PICT808

Cyber Terrorism and Information Warfare

S1 Online 2019

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
Convenor
Stephen McCombie
stephen.mccombie@mq.edu.au

Credit points
4

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

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:

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

Analyse how nation-states and non-nation-states actors utilize 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.

Identify the value of the Internet as a vehicle to recruit, communicate, and fund terrorism.

Analyse the technical, social and political drivers of cyber terrorism and information warfare.

Develop the ability to conduct independent and collaborative research through written and oral presentations

Assessment Tasks

Name	Weighting	Hurdle	Due
Engagement/Participation	10%	No	Weekly
Weekly Quiz	10%	No	Weekly
Case Study	30%	No	See iLearn
Research Essay	50%	No	See iLearn

Engagement/Participation

Due: **Weekly**
Weighting: **10%**

Internal students

Your participation in class should demonstrate that you have read, understood and reflected on course material and weekly readings.   You should bring in related thoughts and material, readings or questions that occur to you throughout the discussion.

You are required to complete the core readings for each module, reflect upon the readings and to then share your reflections on the readings with course colleagues during the on-campus sessions.

Students who attend less than 8 seminars will receive a mark of zero for this component of participation.

External students

Your postings to the online discussion forums should demonstrate that you have read, understood and reflected on course material and weekly readings. You should bring in related thoughts and material, readings or questions that occur to you throughout the discussion. You are required to complete the core readings for each module, reflect upon the readings and share your reflections on the readings with course colleagues through online discussion forum questions. One question will be posted to the discussion forum each week. Responses to each question should be a minimum of 100 words in length.

Students who do not fully participate in at least 8 discussion forums will receive a mark of zero for this component of participation.

See iLearn for marking rubric.

On successful completion you will be able to:

- Identify the value of the Internet as a vehicle to recruit, communicate, and fund terrorism.
- Develop the ability to conduct independent and collaborative research through written and oral presentations

Weekly Quiz

Due: **Weekly**
Weighting: **10%**

Weighting: **10%**

For weeks 3-12 there will be a short online quiz based on the set readings.

On successful completion you will be able to:

- Understand and differentiate characteristics and typologies of different crime threats and trends in the cyber space.
- Analyse how nation-states and non-nation-states actors utilize 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.
- Identify the value of the Internet as a vehicle to recruit, communicate, and fund terrorism.
- Analyse the technical, social and political drivers of cyber terrorism and information warfare.
- Develop the ability to conduct independent and collaborative research through written and oral presentations

Case Study

Due: **See iLearn**
Weighting: **30%**

Due: **See unit iLearn site** Weighting: **30%**

The 2,000 word essay allows students to explore a cyber-terrorism/information warfare case study A detailed marking matrix is available to all enrolled students on the unit iLearn site. Marking criteria includes evaluation of understanding of key concepts, written expression, referencing, structure and layout. The list of case studies will be supplied to students in week 2.

See iLearn for marking rubric.

On successful completion you will be able to:

- Understand and differentiate characteristics and typologies of different crime threats and trends in the cyber space.
- Analyse how nation-states and non-nation-states actors utilize 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.
- Analyse the technical, social and political drivers of cyber terrorism and information warfare.
- Develop the ability to conduct independent and collaborative research through written and oral presentations

Research Essay

Due: **See iLearn**
Weighting: **50%**

Due: **See unit iLearn site** Weighting: **50%**

3,000 word **research** essay.   Students will be required to do extensive, self-led research on a predefined topic related to cyber security practice or procedure. The research topic/question will be provided to students in week 4.

A detailed marking matrix is available to all enrolled students on the unit iLearn site. Marking criteria includes evaluation of understanding of cyber security concepts, arguments put forward and academic support for those arguments, written expression, referencing and structure and layout.

See iLearn for marking rubric.

On successful completion you will be able to:

- Understand and differentiate characteristics and typologies of different crime threats and trends in the cyber space.
- Analyse the technical, social and political drivers of cyber terrorism and information warfare.
- Develop the ability to conduct independent and collaborative research through written and oral presentations

Delivery and Resources

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/

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 SUBMISSION OF ASSESSMENT TASKS

Unless a Special Consideration request has been submitted and approved, (a) **a penalty for lateness will apply** – two (2) marks out of 100 will be deducted per day for assignments submitted after the due date – and (b) **no assignment will be accepted seven (7) 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 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 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. 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.

Policies and Procedures

Macquarie University policies and procedures are accessible from Policy Central (https://staff.mq.edu.au/work/strategy-planning-and-governance/university-policies-and-procedures/policy-central). 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
- Grade Appeal Policy
- Complaint Management Procedure for Students and Members of the Public
- Special Consideration Policy *(**Note:** The Special Consideration Policy is effective from 4 December 2017 and replaces the Disruption to Studies Policy.)*

Undergraduate students seeking more policy resources can visit the Student Policy Gateway (https://students.mq.edu.au/support/study/student-policy-gateway). It is your one-stop-shop for the key policies you need to know about throughout your undergraduate student journey.

If you would like to see all the policies relevant to Learning and Teaching visit Policy Central (https://staff.mq.edu.au/work/strategy-planning-and-governance/university-policies-and-procedures/policy-central).

Student Code of Conduct

Macquarie University students have a responsibility to be familiar with the Student Code of Conduct: https://students.mq.edu.au/study/getting-started/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

Student Support

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

Learning Skills

Learning Skills (mq.edu.au/learningskills) provides academic writing resources and study strategies to improve your marks and take control of your study.

- Workshops
- StudyWise
- Academic Integrity Module for Students
- Ask a Learning Adviser

Student Services and Support

Students with a disability are encouraged to contact the Disability Service who can provide appropriate help with any issues that arise during their studies.

Student Enquiries

For all student enquiries, visit Student Connect at ask.mq.edu.au

If you are a Global MBA student contact globalmba.support@mq.edu.au

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.

Graduate Capabilities

PG - Capable of Professional and Personal Judgment and Initiative

Our postgraduates will demonstrate a high standard of discernment and common sense in their professional and personal judgment. They will have the ability to make informed choices and decisions that reflect both the nature of their professional work and their personal perspectives.

This graduate capability is supported by:

Learning outcomes

- Understand and differentiate characteristics and typologies of different crime threats and trends in the cyber space.
- Analyse how nation-states and non-nation-states actors utilize 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.
- Identify the value of the Internet as a vehicle to recruit, communicate, and fund terrorism.
- Analyse the technical, social and political drivers of cyber terrorism and information warfare.
- Develop the ability to conduct independent and collaborative research through written and oral presentations

Assessment tasks

- Engagement/Participation
- Weekly Quiz
- Case Study
- Research Essay

PG - Discipline Knowledge and Skills

Our postgraduates will be able to demonstrate a significantly enhanced depth and breadth of knowledge, scholarly understanding, and specific subject content knowledge in their chosen fields.

This graduate capability is supported by:

Learning outcomes

- Understand and differentiate characteristics and typologies of different crime threats and trends in the cyber space.
- Analyse how nation-states and non-nation-states actors utilize 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.
- Identify the value of the Internet as a vehicle to recruit, communicate, and fund terrorism.
- Analyse the technical, social and political drivers of cyber terrorism and information warfare.
- Develop the ability to conduct independent and collaborative research through written and oral presentations

Assessment tasks

- Engagement/Participation
- Weekly Quiz
- Case Study
- Research Essay

PG - Critical, Analytical and Integrative Thinking

Our postgraduates will be capable of utilising and reflecting on prior knowledge and experience, of applying higher level critical thinking skills, and of integrating and synthesising learning and knowledge from a range of sources and environments. A characteristic of this form of thinking is the generation of new, professionally oriented knowledge through personal or group-based critique of practice and theory.

This graduate capability is supported by:

Learning outcomes

- Understand and differentiate characteristics and typologies of different crime threats and trends in the cyber space.
- Analyse how nation-states and non-nation-states actors utilize 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.
- Identify the value of the Internet as a vehicle to recruit, communicate, and fund terrorism.
- Analyse the technical, social and political drivers of cyber terrorism and information warfare.
- Develop the ability to conduct independent and collaborative research through written and oral presentations

Assessment tasks

- Engagement/Participation
- Weekly Quiz
- Case Study
- Research Essay

PG - Research and Problem Solving Capability

Our postgraduates will be capable of systematic enquiry; able to use research skills to create new knowledge that can be applied to real world issues, or contribute to a field of study or practice to enhance society. They will be capable of creative questioning, problem finding and problem solving.

This graduate capability is supported by:

Learning outcomes

- Understand and differentiate characteristics and typologies of different crime threats and trends in the cyber space.
- Analyse how nation-states and non-nation-states actors utilize 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.
- Identify the value of the Internet as a vehicle to recruit, communicate, and fund terrorism.
- Analyse the technical, social and political drivers of cyber terrorism and information warfare.
- Develop the ability to conduct independent and collaborative research through written and oral presentations

Assessment tasks

- Engagement/Participation
- Weekly Quiz
- Case Study
- Research Essay

PG - Effective Communication

Our postgraduates will be able to communicate effectively and convey their views to different social, cultural, and professional audiences. They will be able to use a variety of technologically supported media to communicate with empathy using a range of written, spoken or visual formats.

This graduate capability is supported by:

Learning outcomes

- Understand and differentiate characteristics and typologies of different crime threats and trends in the cyber space.
- Analyse how nation-states and non-nation-states actors utilize 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.
- Identify the value of the Internet as a vehicle to recruit, communicate, and fund terrorism.
- Analyse the technical, social and political drivers of cyber terrorism and information warfare.
- Develop the ability to conduct independent and collaborative research through written and oral presentations

Assessment tasks

- Engagement/Participation
- Weekly Quiz
- Case Study
- Research Essay

PG - Engaged and Responsible, Active and Ethical Citizens

Our postgraduates will be ethically aware and capable of confident transformative action in relation to their professional responsibilities and the wider community. They will have a sense of connectedness with others and country and have a sense of mutual obligation. They will be able to appreciate the impact of their professional roles for social justice and inclusion related to national and global issues

This graduate capability is supported by:

Learning outcomes

- Understand and differentiate characteristics and typologies of different crime threats and trends in the cyber space.
- Analyse how nation-states and non-nation-states actors utilize 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.
- Identify the value of the Internet as a vehicle to recruit, communicate, and fund terrorism.
- Analyse the technical, social and political drivers of cyber terrorism and information warfare.
- Develop the ability to conduct independent and collaborative research through written and oral presentations

Assessment tasks

- Engagement/Participation
- Weekly Quiz
- Case Study
- Research Essay