# PICT808

## Cyber Terrorism and Information Warfare

S1 Evening 2016

*Dept of Policing, Intelligence & Counter-Terrorism*

## 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
Yves-Heng Lim
yves-heng.lim@mq.edu.au

Credit points
4

Prerequisites
Admission to MPICT or PGDipPICT or GradDipPICT or PGCertPICT or GradCertPICT or MPICTMIntSecSt or MIntSecStud or PGDipIntSecStud or GradDipIntSecStud or PGCertIntSecStud or PGCertIntell or MCompForens or PGDipCompForens or PGCertCompForens

Corequisites

Co-badged status

Unit description
Computer systems and networks, and the applications that they support, are core elements of critical infrastructure for public and private sector organisations in the twenty-first century. This unit will present a high-level overview of how cyber terrorist threats and foreign states might infiltrate systems and gain control of critical infrastructure. This unit explores how different vertical industries face specific threats from their use of current day technology. The 'human factor' in dealing with cyber terrorist threats will be emphasised.

## 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.

Demonstrate knowledge of relevant theories, cross disciplinary approaches (criminology and information security) and research applicable to the study of cyber terrorism and information warfare.

# Assessment Tasks

| Name | Weighting | Hurdle | Due |
|---|---|---|---|
| Participation/ engagement | 10% | No | Weekly |
| Presentations | 30% | No | Fortnightly |
| Quizzes | 20% | No | Week 4 and Week 10 |
| Major essay | 40% | No | End of Week 11 |

## Participation/ engagement

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

This will encourage students to engage critically in both classroom and online discussions. A variety of different activities will occur each week and students should be prepared to fully participate in these activities. This will include an online discussion for external students, and weekly seminar participation and attendance only for internal students). Please note that if an internal student is unable to attend a seminar they will be required to participate in the online discussion.

Online discussion format: at least one question will be posted to the discussion forum each week. Responses to each question should be a minimum of 100 words in length. Your postings to the online discussions should reflect your understanding and ability to synthesise course readings and seminar content, and to include related thoughts and analysis.

Your postings should advance the group's discussion of ideas and meanings about the material. Some ways you can further discussions include:

- expressing ideas or observations - where possible support them by more than personal opinion or anecdotal evidence;
- making a connection between the current discussion and previous discussion, using personal experience or readings;
- commenting on or expanding another student’s statement;
- posting a substantive question aimed at furthering the group’s understanding.

Please keep your posts brief, one or two paragraphs is sufficient. If citing course readings, in text references are sufficient.

For a posting to be counted for a given week, it must be entered by midnight on the Sunday of that week’s activity. If entered later than this, the posting will not be counted.

A mark for the discussions will be awarded on the basis of:

- For internal students, your attendance and participation in the class (50%), and the content of your contribution (50%) .
- For external students, your participation the online discussion (50%), and the content of your contribution (50%).

In assessing your contributions the following categories will be used:

- Level 1 - Postings providing a single point of view;
- Level 2 - Postings which make reference to other contexts or course material;
- Level 3 - Postings which offer a critical reflection on theoretical perspectives and/or practical experiences.

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.
- Demonstrate knowledge of relevant theories, cross disciplinary approaches (criminology and information security) and research applicable to the study of cyber terrorism and information warfare.

## Presentations

Due: **Fortnightly**
Weighting: **30%**

Objective

Problem based learning (PBL) Presentation in seminars of 15 minutes duration plus Q&A. The aim of this assignment is for groups to undertake a series of in-depth investigations into contemporary topics in cyber terrorism and information warfare. The presentation (from a set list of problems) will cover the content provided in all the learning outcomes. This gives students a specific problem around which to research and incorporate the content provided in lectures and reading. The PBL reinforces critical thinking skills.

Requirements

Internal students: Students are required to form small groups at the beginning of the course. Each group is required to (a) develop a written presentation in the form of PowerPoint slides (or equivalent) and (b) to make an oral presentation using these slides. A different topic is to be selected for each presentation which will be provided in your iLearn.

External students: Students can either form small groups at the beginning of the course, or as individuals as well. Students are required to submit a PowerPoint Presentation (or equivalent) with presenters' notes that, if presented orally, would extend to around 12-15 minutes (approximately 10 slides).  Please note: No oral presentation is required for this assessment task.  Each slide should contain logical, clear and easily understood points that demonstrate understanding of the topic. The notes section of the presentation should discuss or argue the relevance of each of the bullet points in the body of the slide. This enables the lecturer/tutor to assess your understanding of the topic.  You should also place in the notes section the details of the references that you have used in each slide.

Assessment

Internal students: The content of the slides will comprise 15% of the overall 30% course mark. Each group member receives the same mark. The presentation of the slides will then comprise the remaining 15% of the overall course mark. Each group member will be assessed individually. Assessing presentations are compiled in a standard form and a peer/self-assessment form will be collected at the close of each presentation. The marking guide, which will be uploaded in iLearn, will be used to assess the content and presentation. Groups should organize themselves in such a way that work is evenly distributed between members. To this end, each group member must present for approximately equal time per person.

External students: The content of the slides will comprise 30% of the overall course mark. In case of a group presentation, group member receives the same mark. The marking guide, which will be uploaded in iLearn, will be used to assess the content and presentation.

Length

Each presentation should last for 15 minutes including Q&A.

Dates

Presentation will be on Week 3, Week 5, Week 7, Week 9, and Week 11.

For external students, for a presentation to be counted for a given week, it must be submitted by midnight on the Sunday of that week's activity. If entered later than this, the presentation will be not be marked.

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.
- Demonstrate knowledge of relevant theories, cross disciplinary approaches (criminology

and information security) and research applicable to the study of cyber terrorism and information warfare.

## Quizzes

Due: **Week 4 and Week 10**
Weighting: **20%**

Two quizzes during the course will be in Week 4 and Week 10. Each quiz will be a total of one hour of multiple-choice, short answers, essay questions, etc. The quizzes will be online based around the readings and course materials from specified weeks. The quizzes will be available for only a certain period, usually three days. Each quiz will be worth 10%.

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.
- Demonstrate knowledge of relevant theories, cross disciplinary approaches (criminology and information security) and research applicable to the study of cyber terrorism and information warfare.

## Major essay

Due: **End of Week 11**
Weighting: **40%**

Students will choose a topic from a list of given topics that fall within the ambient of cybercrime, information warfare and cyber terrorism. If students are not writing an essay from the given topics, you must seek approval from your instructor on your essay question in the first instance. The essay length is 3000 words excluding references/bibliography. The essay will show student's knowledge of theories and practice and their ability to critically evaluate the chosen topic.

Submission date will be on end of Week 11. A detailed marking matrix will be available on the course iLearn site. Marking criteria in the marking matrix includes evaluation of topic knowledge, supporting evidence & methods, logical argument & readability, use of readings & referencing, essay structure and organisation.

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.
- Demonstrate knowledge of relevant theories, cross disciplinary approaches (criminology and information security) and research applicable to the study of cyber terrorism and information warfare.

# Delivery and Resources

## UNIT REQUIREMENTS AND EXPECTATIONS

- You should spend an average of at least 12 hours per week on this unit. This includes listening to pre-recorded lectures prior to seminar discussions and reading weekly required readings detailed in iLearn.
- Internal students are expected to attend all seminar sessions and external students are expected to contribute to on-line discussions.
- Students are required to 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 EReserve site. Electronic copies of required readings may be accessed at the EReserve site.

## TECHNOLOGY USED AND REQUIRED

- Personal PC 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.
- For technical support go to: http://mq.edu.au/about_us/offices_and_units/informatics/help
- For student quick guides on the use of iLearn go to: http://mq.edu.au/iLearn/student_info/guides.htm

## SUBMITTING ASSESSMENT TASKS

- All assessment tasks are to be submitted, marked and returned electronically. This will only happen through the unit iLearn site.
- Assessment tasks must be submitted either as a PDF or 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 of up to one week are at the discretion of the unit convener. Any requests for extensions must be made in writing before the due date for the submission of the assessment task. Extensions beyond one week are subject to the university's Disruptions Policy (http://www.mq.edu.au/policy/docs/disruption_studies/policy.html#purpose).

LATE SUBMISSION OF ASSESSMENT TASKS

- If an assignment is submitted late, 5% of the available mark will be deducted for each day (including weekends) the paper is late.
- For example, if a paper is worth 20 marks, 1 mark will be deducted from the grade given for each day that it is late (i.e. a student given 15/20 who submitted 4 days late will lose 4 marks = 11/20).
- The same principle applies if an extension is granted and the assignment is submitted later than the amended date.

WORD LIMITS FOR ASSESSMENT TASKS

- Stated word limits do not include references, 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 he 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://mq.edu.au/policy/docs/gradeappeal/policy.html). This process involves all assignments submitted for that unit being reassessed. However, in exceptional cases students may request that a single piece of work is reassessed.

# Policies and Procedures

Macquarie University policies and procedures are accessible from Policy Central. Students should be aware of the following policies in particular with regard to Learning and Teaching:

Academic Honesty Policy http://mq.edu.au/policy/docs/academic_honesty/policy.html

**New Assessment Policy in effect from Session 2 2016** http://mq.edu.au/policy/docs/assessment/policy_2016.html. For more information visit http://students.mq.edu.au/events/2016/07/19/new_assessment_policy_in_place_from_session_2/

Assessment Policy prior to Session 2 2016 http://mq.edu.au/policy/docs/assessment/policy.html

Grading Policy prior to Session 2 2016 http://mq.edu.au/policy/docs/grading/policy.html

Grade Appeal Policy http://mq.edu.au/policy/docs/gradeappeal/policy.html

Complaint Management Procedure for Students and Members of the Public http://www.mq.edu.au/policy/docs/complaint_management/procedure.html

Disruption to Studies Policy http://www.mq.edu.au/policy/docs/disruption_studies/policy.html *The Disruption to Studies Policy is effective from March 3 2014 and replaces the Special Consideration Policy.*

In addition, a number of other policies can be found in the Learning and Teaching Category of 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/support/student_conduct/

## Results

Results shown in *iLearn*, 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.

# 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

## 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.
- Demonstrate knowledge of relevant theories, cross disciplinary approaches (criminology and information security) and research applicable to the study of cyber terrorism and information warfare.

## Assessment tasks

- Participation/ engagement
- Presentations
- Quizzes
- Major 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.
- Demonstrate knowledge of relevant theories, cross disciplinary approaches (criminology and information security) and research applicable to the study of cyber terrorism and information warfare.

## Assessment tasks

- Participation/ engagement
- Presentations
- Quizzes
- Major 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.
- Demonstrate knowledge of relevant theories, cross disciplinary approaches (criminology and information security) and research applicable to the study of cyber terrorism and information warfare.

## Assessment tasks

- Participation/ engagement
- Presentations
- Quizzes
- Major 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.
- Demonstrate knowledge of relevant theories, cross disciplinary approaches (criminology and information security) and research applicable to the study of cyber terrorism and information warfare.

## Assessment tasks

- Participation/ engagement

- Presentations
- Quizzes
- Major 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.
- Demonstrate knowledge of relevant theories, cross disciplinary approaches (criminology and information security) and research applicable to the study of cyber terrorism and information warfare.

### Assessment tasks

- Participation/ engagement
- Presentations
- Quizzes
- Major 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.

### Assessment tasks

- Participation/ engagement
- Presentations
- Quizzes
- Major essay

## Changes since First Published

| Date | Description |
|---|---|
| 11/01/2016 | For approval by HoD. |