Module Specification

Global Landscapes of Cyber Security and Adversaries

Version: 2024-25, v1.0, 11 Jan 2024

Contents

Part 1: Information

Module title: Global Landscapes of Cyber Security and Adversaries

Module code: UFCE88-30-3

Level: Level 6

For implementation from: 2024-25

UWE credit rating: 30

ECTS credit rating: 15

College: College of Arts, Technology and Environment

School: CATE School of Computing and Creative Technologies

Partner institutions: None

Field: Computer Science and Creative Technologies

Module type: Module

Pre-requisites: None

Excluded combinations: None

Co-requisites: None

Continuing professional development: No

Professional, statutory or regulatory body requirements: None

Part 2: Description

Overview: The module focuses on global, regional and national actors of cyber security and adversaries. Employing global perspective, the module pays specific attention to geopolitical, socio-cultural, and ethical aspects of cyber security.

Features: Not applicable

Educational aims: The module aims to develop critical thinking and global perspective among cyber security and digital forensics students.

Outline syllabus: The module broadly focuses on global dynamics of cyber security, the relationship between nation states and threat actors, adversarial behaviours and key actors and adversaries that dominate this landscape.

It considers:

What Constitutes cyberwarfare and it's relationship to cyber-crime

Threat actors including Cyber-activists (a.k.a. hacktavists), APT groups and Terrorists.

Politico-social motivations of threat actors, and how these interact with nation-state activities

Part 3: Teaching and learning methods

Teaching and learning methods: The module is delivered through a series of lectures and seminars.

Module Learning outcomes: On successful completion of this module students will achieve the following learning outcomes.

MO1 Demonstrate understanding of the geopolitical impact on cyber security

MO2 Critically appraise factors contributing to adversarial behaviour

MO3 Demonstrate evaluation of the impact of global and regional policies regulating the cyber security landscape

MO4 Reflect on professional development to date, and evaluate experience to enhance employability and career prospects

Hours to be allocated: 300

Contact hours:

Independent study/self-guided study = 228 hours

Face-to-face learning = 72 hours

Total = 300

Reading list: The reading list for this module can be accessed at readinglists.uwe.ac.uk via the following link https://rl.talis.com/3/uwe/lists/A751FA25-CA25-274B-F941-0DE6526BBF44.html?lang=en&login=1

Part 4: Assessment

Assessment strategy: The module engages students in a practical assessment - through a simulation of a cyber-security crisis. Students are presented with a scenario, and they will be required to work in their allocated teams. Four aspects could be addressed:
Evaluate the situation and identify key factors impacting the crisis;
Decide on the response to the situation by factoring geo-political dynamics;
Present solution/s and explain reasons for the specific response;
Consider and outline key skills developed by undertaking the module and reflect on key skills/knowledge utilized during assessment.

The resit will be a similar exercise where students will have the opportunity the repeat the first-sit exercise with a different scenario but feedback on how they failed to meet the learning objectives at the first sit.

Assessment tasks:

Practical Skills Assessment (First Sit)
Description: A crisis simulation exercise involving students to work in teams to consider, address and propose resolution.
Weighting: 100 %
Final assessment: Yes
Group work: Yes
Learning outcomes tested: MO1, MO2, MO3, MO4

Practical Skills Assessment (Resit)

Description: A crisis simulation exercise involving students to work in teams to consider, address and propose resolution.
Weighting: 100 %
Final assessment: Yes
Group work: Yes
Learning outcomes tested: MO1, MO2, MO3, MO4

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Cyber Security and Digital Forensics [NepalBrit] BSc (Hons) 2022-23

Cyber Security and Digital Forensics [Frenchay] BSc (Hons) 2022-23

Cyber Security and Digital Forensics {Foundation} [Sep][FT][Frenchay][4yrs] BSc (Hons) 2021-22