PICX8080

Cyber Conflict, Cyber Espionage and Cyber Terrorism

Session 1, Online-flexible 2022

Department of Security Studies and Criminology

Contents

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
Jennifer Hunt
jennifer.hunt@mq.edu.au

Credit points
10

Prerequisites
Admission to MCrim or MPICT or MCPICT or GradDipPICT or GradDipCPICT or PGCertPICT or GradCertPICT or GradCertCPICT or MPICTMIntSecSt or MCPICTMIntSecSt or MIntSecStud or GradDipIntSecStud or MInfoTech or MSecStrategicStud or MIntell or MCTerrorism or MCyberSec or GradDipSecStudCr or GradCertSecStudCr or MSecStrategicStudMCrim or MSecStrategicStudMIntell or MSecStrategicStudMCyberSec or MSecStrategicStudMCTerrorism or MIntellMCrim or MIntellMCyberSec or MIntellMCTerrorism or MCyberSecMCTerrorism or MCyberSecMCrim or MCTerrorismMCrim or Master of Cyber Security Analysis or 10cps at 6000 level or 10cps 8000 level

Corequisites

Co-badged status

Unit description
This unit provides an overview of the new and developing threats that cyberspace brings in terms of global security and the implications for corporate, law enforcement and national security responses. The course will analyse cyber attacks involving both nation state actors and non-nation state actors with political motives (including terrorists) through historical, operational and strategic perspectives. Students will gain an understanding of various definitions of cyber espionage, cyber terrorism, cyber warfare and information warfare. They will also be able to analyse how nation states and non-nation state actors utilise the Internet as an attack vector in information warfare to infiltrate digital systems to gain control of critical infrastructure. The unit is interactive and students are expected to actively participate in seminars and online discussion forums.

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: Understand and differentiate characteristics and typologies of different cyber threats and trends in the cyber space.

ULO2: Analyse the technical, social and political drivers of information warfare, cyber conflict and cyber espionage.

ULO3: Analyse how nation-states and non-nation-state actors utilise the Internet as an attack vector in information warfare to infiltrate digital systems and gain control of critical infrastructure, through the use of case studies.

ULO4: Develop the ability to conduct independent and collaborative research through written presentations.

Assessment Tasks

Name	Weighting	Hurdle	Due
Active Engagement	10%	No	Weekly
Quiz	20%	No	Week 6
Case Study	30%	No	Week 8
Research Essay	40%	No	Week 12

Active Engagement

Assessment Type [1]: Participatory task
Indicative Time on Task [2]: 10 hours
Due: **Weekly**
Weighting: **10%**

Students will be required to demonstrate active and critical engagement with course materials. This includes showing a detailed knowledge and understanding of weekly readings and a critical awareness of, and response to, issues raised in the weekly lecture. This will be demonstrated by responding to the weekly questions posted on the online forum as well as engage in forum discussion.

On successful completion you will be able to:

- Understand and differentiate characteristics and typologies of different cyber threats and trends in the cyber space.
- Analyse the technical, social and political drivers of information warfare, cyber conflict and cyber espionage.

- Analyse how nation-states and non-nation-state actors utilise the Internet as an attack vector in information warfare to infiltrate digital systems and gain control of critical infrastructure, through the use of case studies.
- Develop the ability to conduct independent and collaborative research through written presentations.

Quiz

Assessment Type [1]: Quiz/Test
Indicative Time on Task [2]: 10 hours
Due: **Week 6**
Weighting: **20%**

Quizzes will periodically test understanding and application of key concepts and frameworks from the course.

On successful completion you will be able to:
- Understand and differentiate characteristics and typologies of different cyber threats and trends in the cyber space.
- Analyse the technical, social and political drivers of information warfare, cyber conflict and cyber espionage.
- Analyse how nation-states and non-nation-state actors utilise the Internet as an attack vector in information warfare to infiltrate digital systems and gain control of critical infrastructure, through the use of case studies.
- Develop the ability to conduct independent and collaborative research through written presentations.

Case Study

Assessment Type [1]: Case study/analysis
Indicative Time on Task [2]: 20 hours
Due: **Week 8**
Weighting: **30%**

Cyber Attack Case Study

On successful completion you will be able to:

- Understand and differentiate characteristics and typologies of different cyber threats and trends in the cyber space.
- Analyse how nation-states and non-nation-state actors utilise the Internet as an attack vector in information warfare to infiltrate digital systems and gain control of critical infrastructure, through the use of case studies.
- Develop the ability to conduct independent and collaborative research through written presentations.

Research Essay

Assessment Type [1]: Essay
Indicative Time on Task [2]: 36 hours
Due: **Week 12**
Weighting: **40%**

Research Essay on Specific Cyber Issue

On successful completion you will be able to:
- Understand and differentiate characteristics and typologies of different cyber threats and trends in the cyber space.
- Analyse the technical, social and political drivers of information warfare, cyber conflict and cyber espionage.
- Analyse how nation-states and non-nation-state actors utilise the Internet as an attack vector in information warfare to infiltrate digital systems and gain control of critical infrastructure, through the use of case studies.
- Develop the ability to conduct independent and collaborative research through written presentations.

[1] 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.

[2] 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 watching recorded lectures, reading weekly required materials as detailed in iLearn, participating in Ilearn discussion forums and preparing assessments.
- Students are expected to make significant contributions to online course 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. A helpful guide including shortcuts for accessing journal articles remotely is available at: https://www.mq.edu.au/about/facilities/library/covid-19-response/journal-survival-guide

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.
- The course website is available on ilearn. Login at: 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/

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. Assessment due dates in this guide are indicative only and may be adjusted by course convenor.

- 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 SUBMISSION OF ASSESSMENT TASKS

Unless a Special Consideration request has been submitted and approved, (a) a penalty for lateness will apply – 10 marks out of 100 credit will be deducted per day for assignments submitted after the due date – and (b) no assignment will be accepted seven days (incl. weekends) after the original submission deadline. No late submissions will be accepted for timed assessments - e.g. quizzes, online tests.

WORD LIMITS FOR ASSESSMENT TASKS

- Stated word limits include footnotes and footnoted references, but not the reference list, 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 x 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 SEMESTER

- 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.

STAFF AVAILABILITY

- Department staff will endeavour to answer student enquiries in a timely manner (usually 2 business days). Work email is not monitored outside regular work hours, 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.

Policies and Procedures

Macquarie University policies and procedures are accessible from Policy Central (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). 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) 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 or if you are a Global MBA student contact 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/.

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.