [17]. The Australian Commonwealth *"Higher Education Support Act 2003 sets out three groups of Australian higher education providers: universities, other self-accrediting higher education institutions, and state and territory accredited higher education institutions."* [19] This adds to the complexity in developing a categorisation scheme for cybersecurity education at tertiary level. However, as mentioned above, the TAFE system in Australia which up until some years ago only offered so-called "certificate" and "diploma" level courses of two or fewer years duration, moved "up-market" and has started to offer full "bachelor" and "associate bachelor" degree qualifications. These institutions are not categorised as research entities and do not offer postgraduate research degrees such as Ph.D., etc.

The *"Core Body of Knowledge (CBOK)"* of the Australian Computer Society [23] does set out specific requirements for cybersecurity expertise in most of the generic areas of ICT knowledge and also dedicates a complete section, with 5 sub-sections, to "cybersecurity management". These requirements are then mapped against the

learning outcomes stated in the *"Skills Framework for the Information Age (SFIA)"* [24] published by the SFIA Foundation.

5 CYBERSECURITY EDUCATION IN FORMALLY ACCREDITED UNIVERSITY INSTITUTIONS.

5.1 Placement of Cybersecurity Courses.

The following terms are used below and in this paper, as follows:

- **"unit"**- a designated study option normally based around approximately 40 hours of class or equivalent contact with the educational institution, although this term is not used universally across Australia;
- **"course"** - a grouping of study "units" to enable a qualification to be achieved, which may or may not be designated as a specific "cybersecurity" degree;
- **"major"** - a course of study that usually has at least 4 units of study related to cybersecurity and the final qualification contains an indication of this;
- **"minor"** - a course of study that usually has at least 2 units of study in cybersecurity, but may vary from 1 to 3 such units, but the final qualification does not separately designate the area.

In this regard, cybersecurity related courses have been placed under various broad discipline categories for Australian universities, as follows:

- **Science** degree (e.g. Bachelor of Science, Master of Science)
- **IT** degree (e.g. BIT, MIT, BICT, MICT, MITM) with bracketed designation following specifying a specialization / major in Networking and Security, Network and Cybersecurity, or Network Security, etc.
- **Engineering** degree specialising in or having a major in Computer Security
- **Cybersecurity** degree
  Some universities have a strong emphasis on cybersecurity studies, so that they have clearly designated and identified "Cybersecurity" qualifications, as listed in Table 1.

University of New South Wales (UNSW) (including Australian Defence Force Academy - ADFA)	Bachelor of Computing and Cyber Security Master of Cyber Security Master of Cyber Security (Advanced Tradecraft) Master of Cyber Security (Digital Forensics) Master of Cyber Security Operations Master of Cyber Security, Strategy and Diplomacy
Charles Sturt University (CSU)	Master of Information Systems Security
Deakin University (DEAK)	Bachelor of Cyber Security Master of Cyber Security
Latrobe University (LATR)	Master of Cybersecurity (computer Science) Master of Cybersecurity (Business Operations) Master of Cybersecurity (Law)
Monash University (MONA)	Master of Networks and Security
University of South Australia (USA)	Master of Cybersecurity
Edith Cowen University (ECU)	Master of Cyber Security

Table 1: Cybersecurity degree offered at Australian Universities

Some other universities have cybersecurity study units in both major and minor unit groupings in the appropriate available ICT course but not designate a specific

degree title for "cybersecurity". However, four universities apparently have no information technology specific course of study identified at all, i.e. Bond University, Australian Catholic University (ACU), University of Notre Dame Australia (UNDA), and Torrens University while four others have an IT course designated but no identifiable cybersecurity units of study, viz. Southern Cross University (SCU), University of Newcastle, Charles Darwin University (CDU) and University of Adelaide. This would indicate that potentially 20% of Australian universities have no specific involvement in cybersecurity education.

This situation is outlined in Table 2:

Cybersecurity specific degree	UNSW, CSU, DEAK, MONA, LATR, USA, ECU	7
Cybersecurity as a major|minor|specialisation	QUT, CQU, GRIF, JCU, USQ, MACQ, UOW, RMIT, SWIN, FEDU, UCAN, FLIN, CURT, MURD	14
No formal cybersecurity, has a major|minor with 1-3 cybersecurity units	UQ, USC, UNE, USYD, UTS, UWS, UM, VU, ANU, UTAS, UWA	11
IT courses, but no cybersecurity related units	SCU, UNEW, CDU, UA	4
Neither IT nor cybersecurity related units	BOND, ACU, TU, UND	4
Total		40

Table 2: Cybersecurity Education at Australian Universities

Australian Catholic University	ACU
Australian National University	ANU
Bond University	BOND
Central Queensland University	CQU
Charles Darwin University	CDU
Charles Sturt University	CSU
Curtin University of Technology	CURT
Deakin University	DEAK
Edith Cowen University	ECU
Federation University	FEDU
Flinders University	FLIN
Griffith University	GRIF
James Cook University	JCU
La Trobe University	LATR
Macquarie University	MAC
Monash University	MONA
Murdoch University	MURD
Queensland University of Technology	QUT

RMIT University	RMIT
Southern Cross University	SCU
Swinburne University of Technology	SWIN
Torrens University	TU
University of Adelaide	UA
University of Canberra	CAN
University of Melbourne	UM
University of New England	UNE
University of New South Wales	UNSW
University of Newcastle	NEWC
University of Notre Dame	UND
University of Queensland	UQ
University of South Australia	USA
University of Southern Queensland	USQ
University of Sydney	US
University of Tasmania	UTAS
University of Technology Sydney	UTS
University of the Sunshine Coast	USC
University of Western Australia	UWA

University of Western Sydney	UWS
University of Wollongong	UOW
Victoria University	VU

Table 3: Abbreviations for Australian universities

5.2 Notes on Designation of Major / Minor Study

Table 1 indicates the levels of cybersecurity education offered at Australian universities but it should be noted that the designation of a so-called "major" or "minor" area of study within the overall qualification varies markedly across the sector, e.g. Griffith and James Cook (JCU) universities have "networks / security" majors but these only involve 1 specific cybersecurity unit, Curtin University requires a designated "major" to have 5 units, Queensland University of Technology (QUT) specifies a "minor" as 4 units, The University of Queensland (UQ) has 2 cybersecurity units but no designated cybersecurity major or minor.

Security related units of study may only partially cover the designated topic and overall there does not appear to be an overall holistic approach particularly where from 1 to 3 study units only are offered.

5.3 Specialised Cybersecurity Education and Research Centres

One of the earliest specialised cybersecurity education and research centres at university level anywhere in the world, the *"Information Security Research Centre (ISRC)"*, was established in early 1988 at the then Queensland Institute of Technology (QIT), later to become the Queensland University of Technology (QUT) with an author of this paper as its founding director (Caelli). It was later merged into the QUT's *"Information Security Institute (ISI)"* but this was later disbanded around 2007. For example, ISRC predates the COAST lab at Purdue

University by a few years as well as the Information Security Group (ISG) at Royal Holloway, University of London, formed in 1990.

The University of New South Wales (UNSW) at the Australian Defence Force Academy (ADFA) in Canberra, Australia houses the *"Australian Centre for Cyber Security (ACCS)"*, [21] a large group dedicated to education and research in all aspects of cybersecurity including the social / policy realms.

6 COURSE CONTENT

Overall a cursory analysis of course / unit content indicates strong emphasis on "network security" while areas such as "trusted systems", "secure application software development", "software testing and evaluation", "penetration detection and testing", etc. have minimal to no coverage. In particular, the history of the discipline over the last 50 years or so does not appear to be covered in any course. In addition, mathematics units related to cryptography may be included in the minor / major count. Unquestionably, with the scope of cybersecurity studies in the specifically identified cybersecurity degrees can cover much more material in depth. However, this study has highlighted the need for a more holistic approach and identified a number of missing / under-treated areas which need to be addressed as;

- "vertical" vs." horizontal" subject areas, e.g. healthcare requirements, etc. including appropriate national and international standards;
- an understanding of the history of the subject, its present status and likely future trends, e.g. the IS 7498-2 security standard for the OSI model networks, USA "Orange Book" / UK ITSEC, etc.;
- contemporary computing security requirements, including Internet-of-Things (IoT), cloud systems and security of virtualization / container technologies;
- a layered, "security architecture" analysis and development approach from hardware to operating systems to network stacks to middleware to applications, etc. and

- trusted / "trustworthy" computer systems and their evaluation, e.g. the "Common Criteria", etc.
- national and international legal / regulatory arrangements in cybersecurity / cyber conflict, response to attacks / penetration, etc.

Interestingly, for the Australian situation, application software security and its testing / verification are not commonly covered. However, Monash University does offer a "software security" unit of study discussing cybersecurity from the design stage, through to implementation, testing and deployment. The University of Tasmania (UTAS) also offers a security in web programming unit. It has to be noted that these are individual situations and illustrate the problem of uniformity across the university sector.

Often cybersecurity majors or minors seem to actually go hand-in-hand with networking (internetworking) programs. However, this is not obviously insufficient to learn the discipline of cybersecurity across a full information system operated by the public or private sectors. The student obviously must understand the functions / purposes / behaviours of network protocols to understand network system vulnerabilities and then be able to address cybersecurity threats as these impact on both clients and servers on any network. However, at the "computer security" level, the security of the network elements themselves, essentially specifically dedicated computer systems, as well as both clients and server systems is equally important but appears to be downplayed in Australian courses.

7 CONCLUSION

The president of the Australian Computer Society (ACS), Anthony Wong, has stated that *"Australia will need an estimated 100,000 more ICT specialists by 2020 but a mere 4000 IT graduates are produced at tertiary level each year."* [20] Against this background, however, there is also a cautionary note sounded by the Australian Computer Society (ACS) in its 2016 report entitled "Cybersecurity: Threats, Challenges, Opportunities". This report states [22]:

"… The demand for skilled ICT workers will increase from 638K today to 695K by 2020 with ICT university graduates meeting only 1% of this demand. Additionally, there has been a 35% drop in enrolment rates for ICT subjects at universities since 2001."

It goes on to emphasize that at present *"the skills and knowledge required to be a cybersecurity professional doesn't demand the same esteem"* as that enjoyed by lawyers and doctors for example. The report advocates the establishment of *"Academic Centres of Cyber Security Excellence"* [25] and this appears to have gained Federal Government attention but with limited funding compared to overseas experience, e.g. in the USA. Moreover, Australia is dependent upon a reliable and trusted supply chain for information and communications technology products and systems. Such trust needs to be at least tested and even possibly verified requiring suitably qualified and experienced cybersecurity professionals. However, cybersecurity education at the formal university level is very limited in many ways as well as being also geographically disbursed across the nation. It is also placed in different disciplines according to widely different university / faculty and business policies.

Cooperation with industry certification schemes in cybersecurity can be seen in only a very few universities at a time when such certification has attained strong business / industry acceptance. However, traditional universities have major problems in in attracting and maintaining sufficient expert academic staff with appropriate education, experience and research interests in cybersecurity.

There appears to be little change likely in the overall stance of cybersecurity education at formal university level in Australia without more notable government incentives and funding, including such schemes as the USA's "Scholarships for Services" program. Indeed, efforts over the last 2 to 3 years to create a relevant, Federal Government funded cybersecurity "cooperative research centre" across a number of universities has not been successful, reportedly due to lack of funding support from the private sector to augment public sector funding. There is, however, some tentative indication that this could change in the 2017 to 2020 Australian financial years.

REFERENCES

[1] Janczewski, L and Caelli, W.; *"Cyber Conflict and Small States"*, 2015

[2] *"CSIRAC: Australia's First Computer"*, URL https://museumvictoria.com.au/csirac/

[3] Australian Ambassador for Cyber Affairs, Dr Tobias Feakin; URL http://dfat.gov.au/about-us/our-people/homs/Pages/ambassador-for-cyber-affairs.aspx

[4] Feakin, T; in URL https://cybersecuritystrategy.dpmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf

[5] Commonwealth of Australia, Department of the Prime Minister and Cabinet, *Australia's Cyber Security Strategy*, 2016 URL https://cybersecuritystrategy.dpmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf, ISBN 978-1-925238-62-4 Australia's Cyber Security Strategy (PDF).

[6] Global Forum on Cyber Expertise, URL https://www.thegfce.com/

[7] *Advancing and protecting Australia's interests online*, Office of the Cyber Security Special Adviser, Australia, Second issue of the Global Cyber Expertise Magazine - November 2016, URL https://www.thegfce.com/news/news/2016/12/07/advancing-and-protecting-australias-interests-online.

[8] *"Cyber Security Growth Centre"*, URL http://www.innovation.gov.au/page/cyber-security-growth-centre

[9] *"Cyber Security Growth Centre"*, Centres, URL https://industry.gov.au/industry/Industry-Growth-Centres/Pages/Cyber-Security-Growth-Centre.aspx

[10] *"National Centers of Academic Excellence in Cyber Defense"*, USA URL https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/

[11] *"Australian Strategic Policy Institute (ASPI)"*; URL https://www.aspi.org.au/about-aspi

[12] Pearce, R.; *"Queensland to establish Cyber Security Unit: Team to sit inside Queensland Government Chief Information Office."*, Computerworld (Aust), 17 Feb 2016, URL http://www.computerworld.com.au/article/594102/queensland-establish-cyber-security-unit/

[13] Tertiary Education in Australia, URL https://en.wikipedia.org/wiki/Tertiary_education_in_Australia

[14] *"Oceania Cyber Security Centre (OCSC)"*, URL http://oceaniacybersecuritycentre.businesscatalyst.com/

[15] Universities Australia, URL https://www.universitiesaustralia.edu.au/australias-universities/university-profiles

[16] List of Australian Universities, URL http://www.studyinaustralia.gov.au/global/australian-education/universities-and-higher-education/list-of-australian-universities

[17] Tertiary Education Quality and Standards Agency (TEQSA), URL http://www.teqsa.gov.au/

[18] List of universities in Australia, URL https://en.wikipedia.org/wiki/List_of_universities_in_Australia

[19] TAFE-NSW Bachelor of Information Technology (Network Security), URL https://www.tafensw.edu.au/courses/tafe-nsw-degrees/choose-a-degree/bachelor-of-information-technology-network-security

[20] *"Australian Computer Society calls on government to improve gender diversity in tech"*, URL http://www.startupsmart.com.au/news-analysis/acs-calls-on-goverment-to-improve-gender-diversity-in-tech/

[21] *"Australian Centre for Cyber Security (ACCS)"*, URL https://www.unsw.adfa.edu.au/australian-centre-for-cyber-security/

[22] *"ACS Cybersecurity - Threats, Challenges, Opportunities"*; Nov. 2016, URL https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Cybersecurity_Guide.pdf

[23] *"The-ACS-Core-Body-of-Knowledge-for-ICT-Professionals (CBOK)"*, Mar 2017, URL https://more.acs.org.au/__data/assets/pdf_file/0013/24502/The-ACS-Core-Body-of-Knowledge-for-ICT-Professionals-CBOK.pdf

[24] *"SFIA 6: The Complete Reference Guide"*, SFIA Foundation, Mar 2017, URL https://www.sfia-online.org/en/sfia-6

[25] A*cademic Centres of Cyber Security Excellence (ACCSE)*, Australian Government Department of Education and Training, 11 April 2017, URL https://www.education.gov.au/academic-centres-cyber-security-excellence-accse