# MODULE **DESCRIPTOR**

| | | | |
|---|---|---|---|
| **MODULE TITLE** | CYBER WARFARE | | |
| **MODULE CODE** | CO4709 (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 how cyber-attacks and defence intersect with each of the classic warfighting domains.
•Identify and discuss tactics, techniques and procedures of Computer Network Operations, including attack, defend and exploit plus the aspect of social engineering.
•Explore various current cyber threats including ethics and legal issues.

## MODULE **CONTENT**

**Fundamentals**

- What is Cyber Warfare: Definition, Tactical and Operational Reasons, Importance, Case Studies
- Non-State Actors in Computer Network Operations: Individual Actors (Script Kiddies, Malware Authors, Scammers, Blackhats, Hactivists, patriot Hackers), Corporations, Cyber Terrorism, Organized Cyber Crime, Autonomous Actors

**Legal Status of Cyber Warfare and Ethics**

Legal System Impacts and Ethics: Legal Systems, Privacy Impacts, Digital Forensics, Ethics in Cyber warfare

**Cyberspace Battlefield**

- Weaponizing malware: trends, categories, behavior, propagation, malware for hire
- Physical Weapons: Physical and Logical Realms connection, Infrastructure Concerns / SCADA
- Psychological Weapons: Social Engineering, SE Tactics Techniques and Procedures approaches and methodologies.
- Logical Weapons: Reconnaissance tools, Scanning Tools, Access and Escalation Tools, Exfiltration Tools, Sustainment Tools, Assault Tools, Obfuscation Tools. Understand that the tools used in a cyber warfare context are often not conceptually different than the tools utilized in everyday penetration testing of applications, but realize that the scope of their use is greatly increased in a cyber warfare scenario.
- Computer Network Exploitation: Intelligence and Counter Intelligence, Reconnaissance, and Surveillance in a cyber warfare context.

**Cyber Doctrine & Cyber Warriors**

- Doctrine Strategy form around the world, Defending against Cyber attacks, What to protect, Guidance and Directives, operations and Exercises, Security Awareness and Training, Cyber warrior certifications / training / experience skills, Cyber Warfare Forces.

**Cyberspace challenges and the Future of Cyber War**

## INTENDED **LEARNING OUTCOMES**

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

| | |
|---|---|
| 1. | Evaluate and compare theoretical and practical aspects of cyber warfare. |
| 2. | Critically discuss and assess the significance of logical, physical and psychological weapons used in Cyber Warfare. |
| 3. | Identify and assess computer network exploitation, attack and defence processes. |
| 4. | Research and Report on Legal System Impacts and Ethics in Cyber Warfare. |

## TEACHING METHODS

The theoretical material will be delivered during the lectures. Some of the content will be presented by a mixture of student led seminars and build-up of various penetration scenarios. The students are expected to actively participate and prepare for workshops, assessment briefs and other matters relating to the creation of penetration tests and evaluations. There will be occasions when speakers from leading security organisations will be invited to share their industry experiences with the students. During the workshops, students will be introduced to the main existing security tools (students may be asked to carry out security tests in a controllable testing environment as well as other practical work). Furthermore, synchronous (i.e. in class) and/or asynchronous (i.e. blogs) discussions will take place for the students' to discuss their practical findings. As a result of the discussions, additional directed reading may be required.

**Distance Learning**

The module tutor will deliver live online lectures through 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 posted by the module tutor asynchronously, through a Blackboard discussion forum. The tutor will provide appropriate feedback to students' comments posted on the discussion board. Students will also be provided with relevant further reading, web links and resources for independent study. Similarly, to lectures, student led seminars will be delivered using Adobe Connect and/or student led forums. Also, speakers from leading security organizations will be invited, where possible, to deliver live invited talks and enhance the students' experience.

Workshops will be delivered through live sessions e.g. through MS Teams., Where necessary, virtual laboratories will be utilized to give the opportunity to students to apply their practical skills. The students will obtain the practical worksheets from Blackboard and they are expected to follow the instructions included in the practical worksheets 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 laboratories, etc. 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.