



# PICX8049

## Australia and Cyber Intelligence

Session 2, Online-flexible 2022

*Department of Security Studies and Criminology*

### Contents

|                                       |   |
|---------------------------------------|---|
| <u>General Information</u>            | 2 |
| <u>Learning Outcomes</u>              | 2 |
| <u>General Assessment Information</u> | 3 |
| <u>Assessment Tasks</u>               | 4 |
| <u>Delivery and Resources</u>         | 6 |
| <u>Unit Schedule</u>                  | 7 |
| <u>Policies and Procedures</u>        | 8 |

#### **Disclaimer**

Macquarie University has taken all reasonable measures to ensure the information in this publication is accurate and up-to-date. However, the information may change or become out-dated as a result of change in University policies, procedures or rules. The University reserves the right to make changes to any information in this publication without notice. Users of this publication are advised to check the website version of this publication [or the relevant faculty or department] before acting on any information in this publication.

## General Information

Unit convenor and teaching staff

Jeffrey Foster

[jeff.foster@mq.edu.au](mailto:jeff.foster@mq.edu.au)

Credit points

10

Prerequisites

Admission to MPICT or MCP ICT or GradDipPICT or GradDipCPICT or GradCertCPICT or MPICTMIntSecSt or MCP ICTMIntSecSt or MIntSecStud or GradDipIntSecStud or GradCertIntSecStud or MCyberSec or MSecStrategicStudMCyberSec or MIntellMCyberSec or MCyberSecMCTerrorism or MCyberSecMCrim or Master of Cyber Security Analysis

Corequisites

Co-badged status

Unit description

Cyberspace has become a major site for different forms of warfare and coercion, ranging from cyber disruption, through information compromise, all the way to covert information operations on a national level. In this unit students learn how robust cyber intelligence can be used to enhance the often-reactive posture of cyber security. This includes understanding the role of cyber intelligence and counterintelligence within the broad, integrated configuration of cyber-security. Students will learn fundamental intelligence collection and analysis principles and apply them to a cyber-security context. All enrolment queries should be directed to Open Universities Australia (OUA): see [www.open.edu.au](http://www.open.edu.au)

## Important Academic Dates

Information about important academic dates including deadlines for withdrawing from units are available at <https://www.mq.edu.au/study/calendar-of-dates>

## Learning Outcomes

On successful completion of this unit, you will be able to:

**ULO1:** Critique contemporary literature relating to the concepts of cyber intelligence

**ULO2:** Demonstrate higher order communication skills including the ability to formulate sustained, persuasive and original written and oral arguments

**ULO3:** Model academic research skills, particularly the ability to select sources appropriately to integrate knowledge from diverse sources, to critically evaluate its

significance and relevance, synthesise material and present finding logically, rationally and lucidly

**ULO4:** Model intelligence collection and analysis skills, particularly the ability to select and evaluate sources and produce an effective intelligence assessment.

**ULO5:** Evaluate how the intelligence function fits within the dynamic national and internal cybersecurity context.

## General Assessment Information

### SUBMITTING ASSESSMENT TASKS

- All text-based assessment tasks are to be submitted, marked and returned electronically. This will only happen through the unit iLearn site.
- Assessment tasks must be submitted as a MS word document by the due date.
- Most assessment tasks will be subject to a 'Turnitin' review as an automatic part of the submission process.
- The granting of extensions is subject to the university's Special Consideration Policy. Extensions will not be granted by unit conveners or tutors, but must be lodged through Special Consideration: <https://students.mq.edu.au/study/my-study-program/special-consideration>

### Late Assessment Submission Penalty

*Unless a Special Consideration request has been submitted and approved, a 5% penalty (of the total possible mark) will be applied each day a written assessment is not submitted, up until the 7th day (including weekends). After the 7th day, a mark of '0' (zero) will be awarded even if the assessment is submitted. Submission time for all written assessments is set at 11.55pm. A 1-hour grace period is provided to students who experience a technical issue.*

This late penalty will apply to written reports and recordings only. Late submission of time sensitive tasks (such as tests/exams, performance assessments/presentations, scheduled practical assessments/labs) will be addressed by the unit convenor in a Special consideration application.

### WORD LIMITS FOR ASSESSMENT TASKS

- Stated word limits include footnotes and footnoted references, but not bibliography, or title page.
- Word limits can generally deviate by 10% either over or under the stated figure.
- If the number of words exceeds the limit by more than 10%, then penalties will apply. These penalties are 5% of the awarded mark for every 100 words over the word limit. If a paper is 300 words over, for instance, it will lose  $3 \times 5\% = 15\%$  of the total mark awarded for the assignment. This percentage is taken off the total mark, i.e. if a paper was graded

at a credit (65%) and was 300 words over, it would be reduced by 15 marks to a pass (50%).

- The application of this penalty is at the discretion of the course convener.

## REASSESSMENT OF ASSIGNMENTS DURING THE SESSION

- Macquarie University operates a Grade Appeal Policy in cases where students feel their work was graded inappropriately: <http://www.mq.edu.au/policy/docs/gradeappeal/policy.html>
- In accordance with the Grade Appeal Policy, individual works are not subject to regrading.

## Assessment Tasks

| Name  | Weighting | Hurdle | Due                             |
|---|-----------|--------|---------------------------------|
| <a href="#"><u>Intelligence Report</u></a>                      | 25%       | No     | 11:59PM - 3 Oct                 |
| <a href="#"><u>Preliminary Analysis and Collection Plan</u></a> | 20%       | No     | 11:59PM - 22 Aug                |
| <a href="#"><u>Intelligence Briefing</u></a>                    | 25%       | No     | 11:59PM - 28 Oct                |
| <a href="#"><u>Quiz</u></a>                                     | 30%       | No     | 11:59PM - 26 Aug, 16 Sep, 4 Nov |

### Intelligence Report

Assessment Type <sup>1</sup>: Project

Indicative Time on Task <sup>2</sup>: 25 hours

Due: **11:59PM - 3 Oct**

Weighting: **25%**

An open-source intelligence collection on a relevant target culminating in a structured written report.

On successful completion you will be able to:

- Critique contemporary literature relating to the concepts of cyber intelligence
- Demonstrate higher order communication skills including the ability to formulate sustained, persuasive and original written and oral arguments

- Model academic research skills, particularly the ability to select sources appropriately to integrate knowledge from diverse sources, to critically evaluate its significance and relevance, synthesise material and present findings logically, rationally and lucidly
- Model intelligence collection and analysis skills, particularly the ability to select and evaluate sources and produce an effective intelligence assessment.
- Evaluate how the intelligence function fits within the dynamic national and internal cybersecurity context.

## Preliminary Analysis and Collection Plan

Assessment Type <sup>1</sup>: Project

Indicative Time on Task <sup>2</sup>: 25 hours

Due: **11:59PM - 22 Aug**

Weighting: **20%**

A Preliminary analysis of the target based on a scan of readily available material culminating in a detailed collection plan with RFIs.

On successful completion you will be able to:

- Critique contemporary literature relating to the concepts of cyber intelligence
- Demonstrate higher order communication skills including the ability to formulate sustained, persuasive and original written and oral arguments
- Model academic research skills, particularly the ability to select sources appropriately to integrate knowledge from diverse sources, to critically evaluate its significance and relevance, synthesise material and present findings logically, rationally and lucidly
- Model intelligence collection and analysis skills, particularly the ability to select and evaluate sources and produce an effective intelligence assessment.

## Intelligence Briefing

Assessment Type <sup>1</sup>: Project

Indicative Time on Task <sup>2</sup>: 16 hours

Due: **11:59PM - 28 Oct**

Weighting: **25%**

A 10-minute presentation or a two-page intelligence product providing an intelligence evaluation of a relevant target.

On successful completion you will be able to:

- Critique contemporary literature relating to the concepts of cyber intelligence
- Demonstrate higher order communication skills including the ability to formulate sustained, persuasive and original written and oral arguments
- Model academic research skills, particularly the ability to select sources appropriately to integrate knowledge from diverse sources, to critically evaluate its significance and relevance, synthesise material and present findings logically, rationally and lucidly
- Model intelligence collection and analysis skills, particularly the ability to select and evaluate sources and produce an effective intelligence assessment.
- Evaluate how the intelligence function fits within the dynamic national and internal cybersecurity context.

## Quiz

Assessment Type <sup>1</sup>: Quiz/Test

Indicative Time on Task <sup>2</sup>: 10 hours

Due: **11:59PM - 26 Aug, 16 Sep, 4 Nov**

Weighting: **30%**

3 X Quiz covering the prescribed literature in the course.

On successful completion you will be able to:

- Critique contemporary literature relating to the concepts of cyber intelligence
- Evaluate how the intelligence function fits within the dynamic national and internal cybersecurity context.

---

<sup>1</sup> If you need help with your assignment, please contact:

- the academic teaching staff in your unit for guidance in understanding or completing this type of assessment
- the [Writing Centre](#) for academic skills support.

<sup>2</sup> Indicative time-on-task is an estimate of the time required for completion of the assessment task and is subject to individual variation

## Delivery and Resources

### UNIT REQUIREMENTS AND EXPECTATIONS

- You should spend an average of 12 hours per week on this unit. This includes listening to lectures prior to seminar or tutorial, reading weekly required materials as detailed in iLearn, participating in iLearn discussion forums and preparing assessments.
- Internal students are expected to attend all seminar or tutorial sessions, and external students are expected to make significant contributions to on-line activities.
- In most cases students are required to attempt and submit all major assessment tasks in order to pass the unit.

## REQUIRED READINGS

- The citations for all the required readings for this unit are available to enrolled students through the unit iLearn site, and at Macquarie University's library site. Electronic copies of required readings may be accessed through the library or will be made available by other means.

## TECHNOLOGY USED AND REQUIRED

- Computer and internet access are essential for this unit. Basic computer skills and skills in word processing are also a requirement.
- This unit has an online presence. Login is via: <https://ilearn.mq.edu.au/>
- Students are required to have regular access to a computer and the internet. Mobile devices alone are not sufficient.
- Information about IT used at Macquarie University is available at [http://students.mq.edu.au/it\\_services/](http://students.mq.edu.au/it_services/)

## STAFF AVAILABILITY

- Department staff will endeavour to answer student enquiries in a timely manner. However, emails or iLearn messages will not usually be answered over the weekend or public holiday period.
- Students are encouraged to read the Unit Guide and look at instructions posted on the iLearn site before sending email requests to staff.

# Unit Schedule

Tentative Class Schedule

| Module | Week Starting | Topic | Reading |
|--------|---------------|-------|---------|
|        |               |       |         |

|                    |             |   |  |
|--------------------|-------------|---|--|
| 1                  | 25 Jul 2022 | Welcome/Kick-off                          | May (Intro & Ch. 1 to 5)   |
| 2                  | 1 Aug 2022  | Intelligence Collection Planning          | May (Ch. 6 to 9) - Clark (Ch. 1-2)   |
| 3                  | 8 Aug 2022  | Readily available sources                 | Coney (Ch. 1.1-1.5) - Bertram (Preface, Intro, Ch. 1)                              |
| 4                  | 15 Aug 2022 | A Threatening World                       | Cooney (Ch. 2.1-2.3) - Bertram (Ch. 2-3)   |
| 5                  | 22 Aug 2022 | Tasking for in-depth OSINT investigations | Bertram (Ch. 4, Conclusion, Appendix A) - Clark (pp. 176-189)                      |
| 6                  | 29 Aug 2022 | Forensics 1                               | Stanfield (2009) - What are computer forensics                                     |
| 7                  | 5 Sep 2022  | Forensics 2                               | Casey (Ch. 1) - Holt (Ch. 10-11)   |
| InterSession Break | 12 Sep 2022 |   |  |
| InterSession Break | 19 Sep 2022 |   |  |
| 8                  | 26 Sep 2022 | Completing collection                     | Cooney (Ch. 3.1-3.3)   |
| 9                  | 3 Oct 2022  | Writing up the target model               | Cooney (Ch. 4.1-4.4) - Caltagirone (2018) - Industrial Control Threat Intelligence |
| 10                 | 10 Oct 2022 | Preparing verbal Intelligence Briefing    | May (Ch. 10-13) - Hutchins - Intelligence-driven computer network defense          |
| 11                 | 17 Oct 2022 | What does the customer need?              | Caltagirone et al. (2013) - The Diamond Model of Intrusion Analysis                |
| 12                 | 24 Oct 2022 | Last minute trouble shooting              | May (Ch. 14-15 and Conclusion)   |
| 13                 | 31 Oct 2022 | Review                                    | Cooney (Ch. 5.1-5.5 and Afterword)   |

Please note, exact order of topics may vary during the semester as needed.

## Policies and Procedures

Macquarie University policies and procedures are accessible from [Policy Central \(https://policies.mq.edu.au\)](https://policies.mq.edu.au). Students should be aware of the following policies in particular with regard to



## Learning and Teaching:

- [Academic Appeals Policy](#)
- [Academic Integrity Policy](#)
- [Academic Progression Policy](#)
- [Assessment Policy](#)
- [Fitness to Practice Procedure](#)
- [Assessment Procedure](#)
- [Complaints Resolution Procedure for Students and Members of the Public](#)
- [Special Consideration Policy](#)

Students seeking more policy resources can visit [Student Policies](https://students.mq.edu.au/support/study/policies) (<https://students.mq.edu.au/support/study/policies>). It is your one-stop-shop for the key policies you need to know about throughout your undergraduate student journey.

To find other policies relating to Teaching and Learning, visit [Policy Central](https://policies.mq.edu.au) (<https://policies.mq.edu.au>) and use the [search tool](#).

## Student Code of Conduct

Macquarie University students have a responsibility to be familiar with the Student Code of Conduct: <https://students.mq.edu.au/admin/other-resources/student-conduct>

## Results

Results published on platform other than [eStudent](#), (eg. iLearn, Coursera etc.) or released directly by your Unit Convenor, are not confirmed as they are subject to final approval by the University. Once approved, final results will be sent to your student email address and will be made available in [eStudent](#). For more information visit [ask.mq.edu.au](https://ask.mq.edu.au) or if you are a Global MBA student contact [globalmba.support@mq.edu.au](mailto:globalmba.support@mq.edu.au)

## Academic Integrity

At Macquarie, we believe [academic integrity](#) – honesty, respect, trust, responsibility, fairness and courage – is at the core of learning, teaching and research. We recognise that meeting the expectations required to complete your assessments can be challenging. So, we offer you a range of resources and services to help you reach your potential, including free [online writing and maths support](#), [academic skills development](#) and [wellbeing consultations](#).

## Student Support

Macquarie University provides a range of support services for students. For details, visit <http://students.mq.edu.au/support/>

## The Writing Centre

[The Writing Centre](#) provides resources to develop your English language proficiency, academic writing, and communication skills.

- [Workshops](#)
- [Chat with a WriteWISE peer writing leader](#)
- [Access StudyWISE](#)
- [Upload an assignment to Studiosity](#)
- [Complete the Academic Integrity Module](#)

The Library provides online and face to face support to help you find and use relevant information resources.

- [Subject and Research Guides](#)
- [Ask a Librarian](#)

## Student Services and Support

Macquarie University offers a range of [Student Support Services](#) including:

- [IT Support](#)
- [Accessibility and disability support](#) with study
- Mental health [support](#)
- [Safety support](#) to respond to bullying, harassment, sexual harassment and sexual assault
- [Social support including information about finances, tenancy and legal issues](#)

## Student Enquiries

Got a question? Ask us via [AskMQ](#), or contact [Service Connect](#).

## IT Help

For help with University computer systems and technology, visit [http://www.mq.edu.au/about\\_us/offices\\_and\\_units/information\\_technology/help/](http://www.mq.edu.au/about_us/offices_and_units/information_technology/help/).

When using the University's IT, you must adhere to the [Acceptable Use of IT Resources Policy](#). The policy applies to all who connect to the MQ network including students.