Cyber & Information Warfare Leadership Course

Who should attend?

This course is designed for military personnel, defence leaders, and those operating within or alongside military and security environments. It is particularly relevant for:

- **Operational planners and commanders**
- **Intelligence and information operations personnel**
- **Defence policy and strategy staff**
- **Personnel operating in joint or multi-domain environments**

No advanced cyber knowledge is required. The course focuses on operational awareness, decision-making, and battlespace understanding.

Key Organisations

Ministry of Defence

NATO and Allied Forces

Defence Intelligence and Security Organisations

Joint and Multi-Domain Task Forces

Government Security and Defence Agencies

Introduction

Modern conflict no longer exists solely in the physical domain. It now spans cyber, information, and cognitive environments, where adversaries exploit technology, data, and human perception to gain advantage.

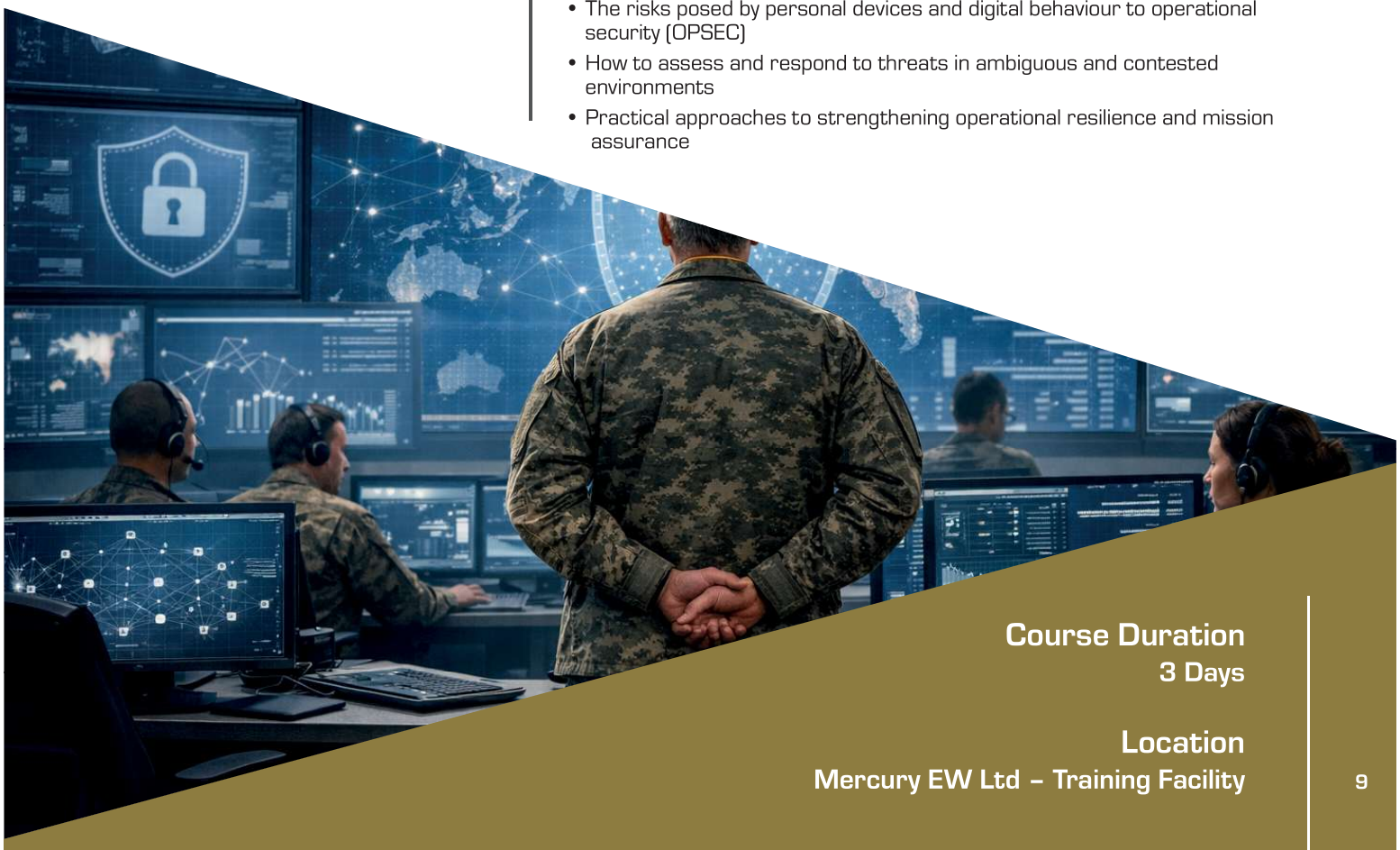
This programme develops operational cyber and information warfare awareness, enabling personnel to understand how hybrid conflict, deception, artificial intelligence, and influence operations shape the modern battlespace.

Through real-world military case studies, strategic discussion, and scenario-based exercises, participants will explore the complexity of operating in contested environments, where attribution is unclear, information is manipulated, and decisions must be made under pressure.

The course enhances situational awareness, operational judgement, and resilience, preparing personnel to operate effectively in modern multi-domain operations.

What you will learn:

- How cyber operations integrate into modern warfare and hybrid conflict
- The role of information warfare, influence, and cognitive operations
- How adversaries exploit social media, data, and perception in conflict environments
- The impact of ransomware and infrastructure disruption on national security
- Legal and ethical considerations in cyber-enabled military operations
- The role of artificial intelligence, deepfakes, and synthetic media in the battlespace
- How cyber supports and shapes kinetic operations
- The risks posed by personal devices and digital behaviour to operational security (OPSEC)
- How to assess and respond to threats in ambiguous and contested environments
- Practical approaches to strengthening operational resilience and mission assurance



Course Duration
3 Days

Location
Mercury EW Ltd – Training Facility