



# PICT808

## Cyber Terrorism and Information Warfare

S1 External 2015

*Dept of Policing, Intelligence & Counter-Terrorism*

### Contents

|                                |   |
|--------------------------------|---|
| <u>General Information</u>     | 2 |
| <u>Learning Outcomes</u>       | 2 |
| <u>Assessment Tasks</u>        | 3 |
| <u>Delivery and Resources</u>  | 6 |
| <u>Policies and Procedures</u> | 8 |
| <u>Graduate Capabilities</u>   | 9 |

#### **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

Allan Watt

[allan.watt@mq.edu.au](mailto:allan.watt@mq.edu.au)

Julian Droogan

[julian.droogan@mq.edu.au](mailto:julian.droogan@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:

- Interpret the characteristics and concepts of both cyber terrorism and information warfare
- Evaluate how cyber terrorist threats and foreign states, might infiltrate systems and gain control of critical infrastructure
- Analyse how different vertical industries face specific treats from their use of current day technology

Conceptualise the 'human factor' in dealing with cyber terrorist threats

Critically examine and interpret Australian and International sources when analysing cyber terrorism and information warfare, information

Synthesis core responses and devise a comprehensive cyber terrorism ready reaction plan

## Assessment Tasks

| Name                        | Weighting | Due           |
|-----------------------------|-----------|---------------|
| <u>Unit Engagement</u>      | 25%       | Weekly        |
| <u>Research Essay</u>       | 25%       | 29 March 2015 |
| <u>Cyber Terrorism Plan</u> | 50%       | 31 May 2015   |

## Unit Engagement

Due: **Weekly**

Weighting: **25%**

This assessment is concerned with all unit learning outcomes.

Your postings to the online discussions should reflect an understanding of your own context and the course material. 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 through online postings and (for internal students) during the on-campus sessions.

Your postings should advance the group's negotiation 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, 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 additional references (if applicable), please provide a bibliographic reference at the end of your post.

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 they are entered later than this, they will not be counted.

In some instances an online quiz may be provided for a week in lieu.

Internal students will follow the same assessment framework within the class each week.

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

1. Your participation in the discussions (40%)
2. The essence of your contributions (60%)

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:

- Interpret the characteristics and concepts of both cyber terrorism and information warfare
- Evaluate how cyber terrorist threats and foreign states, might infiltrate systems and gain control of critical infrastructure
- Analyse how different vertical industries face specific treats from their use of current day technology
- Conceptualise the 'human factor' in dealing with cyber terrorist threats
- Critically examine and interpret Australian and International sources when analysing cyber terrorism and information warfare, information
- Synthesis core responses and devise a comprehensive cyber terrorism ready reaction plan

## Research Essay

Due: **29 March 2015**

Weighting: **25%**

Media and other agencies report incidents of cyber attacks, some of these are labelled as acts of cyber terrorism, some of these may be or more often than not are mislabelled as such.

You should select a recent (since 2012) cyber attack event (in Australia or overseas) and investigate if this is a cyber terror attack or a simple mislabelling of the incident.

1500 words.

The 1500 word essay is a review of a known international cyber attack and what are the specific characteristics of it and does it fall within the ambient of cyber crime, information warfare or cyber terrorism and what makes it specifically differ from one of the other genres.

A detailed marking matrix is available to all enrolled students on the unit iLearn site.

Marking criteria in the marking matrix includes evaluation of topic comprehension, argument, written expression, referencing, essay structure and organisation.

On successful completion you will be able to:

- Interpret the characteristics and concepts of both cyber terrorism and information warfare
- Evaluate how cyber terrorist threats and foreign states, might infiltrate systems and gain control of critical infrastructure
- Analyse how different vertical industries face specific treats from their use of current day technology
- Conceptualise the 'human factor' in dealing with cyber terrorist threats
- Critically examine and interpret Australian and International sources when analysing cyber terrorism and information warfare, information
- Synthesis core responses and devise a comprehensive cyber terrorism ready reaction plan

## Cyber Terrorism Plan

Due: **31 May 2015**

Weighting: **50%**

Prevention and or early detection are better than a cure in most situations. Many agencies have disaster recovery and other contingency plans. However many organisations plans do not extend to cyber terror attacks and in fact many staff would not know what form such an attack found take.

Given this ready reaction plans are a necessity, as well as staff awareness and training in what to do in the event of an attack.

There are many IT based preventive plan templates available from the internet from known IT security agencies such as ISC<sup>2</sup>.

3500 words.

The 3500 word cyber terrorism reaction plan allows students to explore the application of cyber security principals to a real world environment.

A scenario will be provided to students later in the Session.

A detailed marking matrix is available to all enrolled students on the unit iLearn site.

Marking criteria in the marking matrix includes evaluation of topic comprehension, written expression, referencing, plan and orders structure and organisation and workability.

Note:

The plan is to include notes and referencing at the end of the document and not within the main body.

On successful completion you will be able to:

- Interpret the characteristics and concepts of both cyber terrorism and information warfare
- Evaluate how cyber terrorist threats and foreign states, might infiltrate systems and gain control of critical infrastructure
- Analyse how different vertical industries face specific treats from their use of current day technology
- Conceptualise the 'human factor' in dealing with cyber terrorist threats
- Critically examine and interpret Australian and International sources when analysing cyber terrorism and information warfare, information
- Synthesis core responses and devise a comprehensive cyber terrorism ready reaction plan

## **Delivery and Resources**

### 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](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](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](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 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 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

## 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](http://mq.edu.au/policy/docs/academic_honesty/policy.html)

Assessment Policy <http://mq.edu.au/policy/docs/assessment/policy.html>

Grading Policy <http://mq.edu.au/policy/docs/grading/policy.html>

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

Grievance Management Policy [http://mq.edu.au/policy/docs/grievance\\_management/policy.html](http://mq.edu.au/policy/docs/grievance_management/policy.html)

Disruption to Studies Policy [http://www.mq.edu.au/policy/docs/disruption\\_studies/policy.html](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/](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](http://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](http://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](http://ask.mq.edu.au)

## IT Help

For help with University computer systems and technology, visit <http://informatics.mq.edu.au/help/>.

When using the University's IT, you must adhere to the [Acceptable Use 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

- Interpret the characteristics and concepts of both cyber terrorism and information warfare
- Evaluate how cyber terrorist threats and foreign states, might infiltrate systems and gain control of critical infrastructure
- Analyse how different vertical industries face specific threats from their use of current day

technology

- Conceptualise the 'human factor' in dealing with cyber terrorist threats
- Critically examine and interpret Australian and International sources when analysing cyber terrorism and information warfare, information
- Synthesis core responses and devise a comprehensive cyber terrorism ready reaction plan

## **Assessment tasks**

- Unit Engagement
- Research Essay
- Cyber Terrorism Plan

## **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**

- Interpret the characteristics and concepts of both cyber terrorism and information warfare
- Evaluate how cyber terrorist threats and foreign states, might infiltrate systems and gain control of critical infrastructure
- Analyse how different vertical industries face specific treats from their use of current day technology
- Critically examine and interpret Australian and International sources when analysing cyber terrorism and information warfare, information
- Synthesis core responses and devise a comprehensive cyber terrorism ready reaction plan

## **Assessment tasks**

- Unit Engagement
- Research Essay
- Cyber Terrorism Plan

## **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**

- Interpret the characteristics and concepts of both cyber terrorism and information warfare
- Evaluate how cyber terrorist threats and foreign states, might infiltrate systems and gain control of critical infrastructure
- Analyse how different vertical industries face specific treats from their use of current day technology
- Conceptualise the 'human factor' in dealing with cyber terrorist threats
- Critically examine and interpret Australian and International sources when analysing cyber terrorism and information warfare, information
- Synthesis core responses and devise a comprehensive cyber terrorism ready reaction plan

## **Assessment tasks**

- Unit Engagement
- Research Essay
- Cyber Terrorism Plan

## **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**

- Evaluate how cyber terrorist threats and foreign states, might infiltrate systems and gain control of critical infrastructure
- Analyse how different vertical industries face specific treats from their use of current day technology
- Conceptualise the 'human factor' in dealing with cyber terrorist threats
- Critically examine and interpret Australian and International sources when analysing cyber terrorism and information warfare, information
- Synthesis core responses and devise a comprehensive cyber terrorism ready reaction plan

## Assessment tasks

- Unit Engagement
- Research Essay
- Cyber Terrorism Plan

## 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

- Interpret the characteristics and concepts of both cyber terrorism and information warfare
- Evaluate how cyber terrorist threats and foreign states, might infiltrate systems and gain control of critical infrastructure
- Critically examine and interpret Australian and International sources when analysing cyber terrorism and information warfare, information
- Synthesis core responses and devise a comprehensive cyber terrorism ready reaction plan

## Assessment tasks

- Unit Engagement
- Research Essay
- Cyber Terrorism Plan

## 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

- Analyse how different vertical industries face specific treats from their use of current day technology
- Conceptualise the 'human factor' in dealing with cyber terrorist threats

- Synthesis core responses and devise a comprehensive cyber terrorism ready reaction plan