

Master of Cyber Security, Strategy and Risk Management

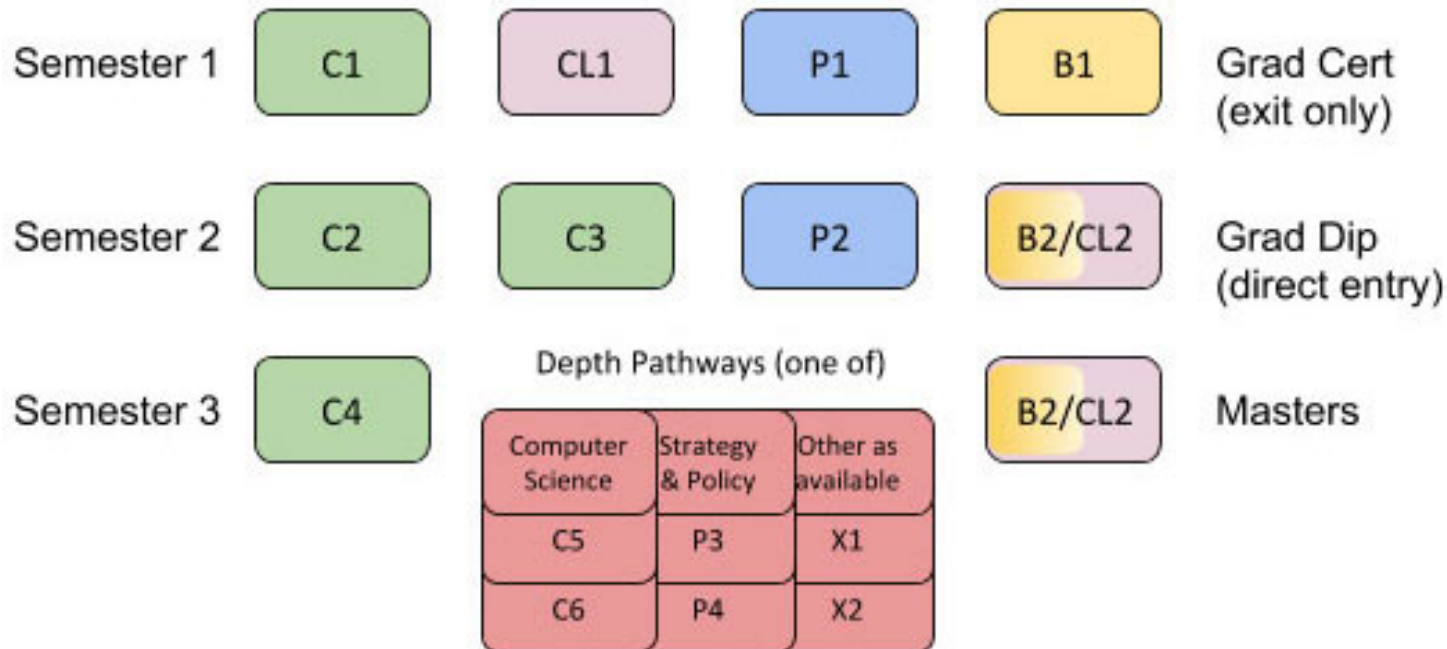
CECS PG Information Session

April 17, 2018

Program Purpose

Provide a working understanding of information, network and software security, across technical, legal, business, and policy dimensions, with a deeper understanding within one of these areas.

Program Structure



Required courses (Master)

C1	COMP6301 Computing Foundations for Cyber Security
C2	COMP6340 Networked Information Systems
C3	COMP6420 Introduction to Data Management, Analysis and Security
C4	COMP7500 Software Security

Required courses (Master)

CL1	LAWS8077 Cyber Law
CL2	CRIM8002 Cyber Security and Cyber Crime
P1	NSPO8006 National Security and Policy Making
P2	NSPO8021 Statecraft and National Security in Cyberspace
B1	MGMT7203 Risk Analysis for Business Management
B2	MGMT8005 Project Risk and Issues Management

Depth Pathway

C5/6	COMP8701 Cyber Defensive Operations (AQF9 version of COMP3701) COMP8702 Cyber Offensive Operations (AQF9 version of COMP3702)
P3/4	NSP8014: Ethics and Technologies of War NSP8017: Malicious Networks: Transnational Terrorism and Crime
Other	Other depth pathways will be offered as available and as approved by the convenor

Learning outcome

- **Leadership in cyber security strategy:**
 - Develop and apply effective cyber security strategies, provide leadership direction for an organization to best prepare itself for operations in a contested environment.
- **Cyber security policy assessment:**
 - Assess the role policy plays in engineering secure systems, technology for policy implementation, and the role of policy in driving the composition of cyber security solutions.

Learning outcome

- Legal and ethical aspects:
 - Compare and contrast the legal and ethical aspects of cyber security at the national and international level.
 - Negotiate the legal, social, regulatory, ethical, and technical issues related to securing information systems and critical infrastructures.

Learning outcome

Technical aspects:

- **Integrate acquired knowledge** in cyber security to propose solutions for real world problems.
- **Monitor, direct, and enhance the protection of cyber systems** through widely accepted standards, procedures and policies.
- **Assess vulnerability** of existing and proposed ICT systems.
- **Manage for cyber security risks**, focusing on decision making, trade-offs, requirements building, team building, and leading.
- Demonstrate **awareness of and responses to a diverse range of cyber threats**

Course overview (CS)

COMP6301 Computing Foundations for Cyber Security:

1. Intro to computer systems
2. Linux fundamentals
3. Intro to programming
4. Overview of software designs fundamentals
5. Vulnerability basics

Course overview (CS)

- **COMP7500 Software Security**
 - Basic principles: security properties, security models, design principles
 - Memory safety
 - Reverse engineering
 - Defense mechanisms
 - Bug finding
 - Exploitation
 - OS security
 - Web security
 - Mobile security

Course overview (CS)

COMP8701 Cyber Defensive Operations (AQF9 version of COMP3701)

- Defensive Cyber Security operations introduces and exercises a complete range of anomaly / intrusion detection and identification mechanisms.
- Students will also learn and exercise handling of an existing intrusion which includes forensic operations as well as securing the remaining systems.
- This is a complete course in cyber defense which enables students on successful completion to operate systems under real-world exposure.

Course overview (CS)

COMP8702 Cyber Offensive Operations (AQF9 version of COMP3702)

- Offensive Cyber Security operations introduces and exercises a complete range of reverse engineering techniques and attack patterns.
- Students will also learn and exercise analysis of systems based on minimal information.
- This is a complete course in cyber attacks which enables students on successful completion to identify and test systems for vulnerabilities without full knowledge or direct access.

Delivery mode

- All courses listed on the Cyber Security course schedule are online intensive courses.
- These are delivered in 4+1+4 mode –
 - 4 weeks of online teaching and assessment,
 - followed by one full-time week on campus at the ANU,
 - followed by another 4 weeks of online teaching and assessment.

Course schedule (indicative)

Academic session 2018	Start-finish dates (9 weeks total)	On-campus intensive (Week 5 out of 9)	Census date	Indicative application closing date
Winter	6 Aug – 5 Oct	3-7 Sept	24 Aug	~30 June
Spring	1 Oct – 30 Nov	29 Oct – 2 Nov	19 Oct	~ 28 Aug

Admission

- Open to domestic students
 - Currently not available for international students
- Applicants for the Graduate Diploma must hold either an Honours degree (AQF8) or a Bachelor degree (AQF7) with a GPA of 4.0 / 7.0, plus one year's relevant work experience.
- Applicants for the Masters must hold a Bachelor degree with a GPA of 5.0 / 7.0, plus three years' relevant work experience.

Contact

- Website: **<https://cecs.anu.edu.au/study>**
- For further information and expressions of interests, contact:
dataanalytics.cecs@anu.edu.au
- Program convener: alwen.tiu@anu.edu.au