Unit of Study: ICT3053 Cyber Defence

Overview

In this unit, students explore cyber threats from a personal, corporate and national security perspective. Students study the principal motivations behind cyberattacks, which may be political, ideological, revenge, or profit-based. The incidence of such attacks are explored, and examples given of key military and government computing systems being hacked. Students also learn defensive techniques to prevent or mitigate the impact of such attacks through the use of policy, procedure and technical controls.

Course(s)	Bachelor of Information Technology
Credit Points	6 credit points
Duration	12 weeks (10 teaching weeks; 1 revision week; 1 final assessment week))
Level	Undergraduate Advanced
Student Workload	Students should expect to spend approximately 10 hours per week over 12 weeks (totalling approximately 120 hours) on learning activities for this unit.
Mode(s) of Delivery	On campus, Blended
Pre-Requisites	BIS2001 Infrastructure and Networking
Unit Coordinator	As per current timetable
Contact Information	Consultation: 1 hour scheduled session

Unit Learning Outcomes

On successful completion of this unit, students will be able to:

ULO1 Analyse trends in cyberattacks.

ULO2 Compare different types of cyber security threats including cyber terrorism, cybercrime, and cyberwarfare.

ULO3 Analyse the motivation, tactics/strategy, and impacts of cyberattacks.

ULO4 Propose security policy, procedural and technical controls to mitigate the threats of cyberattacks.

Weekly Schedule

Detailed information for each week's activities can be found on Unit's Weekly Modules in Canvas.

Week	Topic
Week 1	Introduction to Cyber Warfare & Cyber Terrorism
Week 2	History of Cyber & Cyber Warriors
Week 3	Weapons of Cyber Aggression
Week 4	History of Cyber Conflict
Week 5	Cyber Defence Techniques part 1
Week 6	Cyber Defence Techniques part 2
Week 7	Non-State Actors
Week 8	Cyber Security Policy
Week 9	Ethics & International Law
Week 10	The Future of Cyber Conflict
Week 11	Revision
Week 12	Final Assessments

Assessments

1. All assessments are compulsory.
2. To pass the unit students must:
   - achieve a total of 50% or more of marks offered; and
   - pass all individual invigilated assessments; and
   - have attempted all assessments.

   Where one or more of these requirements are not met, the Board of Examiners will consider a student's overall progress towards meeting the unit learning outcomes and any special circumstances before reaching a decision.
3. The Board of Examiners may grant a supplementary assessment where a student:
   - achieves a total of 45% or more; and
   - has passed all individual invigilated assessments in the unit; and
   - has attempted all assessments; and
   - has a recommendation for supplementary assessment by the Unit Coordinator and the Head of Discipline.

   Where one or more of these requirements are not met, the Board of Examiners will consider a student's overall progress towards meeting the unit learning outcomes and any special circumstances before reaching a decision. Attendance and engagement in class will be considered.
4. APIC awards common result grades as set out in the [Award of Grade Policy.]()

5. Detailed information for each assessment can be found on the Unit's Home Page and in the Assessment Brief.

Assessment Task	Type	Weighting	Due	Length	ULOs
Assessment 1: 5 X Weekly Workshop Activity (Cyber defence blog) Each student will be assigned a set of topics that cover facets of Cyber Defence They will create a short 'news' item on the allocated topic aimed at evaluating the attack and defence mechanisms, which may include description, underpinning concepts, and financial impact/concerns, etc.	Individual	25%	Week 2, 4, 6, 8 and 10	500 words each week (Total 2500 words)	ULO1 ULO2 UL03 UL04
Assessment 2: Cyberattacks Analysis Report Students will complete a report on the broad issue of cyberattacks, including an extended analysis of one or two particular aspects of the issue.	Individual	20%	Week 5	Analysis Report (equiv. 2000 Words)	ULO2 ULO3 ULO4
Assessment 2: Case Study Students will analysis specific cyber events to examine the actors' motivations, strategy adopted, impacts, and potential defensive strategies and present the report along with group members.	Group	30%	Week 8	3500 words + Analysis presentation (equiv. 1500 words)	ULO3 ULO4
Assessment 4: Analysis Report - Cyberattacks and defensive issues and strategies. Students will report on a specific topic. In the report, students will discuss ethical and social issues (including personal liberty, legality, etc.) related to cyberattacks and defensive strategies. Students will present and defend their analysis in a Pecha Kucha presentation.	Individual Invigilated	25%	Week 11, 12	2500 words + Analysis (equiv. 1500 words)	ULO1 ULO2 ULO3 ULO4

Equiv. – equivalent word count based on the Assessment Load Equivalence Guide.

Course Reserve

Course Reserve includes all required resources and reading material for the unit of study. You can access Course Reserve via APIC Library or via the Course Reserve link on the unit's homepage.

Prescribed text(s):

Chapple, M. and Seidl, D., 2021. Cyberwarfare: Information operations in a connected world. Jones & Bartlett Learning.

Recommended Readings:

Walker, M. (2019). CEH certified ethical hacker exam guide (Fourth edition. ed.). New York: McGraw-Hill Education.

Charles P, P. and Shari Lawrence, P., 2015. Security in Computing FIFTH EDITION.

Manjikian, M., 2019. Introduction to cyber politics and policy. CQ Press.

Stallings, W., 2011. Cryptography and network security: principles and practice.

Academic integrity

Ethical conduct and academic integrity and honesty are fundamental to the mission of APIC and academic misconduct will not be tolerated by the College. It is the responsibility of every student to make sure that they understand what constitutes academic misconduct and to refrain from engaging in it. Please refer to APIC's Academic Integrity Policy for further details.

Other Important Information and Links

Special consideration If your academic work is impacted by significant documented illness, hardship, or other adverse circumstances beyond your control, you may make an application for Special Consideration. Please refer to the Assessment Policy for further details.	**Late submission** Penalties apply when work is submitted after the due date without approval. Please refer to the Assessment Policy for information about late submission.
Assessment appeals If you are concerned about a mark you have received for an assessment or final grade, you may apply to formally appeal the grade. Please see the Assessment Policy for further details.	**Award of grades** APIC awards common result grades, set out in the Award of Grade Policy.
Expectations of student conduct Students are expected to conduct themselves in a manner that is consistent with a safe and respectful study environment. More information can be found in the Student Code of Conduct.	**Study resources** APIC Library and Student Learning Support resources and services can be accessed via the Student Lounge or your Dashboard on the OLS (Canvas).

Student Services	Key dates
The Student Services team provides administrative support for students and handles enquiries about enrolment, timetables, important dates and submitting forms. More information can be found on the Student Services page on the OLS (Canvas).	Key dates through the academic year, including teaching periods, census, payment deadlines and exams can be found on the Academic Calendar section of the APIC website.

Changes and Updates to the Unit of Study Guide

This Unit of Study Guide may be updated and amended from time to time. Students will be notified of any changes to the unit via the Online Learning System (Canvas) space for the unit.

This Unit of study Guide was last modified on 2 May 2024.