MODULE **DESCRIPTOR**

MODULE TITLE	CYBER DEFENCE		
MODULE CODE	CO4710 (L7)	**CREDIT VALUE**	20 UK CREDITS / 10 ECTS
SCHOOL	SCHOOL OF SCIENCES		

MODULE **AIMS**

The aims of this module are to:

•Provide an in depth understanding of theoretical and practical aspects of network defence
•Understand the defence in depth concept
•Gain experience in using tools and techniques for cyber defence

MODULE **CONTENT**

Foundation:

- Security attacks, real world cases, security objectives, footprints, network forensics, investigative methodology (OSCAR)

Layered defence strategy cover topics such as:

- Security policies: benefits, success factors, policy types, components. Guidelines for policy development
- Contingency planning: benefits, components of contingency planning, incident response, disaster recovery, business continuity
- Cryptography: PKI, TLS/SSL, PGPs, architectures, main components, principles of operation, examples, trust models, key management
- Firewalls: fundamentals, hardware/software firewalls, filtering technologies, challenges, advantages/disadvantages, next generation firewalls, architectures, firewall policy
- Intrusion detection and prevention systems: fundamental concepts, detection methodologies, benefits, network based, host based, components, topologies
- Threat intelligence: concepts, honeypots, sandboxes, analytical frameworks such as the Lockheed Martin Cyber Kill Chain, the Diamond Model, the MITRE ATT&CK™ Framework, threat intelligence process, threat feeds, visual analytics
- Ransomware: types, evolution and facts, operation, techniques, incident handling, protection

Network

- Sources of Network-Based Evidence (i..e.: Switches, routers, DHCP servers, DNS servers, IDS, IPS, firewalls)
- Evidence acquisition: Physical interception, traffic acquisition software, active acquisition
- Packet Analysis: Protocol analysis tools and techniques, packet analysis tools, case study
- Event Log Aggregation Correlation and Analysis: Sources of logs, log architecture, collecting and analyzing evidence, case study

INTENDED **LEARNING OUTCOMES**

On successful completion of this module a student will be able to:

1. Identify and assess tools and techniques for cyber defence
2. Conduct network packet and network forensics analysis
3. Critically discuss and evaluate evidence collection
4. Research and report on security attacks, cyber defence techniques and tools

TEACHING METHODS

The theoretical material will be delivered during the lectures. The students are expected to actively participate and prepare for workshops, assessment briefs and other matters relating to the acquisition and evaluation of network evidence. During the workshops, students will be introduced to cyber defence tools and techniques. Synchronous (i.e. in class) and/or asynchronous (i.e. blogs) discussions will take place to further discuss the students' practical findings. As a result of the discussions, additional directed reading may be required. There will be occasions when speakers from leading security organisations will be invited to share their industry experiences with the students.

Distance Learning

The module tutor will deliver the theoretical material through live online lectures in Adobe Connect. During the live lectures the participating students will have the opportunity to engage in discussions, present their views and ask questions. The lecture sessions will be recorded and made available to the students through Blackboard. Students who cannot participate in the live lectures will have the opportunity to answer and reflect on guided questions in the subsequent live lectures or participate asynchronously on discussion boards. Where appropriate, students will also be provided with relevant further reading, web links and resources for independent study. Speakers from leading security organizations will be invited, where possible, to deliver live invited talks and enhance the students' experience.

. Virtual laboratories will be utilized to give the opportunity to students to apply their practical skills. Students will be provided with access to virtual laboratories through which they will be able to complete the practical components of the module. The students will obtain the practical sheets from Blackboard and they are expected to follow the instructions included in the practical sheets to complete the lab work. If students have difficulties with a particular exercise, they are expected to contact the module tutor or post a question on the discussion forum, where the module tutor and their peers can provide feedback. Different means of communication will be utilized by the tutor to offer support to the students based on the reported issue, i.e. email, Skype, MS Teams, virtual laboratory, etc.

Through the virtual laboratories, the students are expected to apply their theoretical knowledge to solve security problems in a professional and legal way. Feedback to the students will be provided asynchronously through Blackboard. If the need arises, the module tutor will schedule live sessions to provide further feedback to the students.

ASSESSMENT METHODS

This module is assessed through a report and an examination.