ICT3053 Cyber Defence

Unit Description

Cyber threats come in many forms, including cybercrime, cyber espionage, and cyberattacks on critical infrastructure. These threats can cause significant harm to national security by disrupting critical systems, stealing sensitive information, and undermining public confidence in government institutions.

'Cyber defence' is essential in today's digital world to protect digital assets from cyber threats. It is an ongoing effort that requires a comprehensive approach to ensure the confidentiality, integrity, and availability of digital assets.

Cyber defence is the practice of protecting computer systems, networks, and data from unauthorised access, use, disclosure, disruption, modification, or destruction. It encompasses a variety of security controls and measures that are designed to detect, prevent, and respond to cyber threats.

Credit Points	6 credit points
Duration	12 weeks (10 teaching weeks and 2 revision and assessment weeks)

Unit Learning Outcomes

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

1. Analyse trends in cyberattacks.
2. Compare different types of cyber security threats including cyber terrorism, cybercrime, and cyberwarfare.
3. Analyse the motivation, tactics/strategy, and impacts of cyberattacks.
4. Propose security policy, procedural and technical controls to mitigate the threats of cyberattacks.