Developing Postgraduate Cyber Security Programs at the Australian Centre for Cyber Security at the University of New South Wales Canberra at ADFA

Elena Sitnikova
e.sitnikova@adfa.edu.au

University of New South Wales Canberra
Australian Defence Academy
PO Box 7916 Canberra BC ACT 2610

Abstract - In the modern world of exponentially increasing threats from advanced technologies, many institutions recognise the need for establishing cyber security programs to meet the growing demand for cyber security professionals in industry, government and defence organisations. However, cyber security, cyber defence and cyber war education is still ill represented in Australia. Some directions to overcome the problem is given by the Australian Government (Australia's Cyber Security Strategy) [1] but not yet fully developed. To address this issue, the Australian Centre for Cyber Security (ACCS) at the University of New South Wales (UNSW) Canberra at ADFA has been developing a suite of three postgraduate cyber security programs for the steadily increasing numbers of students from diverse backgrounds interested in studying cyber security and acquiring cyber warfare skills. The Centre is the only one in the world that offers a university degree specialising in cyber war and peace. This paper will describe the structured approach of developing the programs, highlight challenges by providing observations and lessons learned over the past two years, and propose some future directions on how to overcome these challenges.

General Terms

Cyber Security

Keywords

Education, cyber warfare, cross-disciplinary education, postgraduate curriculum

1 INTRODUCTION

The rapidly increasing demand for cyber security professionals in industry, government and defence organisations is pressuring education institutions to develop cyber security programs. In our modern world, cyber security is constantly a hot topic and its popularity is rising among potential students who wish to pursue careers in the field. Traditionally, tertiary cyber security programs attract students from STEM professions who already hold expertise in technical areas such as IT, science, engineering and mathematics.

However, according to Gupta and Buthmann (2007) the Bell Labs Concept of "cyber security" is a broader term consisting of eight vectors of attack and response, and has to address political, social, legal, technical and personnel issues (cited in [2]). This concept creates opportunity to be educated in cyber defence and cyber warfare for students with non-STEM backgrounds (art, business and social sciences) and also students from the Australian Defence Force who do not have tertiary education but possess many years of experience in management roles. These expanded opportunities also help to increase the size and diversity of the skilled security-aware workforce.

Despite the directions given by the Australian Government in its 2016 Defence White Paper [3] and Australia's Cyber Security Strategy [1] on "creating a cyber-smart nation … and fostering skills throughout the education system," cyber security, cyber defence and cyber war education is still ill represented in Australia.

The Australian Centre for Cyber Security (ACCS) at the University of New South Wales (UNSW) Canberra at ADFA has published several papers explaining the needs for cyber security education and its impact on social management and government functions [2][4][5]. "A country's military capability and strategic planning cannot escape the general trend of development in its economy and human resources... The low penetration rate of IT professionals in all echelons of military and strategic planning, a symptom of our desultory outcomes in information technology education, produces defence policy that looks strangely out of step with the emerging digital realities [6]."

To meet the demand from the constantly rising number of students from diverse backgrounds interested in studying cyber security and acquiring the skills to become cyber warfare professionals, a suite of three postgraduate cyber security programs have been gradually developed by the ACCS since 2015. Today the ACCS is the only centre that holds the world's first university degree specialising in cyber war and peace. It provides education and training at a variety of levels, including undergraduate and graduate coursework programs, Research Masters, PhD and Professional Doctorate; it also provides professional short courses with customised versions to fulfil demands from different industry and government organisations. This paper, due to the limitation of space, will only focus on the suite of graduate coursework programs, but will show the pathways to further study at PhD and Professional Doctorate levels.

The paper is organised as follows: Section II introduces readers to the graduate Cyber security programs at ACCS; Section III describes the essential components and specific requirements for the programs; Section IV provides observations and lessons learned; and Section V provides a summary of the current status and suggests future directions.

2 THE AUSTRALIAN CENTRE FOR CYBER SECURITY AND ITS CYBER SECURITY PROGRAMS

The UNSW in Canberra is the awarding body for ADFA's tertiary qualifications. It provides education and research for the Australian Defence Force in Royal Australian Navy (RAN), Australian Army and Australian Air Force (RAAF) and is located at the ADFA grounds in Canberra, the capital of Australia. In addition to educating future leaders of Australian Defence Force, UNSW Canberra is also open to civilian students and provides postgraduate programs and short courses to Department of Defence personnel and the general public [7]. UNSW Canberra offers undergraduate courses to both officer cadets and civilian students leading them to the University Bachelor degrees of Arts, Business, Science, Engineering, and Information Technology. The university also provides opportunities for graduate study and research leading to Master degrees, diplomas and certificates. A variety of postgraduate coursework programs are offered by four different schools in the Humanities and Social Sciences, Environmental and Mathematical Sciences, Business, Engineering and IT faculties, ranging from Arts (history and politics) to Business (governance and strategy) and Engineering (space engineering, capability management and cyber security).

In mid-2014, UNSW Canberra recognised the importance of cyber security research and education by creating the ACCS at ADFA. Since then, ACCS pursues its mission to participate in the development of new paradigms for multi-disciplinary research in the field, to conduct collaborative research projects on selected high priority themes, and to educate and mentor the next generation of Australian leaders in cyber security. The Centre currently has seven full-time academics plus additional 55 staff academics across UNSW in Sydney and Canberra, providing the largest concentration of research and tertiary education for the multi-disciplinary study of cyber security in any single university in the Southern Hemisphere. A number of ACCS academics are part of a team undertaking pioneering research and education on areas are ranging from information technology and engineering to law and politics, and have significant international

reputations for their work. ACCS serves as a national hub for policy related research and education across the full spectrum of cyber security, undertaking research in the following eight priorities:

- Cyber-enabled war, Australian Defence Forces strategies and capability;
- Assessing mission-critical aspects of cyber-attack and defence;
- Cyber Intrusions, detection and forensics;
- Cyber education and skilling, especially for security agencies;
- Human aspects of cyber security and privacy
- Cyber dependency and resilience of critical national infrastructure;
- International thereat environment, diplomatic responses and national security policy;
- Ethics in cyberspace.

Since mid-2014 the ACCS offers an Undergraduate Bachelor in Computing and Cyber Security; three Masters programs: Masters in Cyber Security (8628), Cyber Security Operations (8629) and Cyber Security Strategy and Diplomacy (8631); and more than dozen of professional education short courses. The Centre also provides undergraduate courses to all year 2 and 3 cadets from all four schools at ADFA.

The section below describes ACCS's Masters programs and explains a pathway option through the Masters coursework and Research Project to the Doctor of Cyber Security degree (DSybSec).

3 MASTERS OF CYBER SECURITY PROGRAMS DEVELOPMENT AND STRUCTURE

ACCS offers the most comprehensive range of Master level degrees in Australia. In 2015 the first two coursework Master programs - Cyber Security (8628) and Cyber Security Operations (8629) were offered within the School of Engineering and Information Technology (SEIT). The Cyber Security program also has a specialised stream in Digital Forensics. In 2016 the third program, Cyber Security

Strategy and Diplomacy (8631), was introduced within the School of Humanities and Social Sciences (HASS) to attract students from non-STEM disciplines. The most recent addition in 2017 included a second stream under the general cyber security program: Advanced Tradescraft. The structure of the programs has been evolved over these two years, with some of the original courses being replaced and new courses added. The current offerings are shown in Table 1.

Students undertaking the Master level programs are required to complete eight coursework courses (48 UOC) including core courses and electives (see Table 1). The courses have two delivery modes: Distance (online) Mode and Intensive Delivery Mode (IDM). The Master of Cyber Security courses are offered primarily via IDM due to the nature of the courses and the use of a specially equipped laboratory, the Cyber Range, for hands-on exercises.

Masters students who obtain a high credit average (WAM >= 75) in four courses have the option to undertake a research project worth 12 UOC (ZEIT8297 Project Report), subject to approval of the Postgraduate Coordinator. The project is recommended for those with a strong interest in pursuing original research in a particular area or intending to undertake a higher research qualification. Students undertaking the project are unable to enrol in courses from other coursework programs.

There is a pathway option for Doctor of Cyber Security (DCybSec). The DCybSec provides an opportunity to combine a doctoral thesis with the coursework component of all of our three Masters programs described in this section. The degree consists of one-third coursework (equivalent to two-year full-time study) which may be in any area encountered by student while undertaking coursework. This program is intended to prepare candidates for the highest professional practice, in which they can contribute significantly to the development of the multi-disciplinary study of cyber security.

Postgraduate Coursework Program	Core Courses (6 UOC each)	Elective Courses (6 UOC each)
Masters of Cyber Security (8628)	▪ ZEIT8020 Computer Network Operations ▪ ZEIT8021 Information Assurance ▪ ZEIT8023 Wireless, Mobile and IoT Security ▪ ZEIT8026 Network Security Operations	▪ ZEIT8024 Software Security Lifecycle ▪ ZEIT8025 Reverse Engineering Malware ▪ ZEIT8027 Critical Infrastructure and Control Sys Security ▪ ZEIT8028 Digital Forensics ▪ ZEIT8029 Network and Memory Forensics ▪ ZEIT8030 Big Data and Decision Analytics for Security ▪ ZEIT8036 Humans and Security ▪ ZEIT8042 Modern Exploit Development

Postgraduate Coursework Program	Core Courses (6 UOC each)	Elective Courses (6 UOC each)
Masters of Cyber Security (8628) – Forensics	▪ ZEIT8020 Computer Network Operations ▪ ZEIT8021 Information Assurance ▪ ZEIT8022 Identity and Access Management ▪ ZEIT8025 Reverse Engineering Malware ▪ ZEIT8028 Digital Forensics ▪ ZEIT8029 Network and Memory Forensics	▪ ZEIT8023 Wireles, Mobile and IoT Security ▪ ZEIT8024 Software Security Lifecycle ▪ ZEIT8026 Network Security Operations ▪ ZEIT8027 Critical Infrastructure and Control Sys Security ▪ ZEIT8030 Big Data and Decision Analytics for Security ▪ ZEIT8042 Modern Exploit Development

Postgraduate Coursework Program	Core Courses (6 UOC each)	Elective Courses (6 UOC each)
Masters of Cyber Security (8628) – Advanced Tradescraft	▪ ZEIT8020 Computer Network Operations ▪ ZEIT8021 Information Assurance ▪ ZEIT8023 Wireless Security IoT ▪ ZEIT8025 Reverse Engineering Malware ▪ ZEIT8026 Network Security Operations ▪ ZEIT8030 Big Data and Decision Analytics for Security ▪ ZEIT8042 Modern Exploit Development	▪ ZEIT8027 Critical Infrastructure and Control Sys Security ▪ ZEIT8028 Digital Forensics ▪ ZEIT8029 Network and Memory Forensics

Postgraduate Coursework Program	Core Courses (6 UOC each)	Elective Courses (6 UOC each)
Masters of Cyber Security Operations (8629)	▪ ZEIT8017 Cyber Crime and Cyber Security ▪ ZEIT8018 CyberDefence, Governance and Acquisition ▪ ZEIT8032 Information Assurance Principles ▪ ZEIT8037 Cyber Security Risk Management	▪ ZEIT8015 Cyber Operations ▪ ZEIT8019 Intrusion Analysis & Response ▪ ZEIT8033 Critical Infrastructure Sec Policy & Governance ▪ ZEIT8035 Cyber Terrorism ▪ ZEIT 8043 Cyber and the Law ▪ ZEIT8115 Information Operations ▪ ZEIT8303 Project Management Body of Knowledge ▪ ZHSS8441 Cyber-Security

Postgraduate Coursework Program	Core Courses (6 UOC each)	Elective Courses (6 UOC each)
Masters of Cyber Security, Strategy and Diplomacy (8631) ⋆	▪ ZEIT8032 Information Assurance Principles ▪ ZHSS8441 Cyber-Security ▪ ZHSS8455 Australian Cyber Diplomacy ▪ ZHSS8457 Cyber Security in Asia	▪ Strategy and Politics ▪ ZHSS8125 Strategic Communication ▪ ZHSS8221 Development of the Art of War ▪ ZHSS8403 Global Security ▪ ZHSS8404 Leg & Mor Prob of Int Violence ▪ ZHSS8407 Global Governance ▪ ZHSS8409 Asia-Pacific Security ▪ ZHSS8410 Australian Defence Policy ▪ ZHSS8430 China's Security Policy ▪ ZHSS8431 Comparative Defence Planning

Postgraduate Coursework Program	Core Courses (6 UOC each)	Elective Courses (6 UOC each)
		▪ ZHSS8435 Contemporary Strategy ▪ ZHSS8438 The Justice of War ▪ ZHSS8439 Reforming Repressive Regimes ▪ ZHSS8440 Delinquent Organisations ▪ ZHSS8442 Conflict Transformation ▪ ZHSS8456 Australian Cyber Forces ▪ ZHSS8458 Cyber Policy in China ▪ Technology and Security ▪ ZEIT8015 Cyber Operations ▪ ZEIT8017 Cyber Crime and Cyber Security

Postgraduate Coursework Program	Core Courses (6 UOC each)	Elective Courses (6 UOC each)
		▪ ZEIT8018CyberDefence, Governance and Acquisition ▪ ZEIT8019 Intrusion Analysis & Response ▪ ZEIT8020 Computer Network Operations ▪ ZEIT8024 Software Security Lifecycle ▪ ZEIT8025 Reverse Engineering Malware ▪ ZEIT8026 Network Security Operations ▪ ZEIT8028 Computer Forensics ▪ ZEIT8029 Network and Memory Forensics ▪ ZEIT8033 Critical Infrastructure Sec Policy & Governance

Postgraduate Coursework Program	Core Courses (6 UOC each)	Elective Courses (6 UOC each)
		▪ ZEIT 8043 Cyber and the Law ▪ ZEIT8115 Information Operations
⋆ For Cyber Security Strategy and Diplomacy (8631) Students should complete all core courses and no more than two electives or 12 UOC from each of the following two lists: 1) Strategy and Politics; and 2) Technology and Security		

Table 1: The suite of Masters in Cyber Security Programs at ACCS, UNSW Canberra at ADFA

The total number of part-time students within the first two Cyber Security (8628) and Cyber Security Operations (8629) programs has grown from 60 students in 2015 to 102 students in 2016 and 225 students in 2017 (Fig.1). Enrolment to the third program, Cyber Security Strategy and Diplomacy (8631), introduced in 2016 has increased from 23 students to 55, with a current 2017 total of 280 ACCS students, representing a 125% increase.

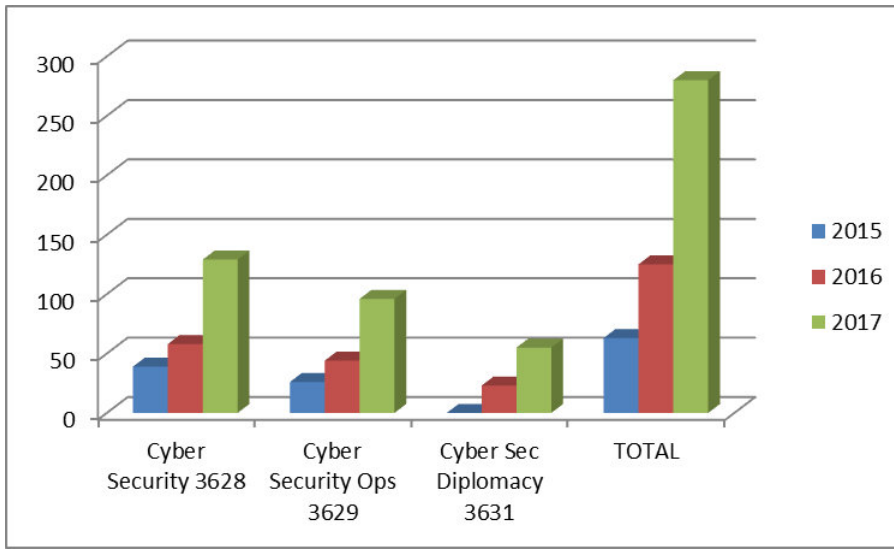

Figure 1: Number of students at ACCS's Master programs

The Master of Cyber Security (8628) is designed for postgraduate scholars and professional managers with appropriate undergraduate qualifications in STEM disciplines: IT, computer science, electrical computer or systems engineering, or a related discipline and / or extensive relevant professional experience who wish to gain a more detailed understanding of the technical skills and expertise relevant to the technical implementation and leadership of the cyber security in a range of social management and government functions. This Masters coursework degree is designed to meet the demand for technical experts who can implement and lead

the technical cyber security function in government, industry, law enforcement, and defence. It provides principles gathered from information systems, systems engineering, computer science, network security, and defence to enhance a career as a cyber security specialist [8]. This program also offers additional streams allowing awards in the Master of Cyber Security with specialisations in Digital Forensics and Advanced Tradescraft.

Stream 1: The Master of Cyber Security in Digital Forensics (ZEITDS8628) is designed for postgraduate scholars with appropriate undergraduate qualifications in a relevant discipline and / or extensive professional experience who wish to develop a high level understanding of the principles and practices of Digital Forensics and to strengthen their skills in this area. Students must complete 6 compulsory courses which provide the underpinning professional knowledge in Digital Forensics and two general electives from the Master of Cyber Security program requirements.

Stream 2: The Master of Cyber Security in Tradescraft (ZEITIS8628) is designed to provide technically competent IT professionals with an accelerated introduction to research, scholarship and major practical techniques in offensive and defensive cyber operations, wireless security, reverse engineering, and exploit development and the analysis of big data in a security context. The elective offerings allow a focus on Digital or Network forensics or critical infrastructure cyber security. Students are required to complete 8 courses (48 UOC) comprising 7 core courses and 1 elective course.

The Master of Cyber Security Operations (8629) is designed for postgraduate scholars and professional managers with appropriate undergraduate qualifications in management or a related discipline and / or extensive relevant professional experience who wish to gain a more detailed understanding of the managerial and technical skills and expertise relevant to planning, operation and acquisition of the cyber security function. This Masters coursework degree is designed to meet the demand for executives and managers who oversee the cyber security function in government, industry, law enforcement and defence. It provides principles gathered

from information systems, cyber security, risk, management and governance for managers seeking to enhance their career in cyber security operations [9].

The Master in Cyber Security, Strategy & Diplomacy program (8631) was developed in 2016 and designed for postgraduate scholars and professional managers with appropriate undergraduate qualifications and / or professional experience in the Social Sciences, Humanities or Information Sciences. The program is offered by HASS and provides advanced interdisciplinary study into the political, military, diplomatic and higher-level management aspects of issues where cyber security, strategy and diplomacy interact. It is intended for students in the diplomatic, defence, justice, public safety, regulatory, management and information sciences. Governments, enterprises, communities and civil society around the world are grappling with strategy and regulation for the new domain of cyberspace, at the same time as their security and other interests are being transformed by the rapid pace of information technology exploitation -- both for beneficial and for malicious purposes. It is widely accepted that the threats in cyber space are escalating while responses to mitigate them are not able to keep up. This program will provide students with the ability to understand the main policy, operational, ethical and informational challenges for security thrown up by the integration or penetration of advanced information technologies into all spheres of human activity [10].

The two programs, Cyber Security Operations (8628) and Cyber Security Strategy and Diplomacy (8631), are designed such way that students can choose a combination of core and plus online elective courses and complete the degree without travelling to Canberra, as they are delivered fully online. This opens a venue for interstate and international students.

4 OBSERVATIONS AND LESSONS LEARNED

In order to run world-class programs successfully, create a highly regarded reputation among ACCS customers including individual students and interested organisations, identification of challenges and lessons learned is essential. The areas

identified are: rapid growing; course convenors and instructors; course development; equipment and labs; cross-institutional collaborations and students.

A. Growing fast. ACCS's

Masters for Cyber security programs shows rapid growth in student enrolments, with an increase of 125% over the past year (Fig.1). The largest distance (online) class in 2016 was 65 students (ZEIT 8032 Information Assurance Principle), however in 2017 the largest class reached 80 students (ZEIT 8017 Cyber Crime). Class size poses challenges to course instructors for monitoring the increased numbers of online discussion posts and keeping students engaged online. The course assignments might require future modifications to overcome this challenge.

The ACCS has already experienced challenges in accommodating IDM classes due to the limited capacity of student computers at the Cyber Range. High demand classes such as ZEIT 8020 Computer Network Operations and ZEIT 8026 Network Security Operations are offered in both semester 1 and 2 and then in 2017 we had to offer the classes twice in each semester that doubled the workload for the course instructor. In response to the growing numbers of students in IDM classes, ACCS is investing in a new Cyber Range laboratory with capacity to accommodate more students and developing a new forensic laboratory.

Some of ACCS courses are still offered only once a year, but consistently growing enrolment will soon demand more classes in both semesters. As the majority of sessional staff are full time industry practitioners, they have limited abilities to run classes in both semesters, leading to workforce challenges for the faculty.

B. Course convenors and instructors.

As described earlier, cyber security is a broad term and has eight vectors of attack and response. Thus, it is essential to have skilled core academic staff that can develop high quality courses within the programs. These academics should be interested in subject matter and not only come with a strong cyber security background but also hold a range of multi-disciplinary skills related to cyber security. For example, skills in cyber security and diplomacy; cyber security and human factors; skills in software security and systems engineering; cyber security policy and law. ACCS has currently seven full-time academics raging from junior to senior academics, and also sessional staff who have contributed to the development of a strong set of courses. Mentoring of junior staff and sessional staff is a vital component in the rapid development of many courses and the fulfilment of required teaching demand, as described in below paragraph.

The percentage of courses delivered in IDM in the Cyber Security (8628) program is very high. For example, among the 12 courses offered in the program including core and electives, only two are distance courses and delivered fully online and the rest in IDM. Students attend the Cyber Range for one week where they participate in hands-on exercises and the rest of 12 weeks study online.

Due to very technical nature of such courses, ACCS employs world-class practitioners in the field to develop and deliver Master courses. These instructors are valuable assets to the program, but are often new to the academic environment or have had limited exposure to academia, and therefore require help and mentoring from the full-time academics in the setup of pedagogical aspects of their teaching, and in educational ethics. Sessional staff also need assistance in learning to navigate the Moodle online environment. The high, and sometimes unpredictable turnover of sessional staff also places extra challenges on the ACCS's academic team.

The full-time academic team face time challenges in developing and delivering new courses, consulting students, and mentoring junior staff and sessional instructors. They must also conduct research and supervise graduate students, submit quality

articles to international peer-reviewed journals, and submit grant applications in order to strengthen the reputation of the UNSW and provide leadership for the growing cyber-security program.

The ACCS has close connections to the professional bodies such Australian Computer Society (ACS), the Information Systems Audit and Control Association (ISACA), International Information System Security Consortium (ISC2). Among our academics we hold several certifications: CISSP, CSSLP, CCFP. Two of the master courses ZEIT 8024 Software Security Lifecycle and ZEIT 8021 Information Assurance and Security are based on ISC2 materials and provide base information on these certificates to students.

C. Course development and modification.

As the cyber security area is constantly evolving, the courses offered by the ACCS require constant updates and sometimes major re-development in order to maintain cutting-edge relevance. Academic research outcomes (publications) are consistently incorporated into course material. Industry professionals contribute real world examples to course content, as well as students already working in the field.

D. Cross-institutional collaboration.

As approximately half the ACCS students are from defence, examples are tied to military requirement, which is developed through collaboration with other military institutions, for example the course ZEIT 8018 Cyber Defence Governance and Acquisition was developed in collaboration with academics from Canfield University. The Masters Cyber Security Program Coordinator has secured a grant to support outreach with the Air Force Institute of Technology (AFIT), the United States Air Force Academy (UAF Academy) and the University of Alabama in Huntsville (UAH).

E. Equipment and Laboratories.

Cyber security education requires well-equipped laboratories. Hands-on practicals are critical to building a high-quality program. Laboratory facilities should

be of sufficient quantity and quality to support the expected size of the program and different specialisation streams (Forensics, Advanced Tradescraft).

Current Cyber Range has 3 labs with 24, 19, and 27 networked computers with VMs to run Windows and Linux, and are isolated from the Internet. The required software and traffic generator is available for student exercises. SCADA tables representing different critical infrastructures with real-world hardware and software to operate process control systems for: water storage tank; water treatment plant, urban village with traffic control, electrical grid and street lights control. A new Cyber Range security lab with 100 workstations and a new Forensics lab with 20 workstations are currently under development.

F. Students.

The majority of students in the Masters of cyber security programs are highly motivated full-time working practitioners who study part-time. Approximately 45% of all students are from Defence, with the others from government and private sector organisations. Often students bring their work situation related cyber security issues to the course discussions and assignments. Some students are choosing a path with the 12 UOC project, which motivates them to deliver their research work within the program back to their work environment. Women comprise around~5% of the student cohort.

In order to ensure the best student outcomes during hands-on practicals, a level of assumed knowledge is required prior to commencing a course. Students receive information from instructors 1-2 weeks prior to IDM and have opportunities to communicate / clarify arrangements with instructors, which provide additional support for students without specific technical knowledge.

5 CONCLUSIONS AND FUTURE DIRECTIONS

This paper describes an initiative from the Australian Centre for Cyber Security (ACCS) at UNSW Canberra at ADFA to develop a suite of three postgraduate cyber security programs to address the constantly increasing number of students

from diverse backgrounds interested in studying cyber security and acquiring the skills to be cyber warfare professionals. This paper describes the structured approach to developing the programs, and highlights challenges by providing observations and lessons learned over the past two years. These include the rapid growth of the program and the courses delivered, as well as the impact on the academic team, the requirement for adequate equipment and labs, and a general description of the student cohort.

With a developing reputation as a centre of excellence in cybersecurity education, ACCS will continue to be the leader in cybersecurity education pioneering in:

- Knowledge transfer through a suite of Masters Degrees that is unique in Australia, oriented to national security agencies and the Australian Defence Forces;
- Promoting development of a broad expertise in Cyber security holistically among students with STEM (IT, science and engineering) and non-STEM (art, business, social science) backgrounds; and also, students from the Australian Defence Forces;
- Regular interaction and collaboration with relevant national security agencies through ACCS academic staff and doctoral students in order to incorporate emerging cyber warfare skills within program content;
- Outreach through ACCS's staff interaction with military institutions world-wide.

REFERENCES

[1] Prime Minister and Cabinet, Department of (2016), *Australia's Cyber Security Strategy*, Commonwealth of Australia. [viewed online 20/04/2017] https://cybersecuritystrategy.dpmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf

[2] Slay J., Training and education for cyber security, cyber defence and cyber warfare, United Service 67(33), Seminar proceedings, September 2016

[3] Defence Department *2016 Defence White Paper* (Commonwealth of Australia: Canberra).

[4] Austin GD, Slay J (2016) *Benchmarking Australia's Cybersecurity Strategy: a Future-looking Checklist*, UNSW Canberra, ACCS Briefing Paper No1 [viewed online 20th April 2017] https://www.unsw.adfa.edu.au/australian-centre-for-cyber-security/sites/accs/files/uploads/BENCHMARKING%20AUSTRALIAN%20CYBER%20SECURITY%20POLICY_0.pdf

[5] Austin GD, Slay J (2016) *Australia's Response to Advanced Technology Threats: An Agenda for the Next Government*, UNSW Canberra, Canberra, Australian Centre for Cyber Cyber Security Discussion Paper No3 [viewed online 20th April 2017] https://www.unsw.adfa.edu.au/australian-centre-for-cyber-security/sites/accs/files/uploads/ADVANCED%20TECHNOLOGY%20THREATS%20AND%20AUSTRALIA%2030%20May%202106mediaversion.pdf

[6] Austin GD (2014) *Australia's Digital Skills for Peace and War*, Australian Journal of Telecommunications and the Digital Economy (AJTDE), vol 2 No4 [viewed online 20th April] http://telsoc.org/ajtde/2014-12-v2-n4/a68

[7] UNSW Handbook [viewed online 17/04 /2017] http://www.handbook.unsw.edu.au/faculties/2014/adfa/adfa.html

[8] Cyber Security Handbook [viewed online 17th April 2017] http://www.handbook.unsw.edu.au/postgraduate/programs/2017/8628.html

[9] Cyber Security Operations Handbook [viewed online 17th April 2017] http://www.handbook.unsw.edu.au/postgraduate/programs/2017/8629.html

[10] Cyber Security, Strategy and Diplomacy Handbook [viewed online 17th April 2017] http://www.handbook.unsw.edu.au/postgraduate/programs/2016/8631.html