UNSW Course Outline

LAWS3040 Regulation for Cyber Security - 2024

Published on the 26 Aug 2024

General Course Information

Course Code : LAWS3040
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 : Undergraduate
Units of Credit : 6

Useful Links

Handbook Class Timetable

Course Details & Outcomes

Course Description

This course provides an introduction to the rapidly growing field of cyber security and to the role played by law and legal professionals in regulating it. This multi-disciplinary course is an opportunity for law students to develop an understanding of the role played by law in cyber policy

and operation, and then to work alongside future security engineers solving cyber security challenges. Law students will focus on the role of regulation, while engineering students (COMP6441/COMP6841 Security Engineering and Cyber Security) will cover more technical computing material, with all students coming together in tutorials to analyse policy and practical challenges. Law students are the 'legal experts' in interdisciplinary spaces, engaging with engineering students in collective problem-solving. Over the course of the Term, students will gain confidence in working collaboratively with engineers.

The course is not a typical law course in its structure or assessment. Law students attend a two hour lecture on the foundations of cyber security (with Engineering students), a two hour law seminar, and a two hour tutorial (with Engineering students) each week. While there are few readings (mostly statutes and policy documents, some cases), there are online law and engineering activities to complete each week. These sometimes take law students outside their comfort zone, encouraging "security thinking" and an "attacker mindset." Students should expect to commit approximately 15 hours a week to the course including attendance, self-directed research, completion of on-line modules, preparation for tutorials and seminars, and completion of assessment.

Foundational security topics to which law students are introduced include insiders, privacy, cybercrime, social engineering, risk, secrets, authentication, physical security, weakest link, supply chain, cognitive biases, organisational change, incident response, security analysis, open source intelligence and reconnaissance. These are introduced through case studies, focusing on recent developments. Legal topics include relevant aspects of tort law, contract law, consumer law, directors duties, privacy law, telecommunications regulation, critical infrastructure regulation, criminal law, national security and law enforcement powers, and international law. The focus is on Australian law, but comparative material is included where relevant. Other regulation (such as national policy and standards) are also discussed. The goal is understanding how the different strands of law apply to current policy problems in the field of cyber security, rather than being a comprehensive coverage of particular doctrinal domains covered elsewhere in the degree. Tutorials provide an interactive opportunity to tackle complex policy problems from a multi-disciplinary perspective.

The primary background needed is a keen, devious and analytical mind. Technical computing skills are not needed. However for those wishing to acquire or appreciate the technical aspects of cyber security – all engineering lectures, classes, and learning activities are open and available for law students to attend. This is entirely optional and non-examinable. It is for those

who are curious. To get the most from this course, students will need to engage in independent study and research and be able to act as independent self-directed learners.

Course Aims

The course aims to introduce law students to core elements of cyber security and the legal and regulatory framework that surrounds it. The course provides opportunities for law students and engineering students to work together on interdisciplinary problems and policy challenges.

Relationship to Other Courses

Taught in conjunction with COMP6441 (Cyber Security and Security Engineering), with a common lecture and joint tutorials.

Course Learning Outcomes

Course Learning Outcomes
CLO1 : Describe and identify main elements of contemporary cyber security (including familiarity with terminology such as vulnerabilities, exploits, root kits, malware, etc) - PLO 8
CLO2 : Understand how security exploits are used, their specific strengths, weaknesses and countermeasures - PLO 8
CLO3 : Understand and apply key principles in security engineering design - PLO 8
CLO4 : Describe the legal and regulatory landscape for cyber security in Australia, including relevant international aspects - PLO 1
CLO5 : Design, justify and effectively communicate policy and solutions for security problems and scenarios - PLOs 7, 8, 9
CLO6 : Analyse and identify flaws in policy and engineering solutions for security problems and scenarios - PLOs 7, 8, 9
CLO7 : Analyse the civil and criminal responsibilities and liabilities of different parties in the context of factual scenarios related to cyber security failures - PLOs 4, 5, 6, 8
CLO8 : Engage in self-directed, independent learning including effective reflection and time management - PLO 12
CLO9 : Demonstrate colleagiality, contribution to a learning community and professionalism - PLOs 10, 11
CLO10 : Think analytically about technical, legal, and policy challenges - PLOs 7, 8

Course Learning Outcomes	Assessment Item
CLO1 : Describe and identify main elements of contemporary cyber security (including familiarity with terminology such as vulnerabilities, exploits, root kits, malware, etc) - PLO 8	• Portfolio • Exam
CLO2 : Understand how security exploits are used, their specific strengths, weaknesses and countermeasures - PLO 8	• Portfolio • Exam
CLO3 : Understand and apply key principles in security engineering design - PLO 8	• Portfolio • Exam
CLO4 : Describe the legal and regulatory landscape for cyber security in Australia, including relevant international aspects - PLO 1	• Exam
CLO5 : Design, justify and effectively communicate policy and solutions for security problems and scenarios - PLOs 7, 8, 9	• Portfolio • Exam
CLO6 : Analyse and identify flaws in policy and engineering solutions for security problems and scenarios - PLOs 7, 8, 9	• Portfolio • Exam
CLO7 : Analyse the civil and criminal responsibilities and liabilities of different parties in the context of factual scenarios related to cyber security failures - PLOs 4, 5, 6, 8	• Exam
CLO8 : Engage in self-directed, independent learning including effective reflection and time management - PLO 12	• Project 'Something awesome' • Portfolio
CLO9 : Demonstrate colleagiality, contribution to a learning community and professionalism - PLOs 10, 11	• Project 'Something awesome' • Portfolio
CLO10 : Think analytically about technical, legal, and policy challenges - PLOs 7, 8	• Project 'Something awesome' • Portfolio • Exam

Learning and Teaching Technologies

Moodle - Learning Management System | WEB CMS course page

Learning and Teaching in this course

This course is designed to foster cross-disciplinary learning on a topic of increasing importance to people, policymakers and businesses. In particular, students apply their knowledge and expertise (gained both outside and inside the course) to solve problems in collaboration with Engineering peers. There are weekly lectures conveying common ideas. There are law seminars which combine discussion, problem-solving and interrogating policy ideas (much like students will be familiar with from other law courses). Tutorials are an opportunity to work on problems

together with Engineering peers, bringing in knowledge of law and regulation to think through proposals and solve problems.

Assessments

Assessment Structure

Assessment Item	Weight	Relevant Dates
Portfolio Assessment Format: Individual	30%	Start Date: Weekly Due Date: Tuesday 10am; except for Tuesday tutorial groups which will have special arrangements.
Project 'Something awesome' Assessment Format: Individual Short Extension: Yes (3 days)	30%	Start Date: Not Applicable Due Date: 01/11/2024 06:00 PM
Exam Assessment Format: Individual	40%	Start Date: Not Applicable Due Date: Not Applicable

Assessment Details
Portfolio

<u>Assessment Overview</u>

Weekly activities, including "class participation" in law seminars.

Feedback – weekly written feedback, from tutors

<u>Course Learning Outcomes</u>

- CLO1 : Describe and identify main elements of contemporary cyber security (including familiarity with terminology such as vulnerabilities, exploits, root kits, malware, etc) - PLO 8
- CLO2 : Understand how security exploits are used, their specific strengths, weaknesses and countermeasures - PLO 8
- CLO3 : Understand and apply key principles in security engineering design - PLO 8
- CLO5 : Design, justify and effectively communicate policy and solutions for security problems and scenarios - PLOs 7, 8, 9
- CLO6 : Analyse and identify flaws in policy and engineering solutions for security problems and scenarios - PLOs 7, 8, 9
- CLO8 : Engage in self-directed, independent learning including effective reflection and time management - PLO 12
- CLO9 : Demonstrate colleagiality, contribution to a learning community and professionalism - PLOs 10, 11
- CLO10 : Think analytically about technical, legal, and policy challenges - PLOs 7, 8

<u>Detailed Assessment Description</u>

20% - Mark from tutors, based on engagement in tutorials and completion of relevant online

activities. Mark is based on 'best' 7 weeks.

10% - Class participation mark for law seminars

<u>Assessment Length</u>

N/A

<u>Submission notes</u>

Varied

<u>Assessment information</u>

Except in extremely exceptional circumstances, there is no special consideration for this assessment. Students are assessed on the basis of the 'best' 7 weeks of submissions. Students are expected to submit *every* week except where a substantial and extended unforeseen circumstance occurs. Such unforeseen circumstances should thus not affect the students' grade unless the substantial unforeseen circumstance prevents submission three or more times.

<u>Assignment submission Turnitin type</u>

This is not a Turnitin assignment

<u>Generative AI Permission Level</u>

Simple Editing Assistance

In completing this assessment, you are permitted to use standard editing and referencing functions in the software you use to complete your assessment. These functions are described below. You must not use any functions that generate or paraphrase passages of text or other media, whether based on your own work or not.

If your Convenor has concerns that your submission contains passages of AI-generated text or media, you may be asked to account for your work. 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.

Students are permitted to use translation, spell-check, and grammar correction tools only.

Project 'Something awesome'

<u>Assessment Overview</u>

Self-selected project

Feedback – Written feedback

Course Learning Outcomes

- CLO8 : Engage in self-directed, independent learning including effective reflection and time management - PLO 12
- CLO9 : Demonstrate colleagiality, contribution to a learning community and professionalism - PLOs 10, 11
- CLO10 : Think analytically about technical, legal, and policy challenges - PLOs 7, 8

Detailed Assessment Description

This will be discussed in detail with students in the course. Students choose a project that will challenge them and develop a plan to complete the project the course over the semester.

Assessment Length

N/A

Submission notes

Moodle

Assessment information

NA

Assignment submission Turnitin type

This is not a Turnitin assignment

Generative AI Permission Level

Simple Editing Assistance

In completing this assessment, you are permitted to use standard editing and referencing functions in the software you use to complete your assessment. These functions are described below. You must not use any functions that generate or paraphrase passages of text or other media, whether based on your own work or not.

If your Convenor has concerns that your submission contains passages of AI-generated text or media, you may be asked to account for your work. 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.

Some students' projects may use generative AI *as part of the project itself*. In that case, the use of generative AI should be disclosed in the proposal. Otherwise, students are permitted to use translation, spell-check, and grammar correction tools only.

Exam

Assessment Overview

Open book exam covering all course content and requiring good analysis of law, policy and security issues.

Feedback – specific feedback on request

Course Learning Outcomes

- CLO1 : Describe and identify main elements of contemporary cyber security (including familiarity with terminology such as vulnerabilities, exploits, root kits, malware, etc) - PLO 8
- CLO2 : Understand how security exploits are used, their specific strengths, weaknesses and countermeasures - PLO 8
- CLO3 : Understand and apply key principles in security engineering design - PLO 8
- CLO4 : Describe the legal and regulatory landscape for cyber security in Australia, including relevant international aspects - PLO 1
- CLO5 : Design, justify and effectively communicate policy and solutions for security problems and scenarios - PLOs 7, 8, 9
- CLO6 : Analyse and identify flaws in policy and engineering solutions for security problems and scenarios - PLOs 7, 8, 9
- CLO7 : Analyse the civil and criminal responsibilities and liabilities of different parties in the context of factual scenarios related to cyber security failures - PLOs 4, 5, 6, 8
- CLO10 : Think analytically about technical, legal, and policy challenges - PLOs 7, 8

Detailed Assessment Description

Take home exam

Open book

Assessment Length

2 hours done over 3 hours

Submission notes

Typed and submitted online

Assignment submission Turnitin type

This is not a Turnitin assignment

Generative AI Permission Level

No Assistance

This assessment is designed for you to complete without the use of any generative AI. You are not permitted to use any generative AI tools, software or service to search for or generate

information or answers.

For more information on Generative AI and permitted use please see here.

General Assessment Information

For 'legal' parts of the course, students should use standard referencing ie AGLC for submitted written work and brief abbreviations in the exam.

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.

<u>Grading Basis</u>

Standard

<u>Requirements to pass course</u>

A final mark over 50% and 80% attendance in seminars, tutorials, and lectures.

Course Schedule

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.

Students must attend 80% of 'core' lectures, 80% of tutorials and 80% of seminars, as a requirement to pass the course.

General Schedule Information

Tuesday 'law' seminar 2-3.30pm (convenor available from 3.30pm until start of lecture)

Tuesday lecture (enrol in synchronous online version if that is your intent) 4-6pm

Monday lecture in Weeks 1 and 10 (can be viewed asynchronously by law students in case of scheduling conflict, but students strongly encouraged to attend synchronously if possible) 6-8pm

Tutorial (timing varies)

OPTIONAL ACTIVITIES:

Monday lecture 6-8pm (compulsory Weeks 1 and 10)

Tuesday "Security Theatre" movie night 6-8pm

Course Resources

Prescribed Resources

Online materials

Recommended Resources

Online materials, and information in classes and tutorials.

Additional Costs

None. There will be one mandatory movie viewing, we will show for free, but students unable to attend that session may need to rent it from a streaming provider.

Course Evaluation and Development

The main suggestions for change from the last time this course was taught (and our responses for this time) are:

1. **Complexity of submission of weekly reflections and greater flexibility.** Going forward, students will only need to submit (1) heading, (2) link (or the answer itself), and (3) asterisk next to best activity of the week. Further only the 'best' 7 weeks will count towards the student's grade.

2. **Explaining the point of the weekly activities to students at the outset.** Will allow some time in law seminars for this each week. Also more explanation on each activity.

3. **Variability in tutor management of LAWS3040 students.** Will run a session early in the term for all tutors on how to manage cross-disciplinary tutorials.

4. **Content alignment (linking law and engineering material).** Will allow some time in law seminars for this each week. Will also have more 'legal' content in main engineering lecture.

5. **Inconsistent communications (tutors, Richard, Lyria, etc).** Centralise communication around assessment and course structure - class Q & A forum.

6. Clearer elaboration of assessment requirements (eg rubrics). Will be done, plus opportunity to ask questions on the central Q&A forum.

Staff Details

Position	Name	Email	Location	Phone	Availability	Equitable Learning Services Contact	Primary Contact
Convenor	Lyria Bennett Moses		L+J Building, F8, Room 246	+612 9385 2254	Half an hour after class, or by 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 Plagarism

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.