



UNSW Course Outline

ZEIT8035 Cyber Terrorism - 2024

Published on the 27 Jun 2024

General Course Information

Course Code : ZEIT8035

Year : 2024

Term : Semester 2

Teaching Period : Z2

Is a multi-term course? : No

Faculty : UNSW Canberra

Academic Unit : School of Systems and Computing

Delivery Mode : Online

Delivery Format : Standard

Delivery Location : UNSW Canberra at ADFA

Campus : UNSW Canberra

Study Level : Postgraduate

Units of Credit : 6

Useful Links

[Handbook Class Timetable](#)

Course Details & Outcomes

Course 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 course will present a high-level overview of how cyber terrorist threats and foreign states, might infiltrate systems and gain control of critical infrastructure. The course 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.

Course Aims

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. The aims of this course are:

- present a high-level overview of how cyber terrorist threats and foreign states might infiltrate systems and gain control of critical infrastructure.
- explore how different vertical industries face specific threats from their use of current day technology.
- explore the 'human factor' in dealing with cyber terrorist threats

Course Learning Outcomes

Course Learning Outcomes
CLO1 : Describe the fundamental principles, key concepts, vital components and definitions of cyber terrorism and cyber war
CLO2 : Compare and contrast cyber terrorism and other forms of terrorism
CLO3 : Understand how terrorists make use of the global communications network to advance their agendas
CLO4 : Evaluate the adequacy of practical approaches to deter, identify and respond to cyber terrorist attacks

Course Learning Outcomes	Assessment Item
CLO1 : Describe the fundamental principles, key concepts, vital components and definitions of cyber terrorism and cyber war	<ul style="list-style-type: none">• Online Discussion• Essay
CLO2 : Compare and contrast cyber terrorism and other forms of terrorism	<ul style="list-style-type: none">• Discussion Summary• Policy Brief• Online Discussion• Essay
CLO3 : Understand how terrorists make use of the global communications network to advance their agendas	<ul style="list-style-type: none">• Discussion Summary• Policy Brief• Essay
CLO4 : Evaluate the adequacy of practical approaches to deter, identify and respond to cyber terrorist attacks	<ul style="list-style-type: none">• Essay

Learning and Teaching Technologies

Moodle - Learning Management System | Blackboard Collaborate

Learning and Teaching in this course

This course uses a variety of teaching strategies that have been developed by your course convenor over many years of experience in previous academic institutions and in industry.

The concepts presented in this course require you to demonstrate skills including structured thinking and decision making in dealing with complex problems. Therefore, the teaching strategies we use aim to provide an engaging and rewarding educational environment to facilitate your learning experiences through developing your expertise in applying cyber security concepts and principles.

The lecture notes provided are synthesized from the required text book and other sources, and are divided into modules to facilitate structured and scheduled studying activities. We provide a course guide to help you understand the connection between the study materials and assignments.

This course is delivered in distance mode and uses Moodle. Instructions will be provided for each module in the course Moodle, explaining what is expected within each topic.

We expect all students to use Moodle, which provides mechanisms to facilitate on-line discussions between students and with the lecturer.

We encourage you to log on to Moodle on a regular basis for updates relating to the course. We expect that you will study as much of the recommended reading material as you can, as well as expanding your reading through the linked references and your own research, reflecting on the studied material and thinking outside the box to comprehend the concepts and techniques taught in this course.

Assessments

Assessment Structure

Assessment Item	Weight	Relevant Dates
Online Discussion Assessment Format: Individual Short Extension: Yes (7 days)	15%	Due Date: 03/08/2024 11:59 PM
Discussion Summary Assessment Format: Individual Short Extension: Yes (7 days)	15%	Due Date: 31/08/2024 11:59 PM
Policy Brief Assessment Format: Individual Short Extension: Yes (7 days)	20%	Due Date: 21/09/2024 11:59 PM
Essay Assessment Format: Individual Short Extension: Yes (7 days)	50%	Due Date: 26/10/2024 11:59 PM

Assessment Details

Online Discussion

Course Learning Outcomes

- CLO1 : Describe the fundamental principles, key concepts, vital components and definitions of cyber terrorism and cyber war
- CLO2 : Compare and contrast cyber terrorism and other forms of terrorism

Detailed Assessment Description

Online Discussion will assess students' knowledge gained during study weeks.

Discussion Summary

Course Learning Outcomes

- CLO2 : Compare and contrast cyber terrorism and other forms of terrorism
- CLO3 : Understand how terrorists make use of the global communications network to advance their agendas

Detailed Assessment Description

Presentation will assess students' ability to work individually on a problem question of choice (see Moodle for details)

Policy Brief

Course Learning Outcomes

- CLO2 : Compare and contrast cyber terrorism and other forms of terrorism
- CLO3 : Understand how terrorists make use of the global communications network to advance their agendas

Detailed Assessment Description

The Policy Brief will require you to provide advice to a government entity of your choice in regards to a range of different cyber terrorism issues (see Moodle for details).

Essay

Course Learning Outcomes

- CLO1 : Describe the fundamental principles, key concepts, vital components and definitions of cyber terrorism and cyber war
- CLO2 : Compare and contrast cyber terrorism and other forms of terrorism
- CLO3 : Understand how terrorists make use of the global communications network to advance their agendas
- CLO4 : Evaluate the adequacy of practical approaches to deter, identify and respond to cyber terrorist attacks

Detailed Assessment Description

The Essay will require deep research on a topic that will be provided. Online readings from books and papers will be provided in Moodle. This material, plus your additional searches on the internet, will provide essential preparation and background for this assignment.

General Assessment Information

Students will receive comments on their assessments within 10 business days of the submission date. Feedback to Forum 1 will be provided before 14 August. We encourage students to refer to the feedback provided and reflect on this for their next assignment. This will allow you to improve your assessments progressively in the light of critical feedback.

You will find more detailed information for each assessment item including deadlines for ongoing on-line activities on Moodle under the Assignment Information page.

Grading Basis

Standard

Requirements to pass course

The four assessment items form the requirements to complete this subject. To pass this course, students will need to achieve at least 50 marks out of a total of 100 marks.

All marks obtained for assessment items during the session are provisional. The final mark as published by the university following the assessment review group meeting is the only official mark.

From 2020 for all cyber Master courses major end- of semester assignments will not be released to the students until the course final results are reviewed by the school and approved.

Course Schedule

Teaching Week/Module	Activity Type	Content
Week 1 : 15 July - 19 July	Lecture	Introduction + What is Terrorism?
Week 2 : 22 July - 26 July	Lecture	Understanding, Locating and Constructing Cyber Terrorism
Week 3 : 29 July - 2 August	Lecture	Rethinking the Threat of Cyber Terrorism
	Activity	Online discussion 1: Due 03/08 at 11:59pm
Week 4 : 5 August - 9 August	Lecture	Putting the 'Cyber' into Cyber Terrorism
Week 5 : 12 August - 16 August	Lecture	Cyber War 1
Week 6 : 19 August - 23 August	Lecture	Cyber War 2
	Activity	Online Discussion 2: Due 24/08 at 11:59pm
	Presentation	Presentation: Due 31/08 at 11:59pm
Week 7 : 9 September - 13 September	Lecture	Policy Brief Workshop
Week 8 : 16 September - 20 September	Lecture	State Strategies for Contesting Cyber Terrorism
	Assessment	Policy Brief: Due 21/09 at 11:59pm
Week 9 : 23 September - 27 September	Lecture	Case Study: Sharp power? China & Russia's use of Cyberspace
Week 10 : 30 September - 4 October	Lecture	Case Study: Extremism Online
	Activity	Online Discussion 3: Due 05/10 at 11:59pm
Week 11 : 7 October - 11 October	Lecture	Australia's and Cyber Terrorism: threats and remedies
Week 12 : 14 October - 18 October	Workshop	Unit Summary + Essay Workshop
Week 13 : 21 October - 25 October	Assessment	No classes Essay Preparation. Essay due 26/10 at 11:59pm

Attendance Requirements

Students are strongly encouraged to attend all classes and review lecture recordings.

Course Resources

Prescribed Resources

This course uses a text which is available as an e-book from the UNSW Canberra library:

Cyber Terrorism Understanding, Assessment and Response

Authors: Chen, Jarvis, Macdonald ISBN 978-1-4939-0962-9 (eBook)

You will need continual access to this eBook to complete this course.

A variety of additional resource materials will also be made available. These comprise:

- Recommended papers and chapters from textbooks, internet based documents, and other sources. In general, these materials will be available through the Moodle page.
- Slides and presentation notes in the form of PowerPoint slides covering the material presented.

These will be made available through the Moodle page for this course.

ADFA Library has a Cyber Security subject guide:

<http://guides.lib.unsw.adfa.edu.au/cybersecurity>

Staff Details

Position	Name	Email	Location	Phone	Availability	Equitable Learning Services Contact	Primary Contact
	Siqi Ma					No	No
	Conor Keane					No	Yes

Other Useful Information

School-specific Information

The Learning Management System

Moodle is the Learning Management System used at UNSW Canberra. All courses have a Moodle site which will become available to students at least one week before the start of semester. Please find all help and documentation (including Blackboard Collaborate) at the Moodle Support page.

UNSW Moodle supports the following web browsers:

- Google Chrome 50+
- Safari 10+

Internet Explorer is not recommended. Addons and Toolbars can affect any browser's performance.

Operating systems recommended are:

- Windows 10,
- Mac OSX Sierra,
- iPad iOS10

Further details:

[Moodle System Requirements](#)

[Moodle Log In](#)

If you need further assistance with Moodle:

For enrolment and login issues please contact:

IT Service Centre

Email: itservicecentre@unsw.edu.au

Phone: (02) 9385-1333

International: +61 2 9385 1333

For all other Moodle issues please contact:

External TELT Support

Email: externalteltsupport@unsw.edu.au

Phone: (02) 9385-3331

International: +61 2 938 53331

Opening hours:

Monday – Friday 7:30am – 9:30 pm

Saturday & Sunday 8:30 am – 4:30pm

Study at UNSW Canberra

Study at UNSW Canberra has lots of useful information regarding:

- Where to get help
- Administrative matters
- Getting your passwords set up
- How to log on to Moodle
- Accessing the Library and other areas.

UNSW Canberra Student Hub

For News and Notices, Student Services and Support, Campus Community, Quick Links, Important Dates and Upcoming Events

School Contact Information

Deputy Head of School (Education): Dr Erandi Hene Kankanamge

E: e.henekankanamge@adfa.edu.au

T: 02 5114 5157

Syscom Admin Support: syscom@unsw.edu.au

T: 02 5114 5284

Syscom Admin Office: Building 15, Level 1, Room 101 (open 10am to 4pm, Mon to Fri)