UNSW SYDNEY

Master of Cyber Security

Build your cyber mindset to secure your future

This program guide contains information for:

- Master of Cyber Security (8649)
- Graduate Diploma in Cyber Security (5649)
- Graduate Certificate in Cyber Security (7649)

Contents

Learn at UNSW – a world leader.

Most employable students

UNSW has been voted as having the most employable students at the AFR Top 100 Future Leaders Awards, 2020, 2021, 2022, 2023 and 2024.

Top ranked for Engineering and Technology

UNSW is ranked 1st in Australia for Engineering and Technology studies.

QS World University Rankings by Subject, 2024

Group of Eight

UNSW is part of the Group of Eight (GO8): Australia's leading research intensive universities.

Highest graduate salaries

UNSW graduates earn the highest average salaries among graduates in Australia.

QILT Graduate Outcomes Survey, 2023

Top 20 worldwide

UNSW is ranked 19th overall in the world.

QS World University Rankings, 2025

Defence connections

This program has been developed in collaboration with industry experts from UNSW Canberra at the Australian Defence Force Academy (ADFA). UNSW Canberra is the only national academic institution with an integrated defence focus.

UNSW Canberra in home to the UNSW Institute for Cyber Security (IFCYBER), the largest concentration of research and tertiary education in the field of cyber security in the Southern Hemisphere. UNSW Canberra Cyber is a centre of excellence that works closely with the UNSW Defence Research Institute and is a member of the NSW Defence Innovation Network.

For more than half a century, UNSW Canberra has combined research and education with one of the world's top military organisations to develop global leaders.

UNSW Canberra Cyber is a leading centre for cyber learning and research. Its cyber security courses will teach you to think outside the box. You will obtain the tools and techniques required to detect, analyse, and confront cyber challenges to help you succeed in this fast-growing industry.

Image of AFDA: Kurt Barnett - UNSW Canberra

Leaders in Engineering

UNSW Engineering is Australia's leading engineering faculty, ranking #1 in Australia for Engineering and Technology studies*. Our innovative teaching and practical work integrated learning shapes the future leaders of engineering.

We believe engineering is about making and doing.

It is about seeing problems and solving them using a mix of lateral thinking, innate curiosity and an enthusiasm for technology. Above all, engineering is about wanting to make a better and safer world. Our students and graduates, trained by expert academics are among the best in the world.

We deliver programs across eight schools: Biomedical Engineering, Chemical Engineering, Civil and Environmental Engineering, Computer Science and Engineering, Electrical Engineering and Telecommunications, Mechanical and Manufacturing Engineering, Minerals and Energy Resources Engineering and Photovoltaics and Renewable Energy Engineering.

A powerhouse of innovation in Australia and the region, UNSW Engineering is home to more than 800 researchers and educators, including expertise across 36 research centres and three institutes.

We translate research into real-world solutions, working closely with businesses, government and community organisations.

**QS World University Rankings by Subject, 2024*

Master of Cyber Security

Cybercrime is a rapidly escalating issue in Australia, with the Australian Cyber Security Centre reporting a 13% rise in cyber incidents in 2023 alone (ACS). This increase underscores the urgent need for cybersecurity professionals, as both businesses and governments face increasingly advanced cyberattacks. The economic impact is significant, with cybercrime costing Australia an estimated $33 billion annually, threatening critical infrastructure and sensitive data (ACS).

At the same time, Australia is experiencing a major shortage of cybersecurity talent. With only one specialist for every 240 companies, this shortfall poses significant risks to businesses. Moreover, the gap is expected to grow, with an estimated shortage of 30,000 professionals in the near future (ACS) (Australian Associated Press). This highlights the importance of investing in advanced education, such as a Master of Cyber Security, to address this critical workforce gap.

The Cyber Security program is designed for ambitious professionals who want to become technical experts or leaders and leverage lucrative career opportunities within the field of cyber. The skills you develop in this program will help you provide safe and secure online experiences, often to some of the most vulnerable online users. Select from either the Security Management and Leadership specialisation or Security Engineering specialisation within this program to further develop your expertise and diversify your career options.

This accelerated program is offered 100% online, meaning you can study anywhere at any time and graduate in only two years without taking time out of the workforce.

Designed for industry needs

Designed by leading cyber security academics and industry experts and built to remain relevant in a continuously developing sector.

Tailored security specialisations

Select from two cyber security specialisations and a range of specific electives to build the masters program that suits your career path, existing skill set and aspirations.

Quality and reputation

Learn cyber security from one of the most highly regarded Australian universities and join our hugely successful and diverse cyber security alumni community.

Accelerated learning with immediate ROI

With intakes every two months, study one course at a time, 100% online and accelerated, instantly adding value to your career and organisation

Masters program specialisations

Graduate Certificate in Cyber Security

Foundation courses

Graduate Diploma in Cyber Security (Security Management and Leadership)

Foundation courses +
Specialisation electives

Graduate Diploma in Cyber Security (Security Engineering)

Foundation courses +
Specialisation electives

Master of Cyber Security (Security Management and Leadership)

Foundation courses +
Specialisation electives +
General electives +
Capstone

Master of Cyber Security (Security Engineering)

Foundation courses +
Specialisation electives +
General electives +
Capstone

Program overview

The Master of Cyber Security program encompasses 12 online courses, with the choice of selecting from a Security Management and Leadership or Security Engineering specialisation.

The masters program consists of four core courses, including at least four specialisation courses, up to three electives, plus a project based capstone. Students may take one non-domain elective with the permission of the Program Convenor.

Master of Cyber Security

Complete 72 Units of Credit (UOC), which is 12 courses (each course is 6 UOC).

Core Courses – complete all

- Data Security and Privacy
- Cyber Security and Ethics
- Principles of Security Engineering

+ Specialisation

Choose 1 of the 2 specialisations and their courses from the right.

+ Capstone Project

Management and Leadership Capstone Project

Specialisation #1

Security Management and Leadership

Specialisation Courses

Students must complete at least 4, maximum of 5:

- Cyber Operations
- Cyber Risk and Resilience
- Cyber Management and Governance
- Cyber Threats and Crime
- Cyber and the Law

Elective Courses

Students may take up to 2:

- Digital Forensics†
- Advanced Penetration Testing^
- Penetration Testing
- Cloud Security
- Reverse Engineering†
- Fundamentals of Coding: C and Assembler
- Operating System Fundamentals for Security#
- *Non-Domain Elective*

  With the permission of the Program Convenor, students may substitute up to 6 UOC elective with any other postgraduate course offered in one of the UNSW Online Programs.

Specialisation #2

Security Engineering

Specialisation Courses

Students must complete at least 4, maximum of 5:

- Cyber Operations
- Digital Forensics†
- Advanced Penetration Testing^
- Penetration Testing
- Cloud Security
- Fundamentals of Coding: C and Assembler
- Operating System Fundamentals for Security

Elective Courses

Students may take up to 2:

- Cyber Operations
- Cyber Risk and Resilience
- Cyber Management and Governance
- Cyber Threats and Crime
- Reverse Engineering
- Cyber and the Law
- *Non-Domain Elective*

  With the permission of the Program Convenor, students may substitute up to 6 UOC elective with any other postgraduate course offered in one of the UNSW Online Programs.

Prerequisites

^ Penetration Testing † Operating System Fundamentals for Security
# Fundamentals of Coding: C and Assembler

Program overview (contd.)

Graduate Diploma in Cyber Security

Complete 48 Units of Credit (UOC), which is 8 courses (each course is 6 UOC).

Core Courses – complete all

- Data Security and Privacy
- Cyber Security and Ethics
- Principles of Security Engineering

+ Specialisation

Choose 1 of the 2 specialisations and their courses from the right.

Specialisation #1

Security Management and Leadership

Specialisation Courses

Students must take at least 4 courses, maximum of 5 courses:

- Cyber Operations
- Cyber Risk and Resilience
- Cyber Management and Governance
- Cyber Threats and Crime
- Cyber and the Law

Elective Courses

Students can take a maximum of 2 courses:

- Digital Forensics†
- Advanced Penetration Testing^
- Penetration Testing
- Cloud Security
- Reverse Engineering†
- Fundamentals of Coding: C and Assembler
- Operating System Fundamentals for Security#
- *Non-Domain Elective*

  With the permission of the Program Convenor, students may substitute up to 6 UOC elective with any other postgraduate course offered in one of the UNSW Online Programs.

Specialisation #2

Security Engineering

Specialisation Courses

Study at least 4 courses, maximum of 5 courses:

- Cyber Operations
- Digital Forensics†
- Advanced Penetration Testing^
- Penetration Testing
- Cloud Security
- Fundamentals of Coding: C and Assembler
- Operating System Fundamentals for Security

Electives Courses

Student can take a maximum of 2 courses:

- Cyber Operations
- Cyber Risk and Resilience
- Cyber Management and Governance
- Cyber Threats and Crime
- Reverse Engineering
- Cyber and the Law
- *Non-Domain Elective*

  With the permission of the Program Convenor, students may substitute up to 6 UOC elective with any other postgraduate course offered in one of the UNSW Online Programs.

Prerequisites

^ Penetration Testing † Operating System Fundamentals for Security
# Fundamentals of Coding: C and Assembler

Program overview (contd.)

Graduate Certificate in Cyber Security

Complete 24 Units of Credit (UOC), which is 4 courses (each course is 6 UOC).

Core Courses – complete all

- Data Security and Privacy
- Cyber Security and Ethics
- Principles of Security Engineering

+ Elective Course

Choose 1 from the list to the right

Elective Courses

Students must complete 1:

- Cyber Operations
- Cyber Risk and Resilience
- Cyber Management and Governance
- Cyber Threats and Crime
- Cyber and the Law
- Digital Forensics
- Penetration Testing
- Cloud Security
- Fundamentals of Coding: C and Assembler

Knowledge areas

Identify, mitigate and defend against risks and attacks

The internet is revolutionising society, enabling new ways to work, live, connect, collaborate and drive economic growth while also exposing a new world of risk. Develop a security engineering mindset to synthesise current trends to anticipate the future of cybercrime and gain an understanding of the current controls that defend against cyber-attacks.

Protect organisations and individuals, their data, and their rights through robust security by understanding and developing tools, techniques and processes. You will learn how organisations can handle data in secure ways; understand the emerging issues and principles of privacy and how to identify, manage and respond to security risks across organisations and current best practice in a rapidly changing global environment.

Global perspective

The Cyber Security program provides coursework from international and local perspectives. Gain a contemporary understanding of global cyber security issues and trends from experts and leading academics to prepare you to anticipate future trends and equip you with the knowledge and skills to deal with them.

Ethics and the law

Learn beyond just the technical, to develop a professional, ethical and legal understanding and approach to the field of cyber. Gain best practice skills to steer organisations through emerging ethical and legal challenges of the cyber landscape. Recognise and respond to future ethical challenges, develop an appreciation of professional issues and best practice and understand ways to effectively analyse and communicate ethical issues related to cyber security.

Understand the current key areas of legislation and how these impact on cyber security professional practice. Survey the current legal framework in relation to cyber security including hacking, privacy, surveillance, government powers to intercept data, protection of national infrastructure, use of spectrum, GPS, military and agencies etc. You will also learn to identify other stakeholders and effectively bring about positive change by addressing the ramifications of current along with future legislation and regulation.

Security Management and Leadership

In pursuing the Security Management and Leadership specialisation you will increase your knowledge and understanding of how business and cyber security intersect. Explore core cyber security concepts and emerging security engineering principles. Apply your knowledge to help lead and manage organisations through real world cyber security problems.

Gain the necessary skills for leadership in the sustainment and growth of an organisation's cyber resources, operations and security. You will also learn to deploy appropriate response and resilience policies to maintain business in the face of a cyber attack. In your management and leadership capstone, you will apply the theory and skills learned throughout the program in practical ways, by collaborating in teams to conduct an exploratory leadership project related to cyber.

Security Engineering

Explore the Security Engineering specialisation, where you will gain detailed security knowledge and technical capabilities. You will develop both fundamental theoretical knowledge and hands-on skills in the science and art of security design and assurance including pentration testing and learn to make effective holistic recommendations for addressing weaknesses and improving security.

Understand paradigms for securing and assuring cloud-based infrastructure at scale and learn to effectively communicate security recommendation, to key stakeholders. You will also develop your technical coding, programmatic along with analytical skills and apply security knowledge to real world applications. In your security engineering capstone unit you will undertake a self-directed learning opportunity and effectively integrate skills learned across the program, to conduct an exploratory technical project related to cyber.

The UNSW Online experience

- We are here to support you, every step of the way, to graduate from one of the world's leading universities. Our online learning environment has been designed to seamlessly fit into your already busy schedule and you'll be able to access course resources on any device, at any time.
- Our academics are some of the best in the world and, even though you're studying online, you can expect your learning experience to be the same high standard as that of our on-campus students.
- Throughout your study journey, you will be able to turn to your Student Success Advisor, who is committed to assisting you from enrolment through to graduation. They are on-hand for all non-academic queries by phone or email.
- You will also have access to Career Success – a curated, self-paced module that provides a framework for thinking about, and taking action to implement, an effective career plan. You will also have access to Career Success – a curated, self-pawced module that provides a framework for thinking about, and taking action to implement, an effective career plan. Through Career Success, you will have access to tools like Career AI (powered by VMock) and CaseCoach, and guides on crafting the perfect LinkedIn profile, resume, and cover letter.

Program details

2025 Indicative domestic program fees^

Master of Cyber Security	Program code: 8649	12 courses	$61,500
Graduate Diploma in Cyber Security	Program code: 5649	8 courses	$40,500
Graduate Certificate in Cyber Security	Program code: 7649	4 courses	$20,000

^All prices are listed in Australian dollars and may exceed the indicative figures listed. Visit our Fees page for up-to-date information inclusive of 2025 indicative International program fees. Fees are subject to annual review by the University and may increase annually, with the new fees effective from the start of each calendar year. Indicative fees are a guide for comparison only based on current conditions and available data. You should not rely on indicative fees.

Program intakes (Hexamesters)

Six intakes annually

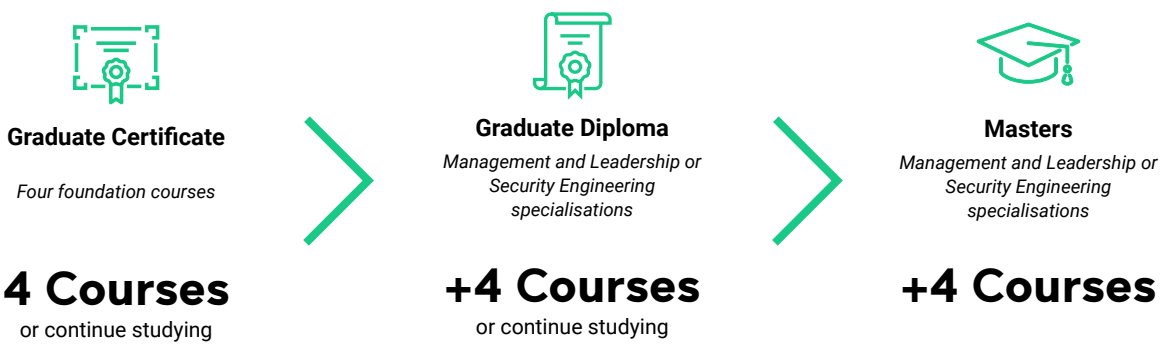
January, March, May, July, September, October

Program duration

Each course is seven-weeks long, plus an Orientation week. UNSW Online advises a minimum of 20–25 hours of study per week. The masters program can be completed in as little as two years.

Nested qualifications

The Master of Cyber Security program also includes a Graduate Certificate in Cyber Security and a Graduate Diploma in Cyber Security. For those who do not qualify for direct entry into the masters program, you may be eligible for entry into the Graduate Certificate. You can articulate from this into the masters program (upon successful completion of the Graduate Certificate and Graduate Diploma). Alternatively, if for whatever reason you choose not to continue to complete the masters program, you can exit with a Graduate Certificate or Graduate Diploma.



Study plans and completion times might vary depending on elective choice, recognition of prior learning (RPL), leave and subject availability. For more information, speak with a Student Advisor.

Entry requirements

UNSW's Postgraduate Coursework Entry Score Calculator

To assist us in assessing your previous study and eligibility for this course, we recommend using the UNSW Postgraduate Coursework Entry Score Calculator as a guide. This calculator converts and scales the grading schemes across the world into a percentage that applies to UNSW entry requirements.

Master of Cyber Security (8649)	Graduate Diploma in Cyber Security (5649)	Graduate Certificate in Cyber Security (7649)
1. Have completed the Graduate Certificate in Cyber Security (or equivalent) with a minimum WAM of 65; **OR** 2. Have completed the Graduate Diploma in Cyber Security (or equivalent); **OR** 3. Have completed a Bachelor degree or higher level qualification in a cognate discipline to the selected specialisation* with a minimum WAM of 65.	1. Have completed the Graduate Certificate in Cyber Security (or equivalent) with a minimum WAM of 65; **OR** 2. Have completed a Bachelor degree or higher level qualification in a cognate discipline to the selected specialisation* with a minimum WAM of 65.	1. Have completed a Bachelor degree or higher level qualification (or equivalent); **OR** 2. Applicants who have not completed a Bachelor degree or higher level qualification are required to have a minimum of 2 years relevant or professional experience* in cyber security or other cyber-related positions.
Limitations on Recognition of Prior Learning • Maximum of 6 core courses (36 UOC) can be granted, where total RPL does not exceed 50% of the program. • Can only be granted based on postgraduate study.	**Limitations on Recognition of Prior Learning** • Maximum of 4 core courses (24 UOC) can be granted, where total RPL does not exceed 50% of the program. • Can only be granted based on postgraduate study.	**Limitations on Recognition of Prior Learning** • Students enrolled in a program that consists of 24 UOC or less are not eligible for RPL.
**ZZENDS Security Management & Leadership cognate disciplines may include Science, Engineering, Business, Leadership, and Policy.* **ZZENES Security Engineering cognate disciplines may include Science, Engineering, and other degrees with substantial computing, mathematics, and/or statistics courses*	**ZZENAS Security Management & Leadership cognate disciplines may include Science, Engineering, Business, Leadership, and Policy.* **ZZENBS Security Engineering cognate disciplines may include Science, Engineering, and other degrees with substantial computing, mathematics, and/or statistics courses.*	**Relevant experience includes being responsible for tasks within cyber-related role that may include technical or governance roles. It can include experience of managing a small team, being a team leader, managing a relevant project.*

English Language

You may need to provide evidence of your English language proficiency to study at UNSW, depending on your educational background and citizenship. UNSW requires a minimum level of English language competency for enrolment. English language skills are essential for webinar comprehension and the completion of coursework, assignments and examinations. If English is not your first language, you will need to provide proof of your English proficiency prior to receiving an offer to study at UNSW. You can do this by providing evidence that you meet one or more of the following criteria:

- English language tests and university English courses
- Prior study in the medium of English
- Other qualifications
- English waivers

Recognition of Prior Learning (RPL)

Your previous studies can be acknowledged as credit towards your online postgraduate studies provided that they meet relevant course requirements. If you are eligible for admission and you have undertaken previous studies at another institution, you may be eligible to apply for Recognition of Prior Learning (RPL).

Students can apply for RPL during the program application process and must ensure all relevant supporting documents are submitted for assessment if requested by Admissions, including course outlines from the same year they completed the relevant course/s as content may change over time. Courses successfully completed within the past ten years can be used for credit transfer within a program as provided within the program rules and the University rules on credit.

For the Master of Cyber Security advanced standing may be possible for up to 50% of the program. Advanced standing or exemption can be granted in the program for cases where core courses were completed in a prior program.

- Find out more about RPL and credit transfer at UNSW

Academic leadership

Dr Rahat Masood, Program Director

Dr Rahat Masood is a Lecturer at the School of Computer Science and Engineering at the University of New South Wales. Her research area focuses on the security and privacy of mobile, web, and IoT platforms, network security, and critical infrastructure protection. More recently, her research has involved privacy risks identification and quantification, and privacy-preserving technologies, particularly from a human behaviour perspective. She received her PhD from the UNSW, in collaboration with the information security and privacy group at Data61-CSIRO. Before joining UNSW, she worked as a postdoctoral fellow at Data61-CSIRO, where she designed and evaluated privacy-preserving algorithms as required by diverse application scenarios.

Rahat is currently collaborating with Cyber Security Cooperative Research Centre (CSCRC) and Australian Defence Forces and on multiple cyber security projects. She was also a visiting scholar at the Sandia National Laboratories (SNL), New Mexico, and Cyber Security Policy and Research Institute (CSPRI) at The George Washington University. Her Master's degree is in Computer & Communication Security from NUST School of Electrical Engineering and Computer Science (SEECS), Pakistan, and Bachelor's degree is in Software Engineering (Honours).

Dr Tom Townsend, Program Director

Dr Tom Townsend is a Senior Lecturer at the University of New South Wales Canberra School of Professional Studies, currently teaching the online Master of Cyber Security. With 14 years of teaching experience overlapping with more than 20 years in IT and Cyber focused roles. He also has experience consulting and working across the federal government, predominantly in the areas of architecture and strategy writing.

In 2022, Tom made the transition into full-time academia, focused on teaching in this Master of Cyber Security program and professional development courses. He is also involved in an eclectic range of research encompassing Design Science, Serious Games, Modelling, and Machine Learning. Tom is passionate about giving students an authentic experience that leans on his eclectic professional experience and a keen interest in teaching and learning.

Get in touch

Our Student Enrolment Advisors are here to help you with all your program and enrolment queries.

studyonline.unsw.edu.au

1300 974 990

future-student@studyonline.unsw.edu.au

Have a question?

Book a 15-minute chat with a Student Advisor

Book now →

Apply to UNSW Online

If you're ready to apply, then we're ready to guide you through the application process.

Visit the UNSW website to start your application or book a call with our Student Enrolment Advisors to discuss entry requirements and any questions you may have.

Apply now →

Course descriptions

Data Security and Privacy

Course overview

Security and privacy are related but distinct concepts; they are also some of the defining terms of the 21st century. This course equips student for handling data in secure ways, understanding the nature and principles of privacy, and how to securely identify manage and respond to privacy risks across large datasets and current best practice in a changing global environment.

Cybersecurity Ethics

Course overview

Ethical and professional behaviour are the cornerstone of cyber security. This course provides students with fundamental ethical frameworks, applied to the cyber security profession. Students analyse topics and current and historic cyber events from ethical, professional, and legal perspectives. The course equips students to recognise, effectively analyse, and respond to future ethical challenges as they arise.

Principles of Security Engineering

Course overview

Today, we have the skills and abilities to engineer secure, reliable, physical infrastructure, but we do not possess the same abilities to build secure digital systems.

This course will introduce you to the principles of the emerging field of Security Engineering, where you will apply engineering principles and practices to the design, operation and assurance of secure systems. A systematic, analytic and reflective approach to designing reliable secure systems from unreliable, insecure components.

Cyber Operations

Course overview

This course provides students with a theoretical framework and technical skills for securing modern networks against cyber-attack(s). The course provides you with an overview of modern attacks and modern defensive measures and tools, including strengths and limitations. The course has a practical focus and equips you with the applied technical skills needed to design and secure modern networks.

Students are assumed to have knowledge of basic TCP/IP networking.

Penetration Testing

Course overview

This course provides a theoretical background to the science and art of penetration testing along with an introduction to hands-on skills used in the process of carrying out a tool-based penetration test. The course also provides an understanding of the legal requirements, professional ethical and self-care issues, technical processes, limitations, reporting requirements and communication skills for non-technical audiences.

Cloud Security

Course overview

This course provides an overview of the rapidly growing field of cloud security. The course addresses the ways in which cloud paradigms change the strengths and vulnerabilities of infrastructure compared with traditional computing environments. The course covers paradigms for securing and assuring cloud-based infrastructure at scale.

Cyber and the Law

Course overview

This course provides a survey of the current legal framework related to cyber security including hacking, privacy, surveillance, government powers to intercept data, GIPA, FOI, protection of national infrastructure, copyright, crime, anti-terror legislation, fraud, money laundering, powers of police, whistle-blowers, use of spectrum, GPS, military, agencies, overseas legal regimes such as GDPR and corporate compliance requirements.

The course also looks at the main industry players and how they interact with the legislation and each other. These include ombudsmen, judicial review, privacy commissioners, ministers at state and federal level, agencies, quasi-governmental bodies such as ASCS, AustCyber and CERTS and the role of the police, AFP, DSD, Cyber command, 5 eyes, APT and nation states. Finally, we look at worldwide trends and likely future directions.

Cyber Threats and Crime

Course overview

The internet is revolutionising our society by driving economic growth and offering new ways to connect and co-operate with one another. As with most change, increasing our reliance on cyberspace brings new opportunities but also new threats. While the internet fosters open markets and open societies, this can also make users more vulnerable to criminals, activists and foreign intelligence services that want to harm us by compromising or damaging our critical data and systems.

Activities that fall under this category are often referred to as high tech crime, computer crimes, or cybercrimes.

Technology-enabled crime encompasses:

- Crimes committed directly against computers and computer systems.
- The use of technology to commit or facilitate traditional crimes.

This course outlines the current and emerging trends in cybercrime from a holistic perspective and how they are being countered. It also discusses emerging technologies and how they might be secured and misused.

Cyber Management and Governance

Course overview

Cyber Management and Governance equips you with the skills for weighing competing challenges for the management of cyber and related governance activities in an organisational context. You will learn how to develop cyber strategies, policies and to apply a critical eye to the cyber challenges facing organisations today. Building an understanding of how these governance tools impact people and the efficacy of cyber security controls and practices.

Cyber Risk and Resilience

Course overview

Cyber resilience is the organisational ability to deliver business or operational outcomes despite cyber attack. True resilience is a measure of both business and cyber understanding. This course provides students with the skills necessary to manage contemporary risks through gaining a systematic understanding of the principles and policies for developing the resilience of communities, businesses, and critical systems.

Fundamentals of Coding: C and Assembler

Course overview

This course will teach you how to program to C and low-level assembly language. It forms an introduction to programming in C and a low-level understanding of the underlying operation of modern computers.

C is introduced slowly and at each step we see how C programs are compiled into corresponding machine code and the details of how the computer actually then executes the program.

This course is suitable even if you have never programmed before or have programmed but are not familiar with C, or assembly. or would like a refresher through the lens of cyber security.

Operating System Fundamentals for Security^

Course overview

This course introduces students to the fundamentals of modern operating systems including how they are attacked, their security mechanisms, and countermeasures. It provides an in-depth look at the services provided by modern Operating Systems, from a security perspective.

Advanced Penetration Testing^^

Course overview

This course teaches offensive security. Coverage will be updated to remain current and includes topics drawn from:

- Advanced web application attacks
- Hand-crafted multi stage and non-tool-based attacks
- Layer 2 attacks
- Social engineering
- Stealth, exploit generation and delivery
- Physical attacks
- Insider attacks
- Negotiating appropriate rules of engagement and managing legal risk
- Reporting and ethical professional frameworks for advanced penetration testing
- Red teaming

Assumed knowledge: Students are expected to be familiar with TCP/IP networking across OSI layers 2-7 and programming / scripting in python or equivalent.

^Pre-requisites: completion of Fundamentals of Coding: C and Assembler
^^Pre-requisites: completion of Penetration Testing

Reverse Engineering^

Course overview

This overall aim of this course is to examine the link between high level code written by humans and low level code executed by systems. An understanding of the ways in which these can differ is essential for developing exploitation skills, and for low level defensive design and testing. This course requires entering students to already understand higher level programming languages such as C and low level machine code for common microprocessors such as x86/x64 or ARM. Students learn software assurance and security analysis as well as basic malware analysis.

Digital Forensics^^

Course overview

Digital forensics is an under-represented area of cyber security. It encompasses the processes and technical understanding surrounding both the investigation of computer crimes and crimes where evidence remains on computing devices. This course provides a strong foundation for both those wanting to specialise in this area of cyber security, and those seeking to understand the processes for improved incident response. Students will be able to forensically analyse digital devices and understand the ethical, legal and self care issues associated with cybercrime investigations.

Management and Leadership Capstone Project*

Course overview

This capstone project provides a self-directed learning opportunity, to allow you to apply the skills learned in this program to an exploratory management or leadership project in cyber security. You will have individual responsibility for the timely completion of a significant engineering or research project under the guidance of a member of academic staff. You will be expected to demonstrate a professional level of preparation, planning, execution, testing and documentation. You will be expected to meet a number of strictly enforced milestones and to take considerable initiative in overcoming obstacles.

For more information about assessing The Capstone Project, please check here

^Pre-requisites: completion of Operating System Fundamentals
^Pre-requisites: completion of Operating System Fundamentals and Fundamentals of Coding: C and Assembler
**Pre-requisites: completion of eight units of credit (eight courses)*

Security Engineering Capstone Project^^

Course overview

Capstone Project provides a self-directed learning opportunity, to allow you to apply the skills learned in this program to an exploratory management or leadership project in cyber security. You will have individual responsibility for the timely completion of a significant engineering or research project under the guidance of a member of academic staff. You will be expected to demonstrate a professional level of preparation, planning, execution, testing and documentation. You will be expected to meet a number of strictly enforced milestones and to take considerable initiative in overcoming obstacles.

This project will need to be pre-approved. Example projects include integrating your learning into a business or organisation, directed novel research (either individually or in a group), or a researched paper that benefits the community at large. Example projects include contributing to, or making new software that benefits the community, a directed project to produce novel research (either individually or as a group), conducting a security assessment and providing appropriate feedback, or integrating your new skills into a business or organisation. This course aims to both integrate the skills and knowledge from the different courses within the degree, and also to provide opportunities to focus on areas that interest you.

^^Pre-requisites: completion of eight units of credit (eight courses)