PICT808

Cyber Terrorism and Information Warfare

S1 External 2014

Centre for Policing, Intelligence and Counter Terrorism

Contents

General Information	2
Learning Outcomes	2
Assessment Tasks	3
Delivery and Resources	6
Unit Schedule	7
Policies and Procedures	7
Graduate Capabilities	8

General Information

Unit convenor and teaching staff
Unit Convenor
Allan Watt
allan.watt@mq.edu.au
Contact via allan.watt@mq.edu.au
Rm 240, Level 2, Building Y3A
By appointment

Credit points
4

Prerequisites
Admission to MPICT or PGDipPICT or PGCertPICT or MPICTMIntSecSt or MIntSecStud or PGDipIntSecStud 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.
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
Task 1	20%	Week 3
Task 2	30%	Week 5
Task 3	50%	Week 12

Task 1

Due: **Week 3**
Weighting: **20%**

Review the unit reference material and other suitable sources to create a presentation on various aspects of Information Operations theory and what is the underlying concern of managers and who importantly are the participants. Students will be required to complete a PowerPoint Presentation with notes, that if presented would extend to around 10 to 20 minutes (10 slides +/-).

The PowerPoint, must contain Speaker Notes as bullet points with appropriate references within the speakers notes section for each slide.

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, PowerPoint structure and organisation.

Total: 800 - 1200 words

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.

Task 2

Due: **Week 5**
Weighting: **30%**

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 2010) cyber attack event (in Australia or overseas) and investigate if this is a cyber terror attack or a simple mislabelling of the incident.

1500 - 2000 words.

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

Task 3

Due: **Week 12**
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 ISC2.

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.
- 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

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.

REQUIRED READINGS

§ The citations for all the required readings for this unit are available to enrolled students 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.

RECOMMENDED READINGS

§ Recommended readings will be posted to the unit iLearn site as Session 1 progresses.

§ Students may consider obtaining a copy of the following book, Richards, D., and Mills, G., (eds) *Victory Among People: Lessons from Countering Insurgency and Stabilising Fragile States,* RUSI, London, 2011. Students have previously found downloading an electronic version on to an E-Book to be an effective means by which the book can be acquired.

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.

§ The unit can only be accessed by enrolled students online through http://ilearn.mq.edu.au

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.

§ All assessment tasks will be subject to a 'TurnitIn' review as an automatic part of the submission process.

§ A plagiarism declaration is automatically completed when work is submitted through "turnitin". This removes the need to submit a coversheet declaration.

§ The granting of extensions of up to one week are at the discretion of the unit convenor. 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 special consideration. The policy for this is detailed under Policy and Procedures.

LATE SUBMISSION OF ASSESSMENT TASKS

There is a penalty for the the late submission of assessment tasks. If an assignment is submitted late it will initially be marked as if it had been submitted on time. However, **5%**of the weighting allocated for the assignment will then be deducted from the mark the student initially achieves in the assessment task for each day it is late. For example if the assessment task's weighting is 20, 1.00 mark per day will be deducted from the initial mark given per day it is late ie a task initially given 15/20 but which is submitted four days late will lose 4 x 1.00 marks. That means 15/20-4marks=11/20.

It is this second mark which will be recorded in gradebook.

The same principle applies if a student seeks and is granted an extension and the assessment task is submitted later than the amended submission date.

Unit Schedule

As advised within iLearn

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

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

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/

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://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 - 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

- Task 1
- Task 2
- Task 3

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.
- 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

- Task 1
- Task 2
- Task 3

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.
- 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

- Task 1
- Task 2
- Task 3

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

- Task 1
- Task 2
- Task 3

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

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 treats from their use of current day technology.
- Conceptualise the 'human factor' in dealing with cyber terrorist.
- 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

- Task 1
- Task 2
- Task 3