PICT808

Information Warfare and Cyberterrorism

S1 Evening 2013

Centre for Policing, Intelligence and Counter Terrorism

Contents

General Information

Unit convenor and teaching staff
Other Staff
Milton Baar
milton.baar@mq.edu.au
Contact via milton.baar@mq.edu.au

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 cyberterrorist threats might be conceived in different horizontal applications, network and protocol layers. The unit explores how different vertical industries (eg, the finance industry) face specific treats from their use of specific protocols and platforms. The 'human factor' in dealing with cyberterrorist 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 the characteristics and concepts of both information warfare and cyber terrorism

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

Evaluate the significance and relevance of information; to integrate and synthesise information; and represent it in an accurate and fully attributed manner

Produce high quality written work that is clear, concise, coherent and logically structured, and that reflects a comprehensive understanding of the subject matter

Develop and effectively communicate a reasoned, balanced, persuasive and original perspective/argument

Assessment Tasks

Name	Weighting	Due
Task 1	20%	Weekly
Task 3	20%	Week 5
Task 2	20%	Weeks 3, 7 10 & 13
Task 4	40%	Week 12

Task 1

Due: **Weekly**
Weighting: **20%**

Participate as follows:

For internal students attending face-to-face sessions at the designated weekly time and location. To obtain maximum marks, students need to attend a minimum of 10 classes and actively participate in class discussions.

For external students participation in the online discussions on iLearn. To obtain maximum marks, students need to actively contribute valid discussion to at least 10 of the weekly discussions. To be valid the discussion must be from the Monday of the scheduled week, through to the Tuesday of the following week.

On successful completion you will be able to:

- Understand the characteristics and concepts of both information warfare and cyber terrorism
- Critically examine and interpret Australian and International sources when analysing information warfare and cyber terrorism, information

- Evaluate the significance and relevance of information; to integrate and synthesise information; and represent it in an accurate and fully attributed manner
- Produce high quality written work that is clear, concise, coherent and logically structured, and that reflects a comprehensive understanding of the subject matter
- Develop and effectively communicate a reasoned, balanced, persuasive and original perspective/argument

Task 3

Due: **Week 5**
Weighting: **20%**

Students are required to 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. A 1500 word essay is required.

On successful completion you will be able to:

- Understand the characteristics and concepts of both information warfare and cyber terrorism
- Evaluate the significance and relevance of information; to integrate and synthesise information; and represent it in an accurate and fully attributed manner
- Produce high quality written work that is clear, concise, coherent and logically structured, and that reflects a comprehensive understanding of the subject matter
- Develop and effectively communicate a reasoned, balanced, persuasive and original perspective/argument

Task 2

Due: **Weeks 3, 7 10 & 13**
Weighting: **20%**

Each week there is a recommended reading supplied; these may be used as the basis of a short review of no more than 250 words plus references. Alternately, students may select a different academic paper in the cybercrime field and review and comment on that paper.

Students must complete four reviews, each worth a maximum of 5 marks.

On successful completion you will be able to:

- Understand the characteristics and concepts of both information warfare and cyber terrorism
- Critically examine and interpret Australian and International sources when analysing information warfare and cyber terrorism, information

- Evaluate the significance and relevance of information; to integrate and synthesise information; and represent it in an accurate and fully attributed manner
- Produce high quality written work that is clear, concise, coherent and logically structured, and that reflects a comprehensive understanding of the subject matter
- Develop and effectively communicate a reasoned, balanced, persuasive and original perspective/argument

Task 4

Due: **Week 12**
Weighting: **40%**

Complete a 3000 word cyber terrorism ready reaction plan

Further details and the assessment rubric will be published on iLearn.

Assignment Submission

Detailed assessment criteria is available to all enrolled students through the Unit iLearn site.

All assignments except for the participation component, are to be submitted through iLearn and are to contain a cover sheet as indicated in the unit guide.

Late Assignments

If an assignment is submitted late, 5% of the available mark will be deducted for each day the paper is late. For example, if the paper is worth 20 marks, 1.00 mark per day will be deducted from the mark given (ie. A student given 15/20 who submitted 4 days late will lose 4 x 1.00 marks: 15/20 – 4 marks = 11/20) The same principle applies if an extension is granted and the assignment is submitted later than the amended date.

Technology Requirements

Online units can be accessed at: http://ilearn.mq.edu.au

PC and Internet access are required. Basic computer skills (e.g., internet browsing) and skills in word processing are also a requirement.

Please consult teaching staff for any further, more specific requirements.

Workload

This is a 4 credit point unit, which equates to a 12 hour workload per week.

On successful completion you will be able to:

- Understand the characteristics and concepts of both information warfare and cyber terrorism
- Critically examine and interpret Australian and International sources when analysing information warfare and cyber terrorism, information
- Evaluate the significance and relevance of information; to integrate and synthesise information; and represent it in an accurate and fully attributed manner
- Produce high quality written work that is clear, concise, coherent and logically structured, and that reflects a comprehensive understanding of the subject matter
- Develop and effectively communicate a reasoned, balanced, persuasive and original perspective/argument

Delivery and Resources

Required and Recommended texts and/or materials

Required and recommended reading is contained in iLearn for enrolled students. These readings are accessible through the Macquarie Library and are held on E-Reserve.

Unit Schedule

Module	Week Commencing	Topic
1	27 Feb	**Introduction to Information Warfare and Cyber Terrorism** An introduction to the unit and a discussion on some of the key elements that transgress from a crime through to full on cyber terrorism. · What is a crime? · What is cyber crime? · What is war? · What is information warfare? · What is terrorism? · What is cyber terrorism? · Why are these different to “hacktivism”? · Does cyber crime lead to cyber terrorism?

2	6 Mar	**Characteristics of Cyber Crime** This week reviews cyber crime and how it can fit within the ambient of most other crimes. This week will examine the following: · Computer Crime Technology · Computer Crime on the Internet · Financial Computer Crime · White-Collar Computer Crime · Crime Offender or Victim · Fake Websites · Money Laundering · Bank Fraud · Advance Fee Fraud
3	13 Mar	**Characteristics of Information Warfare** Information warfare is something that has been in existence for a long time, even since the World Wars. It can now be a war fought on its own. · The concepts of Information warfare · Deny, disrupt & steal · Motivation for attacks · Short term versus long term implications · Defensive acts can disclose intelligence · The impact of the ever changing face of technology · Information warfare in an insurgent war · Internal and external contributing factors
4	20 Mar	**Characteristics of Cyber Terrorism I** Review cyber terrorism and its definition, public perception and “real world” occurrences. · Does cyber terrorism exist? · What are the characteristics of cyber terrorism? · Does there need to be loss of life for it to exist? · Direct and indirect attacks. · What are the key components of a cyber terror attack?

5	27 Mar	**Characteristics of Cyber Terrorism II** · The perpetrator · Place · Action · Tool · Target · Affiliation · Motivation · Known real world incidents
6	3 Apr	**Information Security** Security is a need and not a want and comes at a cost. Some entities take the risk and run with as little security as they are able to get by with. This is a disaster waiting to happen. · What is C.I.A. · What are the key components of information security? · Can we really be secure? · What must be done to be secure? · Physical v virtual security. · Who, what or where are the weakest links?
7	10 Apr	**Preventative Planning** Review of the critical need to have accurate and updated contingency plans · If you fail to plan you plan to fail · Types of contingency plans · Types of organisations that must have one · What is needed in a Cyber Terrorism ready reaction plan · Who is responsible to manage the plan · Levels of criticality · Plan authentication and validation
8	1 May	**Critical Infrastructure** Review who and what really are elements that make up the critical infrastructure · Utilities · Technology · Transport · Finance · Sustenance · Government · The domino effect, should one fall the others will follow

9	8 May	**SCADA Systems** Most critical infrastructure is now managed by SCADA systems, the link between internal and external systems. Should you control the SCADA, you control the infrastructure. · What is SCADA · Why is it so important · What are the risks · Can we bypass and ring fence critical infrastructure · Who's who in the zoo
10	15 May	**The Dark Net** Review of the emerging internet underworld, where drugs, human trafficking, murders and terrorist acts can all be obtained. · What is the dark net? · How can we control it? · Given it now has its own currency, have we already lost control? · Can our total dependence on information technology be our generations biggest downfall? · The dark net could mutate and the underworld generate insurgent cyber attacks, causing an economic impact on the developed world
11	22 May	**Behaviour: Social Engineering** Humans are often the weakest link in information security, as the assumptions underlying security models routinely prove to be infeasible in the real world. For example, users often scribble down their passwords, or use the same password for every service. This session will examine the most common human factors weaknesses in secure systems and strategies to overcome them. · Social engineering in security attacks · Human factors in security · Internal versus external threats · Password control · Social psychological aspects of computer security · Social networking
12	29 May	Post Attack Recovery Recovery post attack is critical in any disaster recovery, but if the attack is still resident, systems will only fail again. · Follow the plan · Locate the source of the attack · Fail safe switch over · Monitor recovery traffic · Post incident reflection · Why did it happed · Who is to blame · Change not blame

13	5 Jun	The Future – New Threats on the Horizon? The arena of information warfare and cyber terrorism has been characterised as an arms race, with both sides gaining a temporary advantage but then losing it to the other side. We will investigate concepts and review developments on both sides. · Security is expensive and often a need and not a want, should we stop and rebuild with a security mindset? · The new threat, mobility of technology · With even greater bandwidth on the horizon, will our further reliance be our demise? · With international boundaries being nonexistent with internet traffic, who will take control? · What impact is the cloud going to have, should they become a cyber terror attack? · Could Australia be sustainable without external communications? · How real is a future cyber terror attack?

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://www.mq.edu.au/policy/docs/academic_honesty/policy.html

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

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

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

Grievance Management Policy http://mq.edu.au/policy/docs/grievance_management/policy.html

Special Consideration Policy http://www.mq.edu.au/policy/docs/special_consideration/policy.html

In addition, a number of other policies can be found in the Learning and Teaching Category of Policy Central.

Student Support

Macquarie University provides a range of Academic Student Support Services. Details of these services can be accessed at: http://students.mq.edu.au/support/

UniWISE provides:

- Online learning resources and academic skills workshops http://www.students.mq.edu.au/support/learning_skills/
- Personal assistance with your learning & study related questions.
- The Learning Help Desk is located in the Library foyer (level 2).
- Online and on-campus orientation events run by Mentors@Macquarie.

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

Details of these services can be accessed at http://www.student.mq.edu.au/ses/.

IT Help

If you wish to receive IT help, we would be glad to assist you at 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 and it outlines what can be done.

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

- Understand the characteristics and concepts of both information warfare and cyber terrorism
- Critically examine and interpret Australian and International sources when analysing information warfare and cyber terrorism, information

Assessment tasks

- Task 1
- Task 3
- Task 2
- Task 4

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

- Critically examine and interpret Australian and International sources when analysing

information warfare and cyber terrorism, information

- Evaluate the significance and relevance of information; to integrate and synthesise information; and represent it in an accurate and fully attributed manner

Assessment tasks

- Task 1
- Task 3
- Task 2
- Task 4

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 the significance and relevance of information; to integrate and synthesise information; and represent it in an accurate and fully attributed manner
- Produce high quality written work that is clear, concise, coherent and logically structured, and that reflects a comprehensive understanding of the subject matter
- Develop and effectively communicate a reasoned, balanced, persuasive and original perspective/argument

Assessment tasks

- Task 1
- Task 3
- Task 4

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 the characteristics and concepts of both information warfare and cyber

terrorism
- Critically examine and interpret Australian and International sources when analysing information warfare and cyber terrorism, information
- Evaluate the significance and relevance of information; to integrate and synthesise information; and represent it in an accurate and fully attributed manner
- Produce high quality written work that is clear, concise, coherent and logically structured, and that reflects a comprehensive understanding of the subject matter
- Develop and effectively communicate a reasoned, balanced, persuasive and original perspective/argument

Assessment tasks

- Task 1
- Task 3
- Task 2
- Task 4

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

- Produce high quality written work that is clear, concise, coherent and logically structured, and that reflects a comprehensive understanding of the subject matter
- Develop and effectively communicate a reasoned, balanced, persuasive and original perspective/argument

Assessment task

- Task 2

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 the characteristics and concepts of both information warfare and cyber terrorism
- Critically examine and interpret Australian and International sources when analysing information warfare and cyber terrorism, information

Assessment tasks

- Task 3
- Task 4