Prifysgol Wrecsam
Wrexham University

Module specification

When printed this becomes an uncontrolled document. Please access the Module Directory for the most up to date version by clicking on the following link: Module directory

Module Code	COM575
Module Title	Cyber Operations
Level	5
Credit value	20
Faculty	FACE
HECoS Code	100376
Cost Code	GACP

Programmes in which module to be offered

Programme title	Is the module core or option for this programme
BSc (Hons) Cyber Security	Core
BSc (Hons) Cyber Security with Industrial Placement	Core

Pre-requisites

None

Breakdown of module hours

Learning and teaching hours	20 hrs
Placement tutor support	0 hrs
Supervised learning e.g. practical classes, workshops	10 hrs
Project supervision (level 6 projects and dissertation modules only)	0 hrs
Total active learning and teaching hours	**30** hrs
Placement / work based learning	0 hrs
Guided independent study	170 hrs
Module duration (total hours)	**200** hrs

For office use only	
Initial approval date	08/11/2023
With effect from date	Sept 2025
Date and details of revision	
Version number	1

Module aims

The Cyber Operations module is designed to provide students with a comprehensive understanding of the principles, strategies, and techniques involved in cyber operations. This module explores the various aspects of offensive and defensive cyber operations, focusing on the tools, methodologies, and best practices used in the field. Students will develop practical skills and knowledge required for cybersecurity professionals engaged in protecting and securing digital assets.

Module Learning Outcomes - at the end of this module, students will be able to:

1	Identify and describe key terminology and definitions related to cyber operations
2	Recognise the principles and benefits of access control models and their roles in security deployments.
3	Explain the principles behind cyber operations concepts and their real-world applications.
4	Apply cyber operations concepts and principles to analyse and mitigate cyber threats.
5	Evaluate the suitability of different strategies in addressing specific security requirements within an organisation.

Assessment

Indicative Assessment Tasks:
This section outlines the type of assessment task the student will be expected to complete as part of the module. More details will be made available in the relevant academic year module handbook.

The assessment strategy for this module is primarily focused on a portfolio assessment approach, constituting 100% of the overall assessment weight. Throughout the module, students will engage in weekly or bi-weekly portfolio tasks designed to reinforce, consolidate, and expand upon their learning experiences. These portfolio tasks serve as opportunities for students to demonstrate their understanding, application, and critical analysis of the concepts and skills taught in the module.
The portfolio tasks are carefully designed to cover a wide range of topics and learning outcomes, ensuring a comprehensive assessment of students' knowledge and abilities in the field of study. Each task may require students to showcase their understanding of key principles, theories, and frameworks related to cyber operations. Additionally, they may be asked to apply their knowledge in practical scenarios by analysing case studies, solving problems, or completing hands-on exercises.

Assessment number	Learning Outcomes to be met	Type of assessment	Weighting (%)
1	1,2,3,4,5	Portfolio	100%

Derogations

None

Learning and Teaching Strategies

Aligned with the principles of the Active Learning Framework (ALF), the module will incorporate a blended digital approach utilising a Virtual Learning Environment (VLE). These resources may include a range of content such as first and third-party tutorials, instructional videos, supplementary files, online activities, and other relevant materials to enhance their learning experience

Indicative Syllabus Outline

Indicative syllabus includes topic areas that may include:

- CyberOps Concepts
- Attacks and Threats
- Security Deployments
- Defence in Depth
- Access Control Models
- Security Monitoring
- Host Based Analysis
- Network Intrusion Analysis
- Security Models
- SOC Metrics

Indicative Bibliography:

Please note the essential reads and other indicative reading are subject to annual review and update.

Essential Reads

O. Santos, *Cisco CyberOps Associate 200-201*, Cisco Press, 2021.

Other indicative reading

M. O'Leary, *Cyber Operations: Building, Defending, and Attacking Modern Computer Networks.* Apress, 2019.

K. Knereler, C. Parker, C. Zimmerman, *11 Strategies of a world class Cybersecurity Operations Centre,* Mitre, 2022.