PICT840

Cyber Crime

S2 External 2014

Centre for Policing, Intelligence and Counter Terrorism

Contents

General Information	2
Learning Outcomes	2
Assessment Tasks	3
Delivery and Resources	4
Unit Schedule	7
Learning and Teaching Activities	8
Policies and Procedures	8
Graduate Capabilities	9

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 MCompForens or PGDipCompForens or PGCertCompForens

Corequisites

Co-badged status

Unit description
Cybercrime refers to an array of criminal activity including offences against computer data and systems, computer-related offences, content offences, and copyright offences. While early computer hackers were more interested in youthful exploration, modern cybercrime is increasingly about criminal profit and this is reflected in the involvement of transnational organised crime groups. This unit will explore the types of cybercrime, the perpetrators, and investigation techniques.

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:

A. Interpret the various aspects of Cyber crime theory and what constitutes criminal and noncriminal offending

B. Classify different incidents into the main cyber crime categories

C. Identify the perpetrators and recognise the threat level each play in the cyber crime

environment

D. Translate theory into practice when interpreting the various core investigation techniques

E. Assess relevant counter measures and their legality in performing such acts on both local and international targets

Assessment Tasks

Name	Weighting	Due
PowerPoint presentation	20%	Week 4
Research Essay	30%	Week 8
Investigation Plan	50%	Week 12

PowerPoint presentation

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

Review the unit reference material and other suitable sources to create a presentation on various aspects of Cyber crime theory and what constitutes criminal and noncriminal offending and which of the main categories they fall into. 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.

On successful completion you will be able to:

- A. Interpret the various aspects of Cyber crime theory and what constitutes criminal and noncriminal offending
- B. Classify different incidents into the main cyber crime categories

Research Essay

Due: **Week 8**
Weighting: **30%**

The question on whether state nations or even larger organisations who are the victims of a cyber attack should be able to launch a destructive counter attack, raises many issues.

Students need to conduct in-depth research on what the issues are, legally, technically and the risks imposed by conducting such counter attacks. They should then prepare an essay based on their findings. Word length 1500 to 2000 words.

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:

- C. Identify the perpetrators and recognise the threat level each play in the cyber crime environment
- E. Assess relevant counter measures and their legality in performing such acts on both local and international targets

Investigation Plan

Due: **Week 12**
Weighting: **50%**

It is critical that students understand the various aspects of cyber crime theory. It is equally critical that students further be able implement this into practice. This assessment will test students understanding of the relevant cyber crime theory and demonstrate their understanding when putting it into practice, as demonstrated with the production of a pre-investigation plan and written orders (SMEAC). A scenario will be published in iLearn during the Session.

Word length 3000 words.

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.

On successful completion you will be able to:

- A. Interpret the various aspects of Cyber crime theory and what constitutes criminal and noncriminal offending
- B. Classify different incidents into the main cyber crime categories
- C. Identify the perpetrators and recognise the threat level each play in the cyber crime environment
- D. Translate theory into practice when interpreting the various core investigation techniques

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.

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

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.

RECOMMENDED READINGS

- Computer Forensics, Electronic Discovery and Electronic Evidence

  Stanfield, A; LexisNexis Butterworths, Sydney, 2009

- Journal of Digital Forensics and Law (JDFSL) (http://www.jdfsl.org/index.htm)
- Criminal Profiling: an introduction to behavioural evidence analysis (4th Edition), Turvey, B; Elsevier 2012
- International Journal of Cyber Criminology (http://www.cybercrimejournal.com/)

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. The Department process for the reassessment of assignments for marking during the semester is as follows:

- You must consult with the unit convenor - A reassessment will only be granted if you have sought and received feedback about your performance on the assessment from the convenor.
- Apply to PICT's Director of Learning and Teaching (or delegated authority) for a reassessment - no more than 7 days after the unit convenor or class tutor has returned the assessment to you. You must make a sound academic case, which demonstrates that you have consulted the unit convenor and as a result of this there is evidence that either the marking criteria were not provided, or there is insufficient feedback to justify the mark given.
- If appropriate, the Head of Department (or delegated authority) will organise the reassessment of work.
- The mark determined after reassessment will be the final mark in that assessment task, and this mark can be lower than the original.

Unit Schedule

Week 1	**Introduction and Unit Overview** • Introductions • Course Organisation • Learning Approach • Assessment • Expectations • Cyber Crime defined
Week 2	**Cyber Crime Cases**
Week 3	**Cyber Criminals**
Week 4	**Cyber Law I**
Week 5	**Cyber Law II**
Week 6	**Counter Measures**
Week 7	**Pre Investigation Planning/Management**
Week 8	**Scene Attendance**

Week 9	**Digital Forensics I**
Week 10	**Digital Forensics II & Mobile Forensics**
Week 11	**e.discovery**
Week 12	**Cyber Space Investigations**
Week 13	**Future trends**

Learning and Teaching Activities

Unit Description

Cyber crime refers to an array of criminal activity including offences against computer data and systems, computer-related offences, content offences, and copyright offences. While early computer hackers were more interesting in youthful exploration, modern cyber crime is increasingly about criminal profit and this is reflected in the involvement of transnational organised crime groups. This unit will explore the types of cyber crime, the perpetrators, investigation techniques, and counter measures.

Expectations

To achieve a successful result, it is expected that you should spend, on average, at least 12 hours per week on this unit. This time should be spent on the following activities: • Reading any prescribed texts; • Keeping up to date on current events in cyber crime; • Actively engage with other students to share knowledge • Undertaking the necessary research for the assignments.

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

- A. Interpret the various aspects of Cyber crime theory and what constitutes criminal and noncriminal offending
- B. Classify different incidents into the main cyber crime categories
- C. Identify the perpetrators and recognise the threat level each play in the cyber crime environment
- D. Translate theory into practice when interpreting the various core investigation techniques
- E. Assess relevant counter measures and their legality in performing such acts on both local and international targets

Assessment tasks

- PowerPoint presentation
- Research Essay
- Investigation 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

- A. Interpret the various aspects of Cyber crime theory and what constitutes criminal and noncriminal offending
- B. Classify different incidents into the main cyber crime categories
- C. Identify the perpetrators and recognise the threat level each play in the cyber crime environment
- D. Translate theory into practice when interpreting the various core investigation techniques
- E. Assess relevant counter measures and their legality in performing such acts on both local and international targets

Assessment tasks

- PowerPoint presentation
- Research Essay

- Investigation 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

- A. Interpret the various aspects of Cyber crime theory and what constitutes criminal and noncriminal offending
- B. Classify different incidents into the main cyber crime categories
- C. Identify the perpetrators and recognise the threat level each play in the cyber crime environment
- D. Translate theory into practice when interpreting the various core investigation techniques
- E. Assess relevant counter measures and their legality in performing such acts on both local and international targets

Assessment tasks

- PowerPoint presentation
- Research Essay
- Investigation 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

- A. Interpret the various aspects of Cyber crime theory and what constitutes criminal and noncriminal offending
- B. Classify different incidents into the main cyber crime categories
- C. Identify the perpetrators and recognise the threat level each play in the cyber crime environment
- D. Translate theory into practice when interpreting the various core investigation

techniques

- E. Assess relevant counter measures and their legality in performing such acts on both local and international targets

Assessment tasks

- PowerPoint presentation
- Research Essay
- Investigation 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 outcome

- D. Translate theory into practice when interpreting the various core investigation techniques

Assessment tasks

- PowerPoint presentation
- Investigation 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

- A. Interpret the various aspects of Cyber crime theory and what constitutes criminal and noncriminal offending
- B. Classify different incidents into the main cyber crime categories
- C. Identify the perpetrators and recognise the threat level each play in the cyber crime environment
- D. Translate theory into practice when interpreting the various core investigation techniques

- E. Assess relevant counter measures and their legality in performing such acts on both local and international targets

Assessment tasks

- PowerPoint presentation
- Research Essay
- Investigation Plan