PICT954

Simulation in Cyber Security

S2 Evening 2019

Department of Security Studies and Criminology

Contents

General Information

Unit convenor and teaching staff
Yves-Heng Lim
yves-heng.lim@mq.edu.au

Fred Smith
fred.smith@mq.edu.au

Credit points
4

Prerequisites
(Admission to MCyberSec or MSecStrategicStudMCyberSec or MIntellMCyberSec or MCyberSecMCTerrorism or MCyberSecMCrim) and 24cp at 800 level or above

Corequisites
PICT848 and PICT812

Co-badged status

Unit description
This unit provides students with an opportunity to apply the knowledge they have gain throughout their program of study to a real world crisis. By participating in a dynamic simulation, students will be required to solve problems and find solutions to real world challenges. Students will be assigned to an executive team that includes students with different skill sets and knowledge. These executive teams may include strategists, intelligence analysts, criminologists, counter terrorism experts, and cyber security analysts. Students enrolled in Simulation in Cyber Security will perform the role of the cyber security analyst. Their mission will be to formulate solutions by employing the academic, research, analysis and workplace skills they acquired throughout their program. In particular, they will be required to use their knowledge of cyber security suites –including offensive tools– to provide detailed assessments of the evolving situation/scenario. They will also be responsible for the cyber security sections of ministerial briefing papers that each group will have to provide as part of their assessment tasks. The student will be required to make policy recommendations based on his assessment of the situation.

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:

1. Understand the strengths and weaknesses of simulation & role playing as an educational and professional tool.
2. Understand decision-making, bargaining situations and group dynamics in a political-strategic context.
3. Use tools and software commonly used to attack/protect networks in complex and evolving real-world situations.
4. Communicate disciplinary knowledge to professional audiences through the Cyber Security sections of the briefing papers.

Assessment Tasks

Name	Weighting	Hurdle	Due
Quiz.	10%	No	Week 3
Simulation Week 4 and Week 7	10%	No	Week 4 and Week 7
Ministerial Brief/Memo	45%	No	Week 9
Simulation	35%	Yes	Week 12

Quiz.

Due: **Week 3**
Weighting: **10%**

Covering Subject Matter (lectures and readings) in Weeks 1, 2 & 3.

On successful completion you will be able to:

- 1. Understand the strengths and weaknesses of simulation & role playing as an educational and professional tool.
- 2. Understand decision-making, bargaining situations and group dynamics in a political-strategic context.

Simulation Week 4 and Week 7

Due: **Week 4 and Week 7**
Weighting: **10%**

On week 4 and week 7, students will participate in two small-scale war games.

All students are required to make at least three posts on the dedicated forums.

Please refer to iLearn for additional details.

On successful completion you will be able to:

- 1. Understand the strengths and weaknesses of simulation & role playing as an educational and professional tool.

Ministerial Brief/Memo

Due: **Week 9**
Weighting: **45%**

Group assignment.

Working as part of a team tasked with writing a ministerial brief/memo on a security and criminology-related scenario, write a 'Cyber Threat assessment' and contribute to the executive summary and recommendations in that assessment.

Individual contribution (40%): Cyber Threat Assessment: 2,500 word policy memo.

Group grade (5%): The Ministerial Brief/Memo will include an executive summary (500 words) and policy recommendations (500 words) that are written collaboratively by your team.

Please refer to Ilearn for details.

On successful completion you will be able to:

- 3. Use tools and software commonly used to attack/protect networks in complex and evolving real-world situations.
- 4. Communicate disciplinary knowledge to professional audiences through the Cyber Security sections of the briefing papers.

Simulation

Due: **Week 12**
Weighting: **35%**
This is a hurdle assessment task (see assessment policy for more information on hurdle assessment tasks)

Group assignment.

Hurdle Assessment.

Internal:

In Week 12, each student team will be presented with a war gaming scenario. Each team will be required to provide policy recommendations to the control group (convenors) as the situation unfolds over a number of simulation moves or turns.

Individual (25%): At the end of each turn, you will present a Decision Brief (Cyber Security) to the control team.

Group (5%): At the end of each turn, your team will present a synthesis of the decisions made by the team.

Peer grading (5%): At the end of the simulation, students will grade the performance of other members of their team.

External:

In Week 12, each student team will be presented with a war gaming scenario. Each team will be required to provide policy recommendations to the control group (convenors) as the situation unfolds over a number of simulation moves or turns.

The simulation will be run over a two week period during Weeks 12 and 13, with a set-time turn structure.

Individual (25%): At the end of each turn, you will present a Decision Brief (Cyber Security) to the control team.

Group (5%): At the end of each turn, your team will present a synthesis of the decisions made by the team.

Peer grading (5%): At the end of the simulation, students will grade the performance of other members of their team.

Please refer to iLearn for additional details.

On successful completion you will be able to:

- 1. Understand the strengths and weaknesses of simulation & role playing as an educational and professional tool.
- 2. Understand decision-making, bargaining situations and group dynamics in a political-strategic context.
- 3. Use tools and software commonly used to attack/protect networks in complex and evolving real-world situations.
- 4. Communicate disciplinary knowledge to professional audiences through the Cyber Security sections of the briefing papers.

Delivery and Resources

DELIVERY AND RESOURCES

UNIT REQUIREMENTS AND EXPECTATIONS

- You should spend an average of 12 hours per week on this unit. This includes listening

to lectures prior to seminar or tutorial, reading weekly required materials as detailed in iLearn, participating in Ilearn discussion forums and preparing assessments.

- Internal students are expected to attend all seminar or tutorial sessions, and external students are expected to make significant contributions to on-line activities.
- In most cases students are required to attempt and 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 site. Electronic copies of required readings may be accessed through the library or will be made available by other means.

TECHNOLOGY USED AND REQUIRED

- Computer 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.
- Information about IT used at Macquarie University is available at http://students.mq.edu.au/it_services/

SUBMITTING ASSESSMENT TASKS

- All text-based assessment tasks are to be submitted, marked and returned electronically. This will only happen through the unit iLearn site.
- Assessment tasks must be submitted as a 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 is subject to the university's Special Consideration Policy. Extensions will not be granted by unit conveners or tutors, but must be lodged through Special Consideration: https://students.mq.edu.au/study/my-study-program/special-consideration

LATE SUBMISSION OF ASSESSMENT TASKS

Unless a Special Consideration request has been submitted and approved, (a) **a penalty for lateness will apply** – two (2) marks out of 100 will be deducted per day for assignments submitted after the due date – and (b) **no assignment will be accepted seven (7) days (incl. weekends) after the original submission deadline**. No late submissions will be accepted for timed assessments – e.g. quizzes, online tests.

WORD LIMITS FOR ASSESSMENT TASKS

- Stated word limits include footnotes and footnoted references, but not 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 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://www.mq.edu.au/policy/docs/gradeappeal/policy.html
- In accordance with the Grade Appeal Policy, individual works are not subject to regrading.

STAFF AVAILABILITY

- Department staff will endeavour to answer student enquiries in a timely manner. However, emails or iLearn messages will not usually be answered over the weekend or public holiday period.
- Students are encouraged to read the Unit Guide and look at instructions posted on the iLearn site before sending email requests to staff.

Unit Schedule

Week 1. Introduction.

Week 2. Simulations and Wargames: an Overview.

Week 3. Decision biases and blind spots.

Week 4. Mini-simulation I.

Week 5. Decision-making and leadership.

Week 6. "The 'I' in Team"

Week 7. Mini-simulation II.

Week 13 (Saturday and Sunday). Simulation.

Policies and Procedures

Macquarie University policies and procedures are accessible from Policy Central (https://staff.mq.edu.au/work/strategy-planning-and-governance/university-policies-and-procedures/policy-central). Students should be aware of the following policies in particular with regard to Learning and Teaching:

- Academic Appeals Policy
- Academic Integrity Policy
- Academic Progression Policy
- Assessment Policy
- Fitness to Practice Procedure
- Grade Appeal Policy
- Complaint Management Procedure for Students and Members of the Public
- Special Consideration Policy *(**Note:** The Special Consideration Policy is effective from 4 December 2017 and replaces the Disruption to Studies Policy.)*

Undergraduate students seeking more policy resources can visit the Student Policy Gateway (https://students.mq.edu.au/support/study/student-policy-gateway). It is your one-stop-shop for the key policies you need to know about throughout your undergraduate student journey.

If you would like to see all the policies relevant to Learning and Teaching visit Policy Central (https://staff.mq.edu.au/work/strategy-planning-and-governance/university-policies-and-procedures/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/study/getting-started/student-conduct

Results

Results published on platform other than eStudent, (eg. iLearn, Coursera etc.) 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 or if you are a Global MBA student contact globalmba.support@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

If you are a Global MBA student contact globalmba.support@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

- 1. Understand the strengths and weaknesses of simulation & role playing as an educational and professional tool.
- 2. Understand decision-making, bargaining situations and group dynamics in a political-strategic context.
- 3. Use tools and software commonly used to attack/protect networks in complex and evolving real-world situations.
- 4. Communicate disciplinary knowledge to professional audiences through the Cyber Security sections of the briefing papers.

Assessment tasks

- Quiz.
- Simulation Week 4 and Week 7
- Ministerial Brief/Memo
- Simulation

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

- 3. Use tools and software commonly used to attack/protect networks in complex and evolving real-world situations.
- 4. Communicate disciplinary knowledge to professional audiences through the Cyber Security sections of the briefing papers.

Assessment tasks

- Ministerial Brief/Memo
- Simulation

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

- 1. Understand the strengths and weaknesses of simulation & role playing as an educational and professional tool.
- 2. Understand decision-making, bargaining situations and group dynamics in a political-strategic context.
- 3. Use tools and software commonly used to attack/protect networks in complex and evolving real-world situations.

Assessment tasks

- Quiz.
- Simulation Week 4 and Week 7
- Ministerial Brief/Memo
- Simulation

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

- 1. Understand the strengths and weaknesses of simulation & role playing as an educational and professional tool.
- 2. Understand decision-making, bargaining situations and group dynamics in a political-strategic context.
- 3. Use tools and software commonly used to attack/protect networks in complex and evolving real-world situations.

Assessment tasks

- Quiz.
- Simulation Week 4 and Week 7
- Ministerial Brief/Memo
- Simulation

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

- 1. Understand the strengths and weaknesses of simulation & role playing as an educational and professional tool.
- 2. Understand decision-making, bargaining situations and group dynamics in a political-strategic context.
- 4. Communicate disciplinary knowledge to professional audiences through the Cyber Security sections of the briefing papers.

Assessment tasks

- Quiz.
- Simulation Week 4 and Week 7
- Ministerial Brief/Memo
- Simulation

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

- 1. Understand the strengths and weaknesses of simulation & role playing as an educational and professional tool.
- 2. Understand decision-making, bargaining situations and group dynamics in a political-strategic context.

Assessment tasks

- Quiz.
- Simulation Week 4 and Week 7
- Simulation