Overview

The Master of Cyber Security Operations is a postgraduate award offered by the School of Engineering and Information Technology. It 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 coursework masters 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.
Faculty
UNSW Canberra at ADFA

Campus
Canberra

Study Level
Postgraduate

Typical duration
1 Years

Delivery Mode
Distance

Intake Period
Semester 1, Semester 2

Academic Calendar
UNSW Canberra Calendar

Minimum Units of Credit
48

Award type
Masters (Coursework)

Award(s)
Master of Cyber Security Operations - MCyberSecOps
Learning Outcomes

1. Graduates will evaluate cyber security operations practices and their interaction with a wide range of international and national issues.

Global Citizens

2. Graduates will have demonstrated the application of knowledge and skills with creativity and initiative in new situations in professional practice or for further learning in Cyber Security Operations.

Leaders

3. Graduates will be able to communicate effectively to a range of audiences and be capable of independent and collaborative inquiry, working effectively with others in the field of Cyber Security Operations.

Scholars

4. Graduates will have demonstrated the application of knowledge and skills within Cyber Security Operations with high level personal autonomy and accountability

Professionals

5. Graduates will have demonstrated the application of knowledge and skills to plan and execute a substantial research-based project or piece of scholarship within Cyber Security Operations

Professionals

6. Graduates will have acquired advanced disciplinary knowledge and skills in Cyber Security Operations, and an ability to apply these in a range of contexts.

Professionals Scholars

7. Graduates will have developed advanced critical thinking and problem solving skills and be able to apply them to Cyber Security Operations.

Scholars

Graduate Capabilities:

For more information on Graduate Capabilities, please click on this link.
Program Structure

Students must complete 48 UOC as a standalone program.

1. Core courses - 24 UOC
2. Prescribed elective courses - 24 UOC

Core Courses

Students must take 24 UOC of the following courses.

ZEIT8017  |  6 UOC
Cyber Crime and Cyber Security

ZEIT8018  |  6 UOC
Cyber Resilience: Management Governance and Acquisition

ZEIT8032  |  6 UOC
Information Assurance Principles

ZEIT8037  |  6 UOC
Cyber Security Risk Management

Prescribed Electives List 1

Students can take up to a maximum of 24 UOC of the following courses.

YCAN8000  |  6 UOC
US Cyber Policy and Information Security

ZEIT8019  |  6 UOC
Intrusion Analysis and Response

ZEIT8020  |  6 UOC
Cyber Offence: Threats and Opportunities

ZEIT8024  |  6 UOC
Software Security Lifecycle
<table>
<thead>
<tr>
<th>Code</th>
<th>UOC</th>
<th>Course Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZEIT8025</td>
<td>6</td>
<td>Reverse Engineering</td>
</tr>
<tr>
<td>ZEIT8026</td>
<td>6</td>
<td>Cyber Defence: Network Security Operations</td>
</tr>
<tr>
<td>ZEIT8027</td>
<td>6</td>
<td>Critical Infrastructure and Control System Security</td>
</tr>
<tr>
<td>ZEIT8028</td>
<td>6</td>
<td>Digital Forensics</td>
</tr>
<tr>
<td>ZEIT8029</td>
<td>6</td>
<td>Network and Memory Forensics</td>
</tr>
<tr>
<td>ZEIT8030</td>
<td>6</td>
<td>Big Data and Decision Analytics for Security</td>
</tr>
<tr>
<td>ZEIT8033</td>
<td>6</td>
<td>Critical Infrastructure Security Policy and Governance</td>
</tr>
<tr>
<td>ZEIT8035</td>
<td>6</td>
<td>Cyber Terrorism</td>
</tr>
<tr>
<td>ZEIT8036</td>
<td>6</td>
<td>Humans and Security</td>
</tr>
<tr>
<td>ZEIT8043</td>
<td>6</td>
<td>Cyber and the Law</td>
</tr>
<tr>
<td>ZPEM8208</td>
<td>6</td>
<td>Human Factors and the Technological Interface</td>
</tr>
</tbody>
</table>

Prescribed Electives List 2
Students should complete no more than two electives (12 UOC) from the list below:

Note: Students may complete up to two courses (12 UOC) from a related coursework program with the approval of the Postgraduate Coordinator.

**ZEIT8015 | 6 UOC**  
Cyber Operations

**ZEIT8115 | 6 UOC**  
Information Operations

**ZEIT8303 | 6 UOC**  
Project Management Body of Knowledge

**ZHSS8441 | 6 UOC**  
Cyber-Security and World Politics

**Research Project**

Students can take up to a maximum of 12 UOC of the following courses.

**ZEIT8260 | 6 UOC**  
Project Report - Cyber Security (Part Time)

**ZEIT8261 | 12 UOC**  
Project Report - Cyber Security (Full Time)

**Research Project Maturity Requirement**

Students must have completed 24 UOC before taking any of the following courses.

**ZEIT8260 | 6 UOC**  
Project Report - Cyber Security (Part Time)

**ZEIT8261 | 12 UOC**  
Project Report - Cyber Security (Full Time)

**Enrolment Disclaimer**
Unless advised otherwise by your program authority, you should follow the rules for the handbook for the year you commenced your program. You are also responsible for ensuring you enrol in courses according to your program requirements. myUNSW enrolment checks that you have met enrolment requirements such as pre-requisites for individual courses but not that a course will count towards your program requirements.
Admission Requirements

Entry Requirements

To gain entry into a Master of Cyber Security Operations (8629), an applicant must meet one of the following entry requirements:

1. Completion of a Bachelor degree with honours in the same or a related discipline* from a recognised institution; or

2. Completion of a Graduate Diploma or Graduate Certificate in the same or a related discipline* from a recognised institution; or

3. Completion of a Bachelor degree in the same or a related discipline* from a recognised institution; and completion of at least three years relevant full-time professional experience; or

4. Completion of a Bachelor degree in a non-related discipline; and completion of at least four years relevant full-time professional experience; or

5. Evidence of other qualifications and professional experience to be assessed as acceptable grounds for admission into the program by the relevant Program Authority. In certain circumstances, students may be required to undertake and successfully complete a relevant non-award course as a condition for admission into the program. This non-award course may also be credited towards the program upon admission.

*Related Discipline/s: Business or Management

For more information about admission requirements for various UNSW programs, visit the following website(s):

Domestic Students
International Student
Program Requirements

Progression Requirements

Exit Arrangements:

Students who do not complete the full Master program requirements may exit the program with a Graduate Certificate in Cyber Security Operations qualification (24 UOC). Of the four courses, students must complete a minimum of two core courses and two other courses from the 8629 program.

For any advanced standing granted on entry into the Masters program, a maximum of 12 UOC advanced standing can be applied to the Graduate Certificate. It is still a requirement that the student complete at least one core course at UNSW.

For more information on university policy on progression requirements please visit Academic Progression.
Recognition of Achievement

Award with Excellence

The Award with Excellence is awarded in coursework masters programs, including Masters (Extension) but with the exception of Masters (Extended) such as JD and MD, when a Weighted Average Mean (WAM) of at least 80% has been achieved and at least 50% of the requirements of the award are completed at UNSW. All eligible programs will award 'with Excellence' except in special circumstances where approval of Academic Board has been given for a program to opt out.

For more information, please visit:

Current Students Award with Excellence
Additional Information

PLuS Alliance

This program is part of the PLuS Alliance, a new international university partnership between UNSW, Arizona State University (ASU) and King's College London (KCL).

Students enrolled in this program will be able to complete the elective identified above, online from Arizona State University. Further information will be added to the School of Engineering and Information Technology website.
Program Fees

At UNSW fees are generally charged at course level and therefore dependent upon individual enrolment and other factors such as student's residency status. For generic information on fees and additional expenses of UNSW programs, click on one of the following:

- Domestic Students
- Commonwealth Supported Students
- International Students

Additional Expenses

Computer, internet and texts
Pre-2019 Handbook Editions

Access past handbook editions (2018 and prior)

Pre-2019 Handbook Editions
© UNSW Sydney (CRICOS Provider No.: 00098G), 2019. The information contained in this Handbook is indicative only. While every effort is made to keep this information up-to-date, the University reserves the right to discontinue or vary arrangements, programs and courses at any time without notice and at its discretion. While the University will try to avoid or minimise any inconvenience, changes may also be made to programs, courses and staff after enrolment. The University may also set limits on the number of students in a course.

Authorised by Deputy Vice-Chancellor (Academic)
CRICOS Provider Code 00098G
ABN: 57 195 873 179