



## UNSW Course Outline

# JURD7330 Cybercrime, Information Security and Digital Enforcement - 2024

Published on the 25 Aug 2024

## General Course Information

Course Code : JURD7330

Year : 2024

Term : Term 3

Teaching Period : T3

Is a multi-term course? : No

Faculty : Faculty of Law and Justice

Academic Unit : School of Law, Society and Criminology

Delivery Mode : In Person

Delivery Format : Standard

Delivery Location : Kensington

Campus : Sydney

Study Level : Postgraduate

Units of Credit : 6

### Useful Links

[Handbook Class Timetable](#)

## Course Details & Outcomes

### Course Description

This course examines the legal regulation of cybercrime, information security and digital

enforcement, with a focus on intellectual property and communications media.

Using a comparative and practical approach, the course surveys the explosion in crimes that use the resources of the internet, smart phones, artificial intelligence, drones and computers to achieve illegal goals. It explores new online crimes against computers, the data they contain, and the services they are used to deliver, such as hacking, denial of service attacks, digital extortion, and other challenges to critical infrastructure of the online world. It also examines the transformation of existing crimes – such as copyright piracy, economic espionage, identity theft, fraud, bullying, and extortion – into more serious and problematic challenges to law enforcement. The course considers how nation-states regulate unlawful activity in an environment that crosses international borders and increasingly involves activities on the dark net.

This is a fast developing area of law, and this will be reflected in the material studied in the course. Main cybercrime topics that are expected to be covered in the course include:

- the evolving nature of cybercrime, information security challenges and digital enforcement;
- national and international legal and policy frameworks;
- cyberbullying, cyberstalking and online harassment;
- electronic data and identity theft including biometric data;
- digital piracy, trademark counterfeiting, economic espionage and trade secret violations, and digital enforcement;
- attacks on infrastructure, including hacking, denial of services, ransomware and other forms of digital extortion;
- pornography and obscenity including child pornography, sexting and non-consensual pornography ('revenge porn');
- disinformation, misinformation (for example, fake news and deep fakes) and other forms of cyber-fraud;
- information security, including privacy and surveillance challenges;
- the use of cyberspace for terrorism, political destabilization and organized crime;
- cybercrime, information security and digital enforcement post-COVID.
- cyber-terrorism and information warfare, including the growing use of cyberspace to promote political destabilization.

A technical background is not required.

## Course Aims

The aims of the course are to ensure that you are familiar with the central principles of three inter-related components:

cybercrime, security and digital law enforcement.

## Relationship to Other Courses

This course falls within the Media, Intellectual Property and Technology Law specialisation in the LLM program. Students may find other courses in that specialisation complement their studies of cybercrime, security and digital law enforcement.

## Course Learning Outcomes

Course Learning Outcomes
CLO1 : Demonstrate a nuanced understanding of the integration, complexity and inter-disciplinary aspects of cybersecurity and cybercrime through looking at topics from both international and comparative perspectives including recent developments (PLOs 1, 4, 5, 6 and 7).
CLO2 : Demonstrate the ability to problem solve specific narrow cybersecurity/cybercrime issues from an inter-disciplinary approach, including both academic approaches as well as industry approaches to topics (PLOs 3, 5, 6, 7 and 8).
CLO3 : Demonstrate the ability to effectively communicate complex cybersecurity and cybercrime issues both in writing and orally at an individual level, as well as collaboratively (PLOs 1, 6, 9 and 10).
CLO4 : Demonstrate the ability to apply knowledge and skills to produce an independent and substantial research outcome (PLOs 5, 6, 8, 9, 10, 12)

Course Learning Outcomes	Assessment Item
CLO1 : Demonstrate a nuanced understanding of the integration, complexity and inter-disciplinary aspects of cybersecurity and cybercrime through looking at topics from both international and comparative perspectives including recent developments (PLOs 1, 4, 5, 6 and 7).	<ul style="list-style-type: none"><li>• Class Participation</li><li>• Research Proposal</li><li>• Research Essay</li></ul>
CLO2 : Demonstrate the ability to problem solve specific narrow cybersecurity/cybercrime issues from an inter-disciplinary approach, including both academic approaches as well as industry approaches to topics (PLOs 3, 5, 6, 7 and 8).	<ul style="list-style-type: none"><li>• Research Proposal</li><li>• Research Essay</li></ul>
CLO3 : Demonstrate the ability to effectively communicate complex cybersecurity and cybercrime issues both in writing and orally at an individual level, as well as collaboratively (PLOs 1, 6, 9 and 10).	<ul style="list-style-type: none"><li>• Class Participation</li><li>• Research Essay</li></ul>
CLO4 : Demonstrate the ability to apply knowledge and skills to produce an independent and substantial research outcome (PLOs 5, 6, 8, 9, 10, 12)	<ul style="list-style-type: none"><li>• Research Essay</li></ul>

# Learning and Teaching Technologies

Moodle - Learning Management System | Blackboard Collaborate

## Assessments

### Assessment Structure

Assessment Item	Weight	Relevant Dates
Class Participation Assessment Format: Individual	20%	Start Date: Throughout the course Due Date: 01/11/2024 04:00 PM
Research Proposal Assessment Format: Individual	20%	Due Date: 03/10/2024 04:00 PM
Research Essay Assessment Format: Individual	60%	Start Date: Not Applicable Due Date: 22/11/2024 04:00 PM

## Assessment Details

### Class Participation

#### Assessment Overview

This assessment requires you to prepare for and actively engage in class-based and online activities.

#### Course Learning Outcomes

- CL01 : Demonstrate a nuanced understanding of the integration, complexity and inter-disciplinary aspects of cybersecurity and cybercrime through looking at topics from both international and comparative perspectives including recent developments (PLOs 1, 4, 5, 6 and 7).
- CL03 : Demonstrate the ability to effectively communicate complex cybersecurity and cybercrime issues both in writing and orally at an individual level, as well as collaboratively (PLOs 1, 6, 9 and 10).

#### Detailed Assessment Description

Class participation credit can be earned through active, substantive participation in discussions, chats, and in-class exercises during the synchronous class meetings and through posts to enhance in class participation scores.

#### Assessment Length

N/A

#### Submission notes

Students must finish forum posts and submit a Reflective Commentary by the due date.

### Assignment submission Turnitin type

This assignment is submitted through Turnitin and students do not see Turnitin similarity reports.

### Generative AI Permission Level

#### **Planning/Design Assistance**

You are permitted to use generative AI tools, software or services to generate initial ideas, structures, or outlines. However, you must develop or edit those ideas to such a significant extent that what is submitted is your own work, i.e., what is generated by the tool, software or service should not be a part of your final submission. You should keep copies of your iterations to show your Course Authority if there is any uncertainty about the originality of your work.

If your Convenor has concerns that your answer contains passages of AI-generated text or media that have not been sufficiently modified you may be asked to explain your work, but we recognise that you are permitted to use AI generated text and media as a starting point and some traces may remain. If you are unable to satisfactorily demonstrate your understanding of your submission you may be referred to UNSW Conduct & Integrity Office for investigation for academic misconduct and possible penalties.

For more information on Generative AI and permitted use please see [here](#).

## **Research Proposal**

### Assessment Overview

This assessment requires you to write a research proposal. This proposal will inform your research essay assessment.

### Course Learning Outcomes

- CLO1 : Demonstrate a nuanced understanding of the integration, complexity and inter-disciplinary aspects of cybersecurity and cybercrime through looking at topics from both international and comparative perspectives including recent developments (PLOs 1, 4, 5, 6 and 7).
- CLO2 : Demonstrate the ability to problem solve specific narrow cybersecurity/cybercrime issues from an inter-disciplinary approach, including both academic approaches as well as industry approaches to topics (PLOs 3, 5, 6, 7 and 8).

### Detailed Assessment Description

The proposal briefing must be a maximum of 1,500 words, excluding citations and bibliography. Your briefing should include a brief topic statement indicating the subject matter of the topic your research essay will address, including what position you are taking regarding that topic. It

should also include a detailed outline of the flaws that you intend to address and a short bibliography of sources you will be considering.

### **Assessment Length**

1,500 words

### **Assignment submission Turnitin type**

This assignment is submitted through Turnitin and students do not see Turnitin similarity reports.

### **Generative AI Permission Level**

#### **Planning/Design Assistance**

You are permitted to use generative AI tools, software or services to generate initial ideas, structures, or outlines. However, you must develop or edit those ideas to such a significant extent that what is submitted is your own work, i.e., what is generated by the tool, software or service should not be a part of your final submission. You should keep copies of your iterations to show your Course Authority if there is any uncertainty about the originality of your work.

If your Convenor has concerns that your answer contains passages of AI-generated text or media that have not been sufficiently modified you may be asked to explain your work, but we recognise that you are permitted to use AI generated text and media as a starting point and some traces may remain. If you are unable to satisfactorily demonstrate your understanding of your submission you may be referred to UNSW Conduct & Integrity Office for investigation for academic misconduct and possible penalties.

For more information on Generative AI and permitted use please see [here](#).

## **Research Essay**

### **Assessment Overview**

This assessment requires you to write a research essay.

### **Course Learning Outcomes**

- CLO1 : Demonstrate a nuanced understanding of the integration, complexity and inter-disciplinary aspects of cybersecurity and cybercrime through looking at topics from both international and comparative perspectives including recent developments (PLOs 1, 4, 5, 6 and 7).
- CLO2 : Demonstrate the ability to problem solve specific narrow cybersecurity/cybercrime issues from an inter-disciplinary approach, including both academic approaches as well as industry approaches to topics (PLOs 3, 5, 6, 7 and 8).
- CLO3 : Demonstrate the ability to effectively communicate complex cybersecurity and

cybercrime issues both in writing and orally at an individual level, as well as collaboratively (PLOs 1, 6, 9 and 10).

- CL04 : Demonstrate the ability to apply knowledge and skills to produce an independent and substantial research outcome (PLOs 5, 6, 8, 9, 10, 12)

### **Detailed Assessment Description**

The Research Essay must constitute original work by you done specifically for this course and should show a thorough understanding of the subject matter and must demonstrate original research beyond the course materials, including law review articles, cases, and Internet materials as appropriate.

### **Assessment Length**

4,500 words

### **Assignment submission Turnitin type**

This assignment is submitted through Turnitin and students do not see Turnitin similarity reports.

### **Generative AI Permission Level**

#### **Planning/Design Assistance**

You are permitted to use generative AI tools, software or services to generate initial ideas, structures, or outlines. However, you must develop or edit those ideas to such a significant extent that what is submitted is your own work, i.e., what is generated by the tool, software or service should not be a part of your final submission. You should keep copies of your iterations to show your Course Authority if there is any uncertainty about the originality of your work.

If your Convenor has concerns that your answer contains passages of AI-generated text or media that have not been sufficiently modified you may be asked to explain your work, but we recognise that you are permitted to use AI generated text and media as a starting point and some traces may remain. If you are unable to satisfactorily demonstrate your understanding of your submission you may be referred to UNSW Conduct & Integrity Office for investigation for academic misconduct and possible penalties.

For more information on Generative AI and permitted use please see [here](#).

## **General Assessment Information**

For further information on generative AI use in the Faculty of Law & Justice, please review the section titled 'Academic Honesty and Plagiarism' under the 'Other Useful Information' tab.

## Grading Basis

Standard

## Requirements to pass course

50% Overall

# Course Schedule

Teaching Week/Module	Activity Type	Content
Week 2 : 16 September - 22 September	Topic	Introduction to Cybercrime
Week 3 : 23 September - 29 September	Topic	Hacking, Ransomware and Other Computer Intrusions
Week 4 : 30 September - 6 October	Topic	Cyberbullying, Revenge Porn and Other Virtual Assaults
Week 5 : 7 October - 13 October	Topic	Data Privacy, Government Surveillance and the Dark Net
Week 6 : 14 October - 20 October	Topic	Information Warfare and Cross-Border Challenges
Week 7 : 21 October - 27 October	Topic	Future Battlegrounds and Challenges

## Attendance Requirements

Please see information about attendance requirements in **Law & Justice Assessment Procedure** and **Student Information** located in the Other Useful Information tab in the Academic Information field.

Please be advised there will be no classes on public holidays. If your class falls on a public holiday, alternative arrangements will be made by the course convenor to make up the missed class.

## General Schedule Information

Classes will run online from 9am-1pm on Saturdays. The online 'Collaborate' classes can be accessed through Moodle.

# Course Resources

## Prescribed Resources

There is no required textbook. Readings for the course will be advised on Moodle.

## Recommended Resources

Readings for the course will be advised on Moodle.



# Course Evaluation and Development

Students are invited to provide informal feedback throughout the course and feedback will be gathered through the MyExperience survey at the end of term. This feedback will be analysed to improve the student learning experience.

## Staff Details

Position	Name	Email	Location	Phone	Availability	Equitable Learning Services Contact	Primary Contact
Convenor	Alexandra George		Law Building		Please email to make an appointment	Yes	No
Lecturer	Doris Long		USA		Please email to make an appointment	Yes	Yes

## Other Useful Information

### Academic Information

Upon your enrolment at UNSW, you share responsibility with us for maintaining a safe, harmonious and tolerant University environment.

You are required to:

- Comply with the University's conditions of enrolment.
- Act responsibly, ethically, safely and with integrity.
- Observe standards of equity and respect in dealing with every member of the UNSW community.
- Engage in lawful behaviour.
- Use and care for University resources in a responsible and appropriate manner.
- Maintain the University's reputation and good standing.

For more information, visit the [UNSW Student Code of Conduct Website](#).

### UNSW Law & Justice Assessment Policy

It is essential that all students undertaking this course read and abide by the [UNSW Law & Justice Assessment Policy & Student Information](#). This document includes information on Class Attendance, Late Work, Word Limits, Marking, Special Consideration, Workload, and Academic Misconduct & Plagiarism. More information can also be found at [Assessment & Exam Information](#).

Information regarding Course Outlines are subject to change and students are advised to check updates. If there is a discrepancy between the information posted here and the handbook or the UNSW Law & Justice website, please contact [Student Services via The Nucleus Hub](#) for advice. UNSW Law & Justice reserves the right to discontinue or vary such courses or staff allocations at any time. If your course is not here, please visit [Handbook](#) for information.

## Academic Honesty and Plagiarism

As a student at UNSW you are expected to display [academic integrity](#) in your work and interactions. Where a student breaches the [UNSW Student Code](#) with respect to academic integrity, the University may take disciplinary action under the Student Misconduct Procedure. To assure academic integrity, you may be required to demonstrate reasoning, research and the process of constructing work submitted for assessment.

To assist you in understanding what academic integrity means, and how to ensure that you do comply with the UNSW Student Code, it is strongly recommended that you complete the [Working with Academic Integrity](#) module before submitting your first assessment task. It is a free, online self-paced Moodle module that should take about one hour to complete.

## Generative AI

Using generative AI to conduct research or to organise your argument is not prohibited but is not encouraged. We note that the output from generative AI tools is often incorrect and almost always more superficial than is required to achieve a passing grade. Moreover, any substantive errors in the assessment, such as inappropriate references or incorrect statements, will be regarded negatively by the marker, just as they would if not generated by AI. You should limit your use of AI to simple editorial assistance, such as standard editing and referencing functions in word processing software in the creation of your submission. You must not use any functions that generate or paraphrase passages of text, whether based on your own work or not. If your marker or Turnitin identify the wrongful use of generative AI in the text of your assessment submission, including the use of paraphrasing software, your assessment may be referred to the Student Integrity team for investigation. Please go to the link for further information about [referencing and acknowledging the use of artificial intelligence tools](#).

## Prohibition on use of translation apps

With limited exceptions for language study, the course of study and assessment in Australian universities must be in English (Higher Education Standard Framework (Threshold Standards))

2021 1.5 6(c)).

In Law & Justice many classes have assessable class participation. This must be in English. **Use of a translation device to assist with contributions to class discussion is not allowed.** Marks for class participation may be reduced where use of translation devices is detected. Similar prohibitions apply to use of any other generative text app that is not specifically permitted by the class teacher. However, use of translation software to assist a student to understand material outside of class, or to assist with preparation for assessment is generally permitted.

Further considerations apply to LLB and JD students. International lawyers who seek to be admitted in NSW must satisfy an English proficiency test. That test is expressed as equivalent to IELTS scores of 7.0 -8.0 across the tests. It is assumed that UNSW graduates are at or above those levels of English proficiency. Use of translation apps can impede the attainment of that level of proficiency. Students should avoid behaviours that put them at risk of breach of legal requirements which can have significant consequences, including potential consequences for your admission as a lawyer.

## Submission of Assessment Tasks

Before submitting assessment items all students must read and abide by the [UNSW Law & Justice Assessment Policy & Student Information](#).

## Special consideration

Special consideration is primarily intended to provide you with an extra opportunity to demonstrate the level of performance of which you are capable. To apply, and for further information, see Special Consideration on the UNSW [Current Students](#) page.

## Feedback

UNSW Law & Justice appreciates the need for students to have feedback on their progress prior to the last date for withdrawal without failure. All courses will therefore provide feedback to students prior to this date, as well as throughout the course. However, students should note that feedback does not take the form only of formal grades and written comments on written assessments. Rather, formative feedback, which helps students to self-assess, to identify misunderstandings, and to identify areas requiring further work, will occur during class and possibly online. For example, where a teacher asks the class a question, all students should think about how they might answer. Even though not all students will necessarily be able to respond

orally, everyone can reflect on their tentative answer in light of the teacher's response and subsequent class discussion. If you are struggling to understand what is being asked in class, or if your tentative answers prove incorrect and subsequent discussion does not clear things up, then you should continue to ask questions (of yourself, your peers or your teacher). Similarly, you can get a sense of your ability in a course through peer feedback during group work, your teacher's responses to your in-class contributions, and your own response to in-class problems and examples (whether or not you are called on to relay your answer to the class) and also your online activities and responses by others to those activities. Students enrolled in this course may check their Moodle course page for details on the specific feedback used in this course.

## Faculty-specific Information

### Additional support for students

- Student support: <https://www.student.unsw.edu.au/support>
- Academic Skills and Support: <https://student.unsw.edu.au/academic-skills>
- Student Wellbeing, Health and Safety: <https://student.unsw.edu.au/wellbeing>
- Equitable Learning Services: <https://student.unsw.edu.au/els>
- UNSW IT Service Centre: <https://www.myit.unsw.edu.au>

### Course improvement

Student feedback is very important to continual course improvement. This is demonstrated within the Faculty of Law & Justice by the implementation of the UNSW online student survey myExperience, which allows students to evaluate their learning experiences in an anonymous way. myExperience survey reports are produced from each survey. They are released to staff after all student assessment results are finalised and released to students. Course convenors will use the feedback to make ongoing improvements to the course. Students enrolled in this course may check their Moodle course page for details on the actions taken in response to evaluation feedback in Student Survey.

## School Contact Information

Please contact [Nucleus Student Hub](#) for all enquiries. The Nucleus acts as a central communications hub for UNSW and will distribute your enquiry to the best person to respond.