mercury

EW & Defence Training Services

Course Brochure

2026 - 27

Contents

Scan the QR code to view our full range of services and start your training journey with Mercury EW

General Course Information

Introduction

Mercury EW Ltd is a veteran owned company populated by His Majesty's Forces professionals who have extensive operational and technical expertise in the field of EW and intelligence. We pride ourselves on delivering high quality, customer-focused, training and consultancy services to the international Defence Industry. We have developed an expansive portfolio of training solutions through working with the UK Ministry of Defence (MOD), as well as Armed Forces and capability providers spanning 24 countries, including those within the Middle and Far East regions. Our services include; consultancy, operational support, and training analysis, design, development, and delivery.

Training Design and Delivery

Mercury EW Ltd training staff are all certified Defence Trainers, skilled at designing and delivering engaging and inclusive training to customers of all backgrounds and experience. Our courses can be tailored from foundation level to deep technical expertise, always enriched by a variety of operational, real-world examples.

We conduct all training design and development in alignment with the UK Ministry of Defence's (MoD) Joint Service Publication 822 – Defence Systems Approach to Training (DSAT) or international equivalent. The DSAT process aims to ensure that all training courses are fit for purpose by being designed for the operational role(s) in question.

Each course is supported with a formalised document set, providing a recognised audit trail for the customer. A typical Course Document Set (CDS) could include: a Formal Training Statement (FTS) (details all elements of a job to be taught, including the conditions and standards expected); course material (PowerPoint, student exercises, etc.); Learning Specifications (LSpecs) (used to assist an instructor in delivering all aspects of each lesson); Assessment Strategy (AStrat); student/user handbooks; and a Training Authorisation Document (TRaD) (used for the management and change control of training). Mercury EW Ltd use a blend of learning material to enhance their courses e.g. visual slides, practical syndicate exercises, equipment simulation, and scenario generation.

Bespoke Requests

All courses can be tailored to your organisation's needs, with flexible durations and adaptable syllabuses available on request. Course content and learning objectives of each course can be recognised and fully validated by a leading UK University. On successful completion of an accredited course students gain recognised University awarded Credit Accumulation Transfer Scheme (CATS) points at either PG Certificate or PG Diploma level.

Training Facilities

All courses outlined in the brochure can be delivered at Mercury EW Ltd's training facility, with many also available at the customer's chosen location. This includes software-driven practical training serials, subject to stable connectivity. We also have the capability to deliver our portfolio of training courses virtually if required.

Mercury EW Ltd.'s new training facility located at the Head Office in Haverholme Priory Offices offers the following amenities:

- Modern conference room facilities
- Fully interactive touchscreen whiteboards and Epson HD short throw projectors
- Integrated 10Gbps Local Area Network (LAN)
- Powerful HP Windows 11 Pro student workstations with Dell Ultra-Wide HD monitors
- Real time distribution of training media to student monitors
- Private car parking
- Student rest area
- Separate room for religious requirements

Mercury EW Ltd can also provide comprehensive administrative and logistical support for all courses, including:

- Airport transfers
- Arranging suitable accommodation, hotel or rented
- Catering available from simple refreshments to full buffet lunch
- Local information packs
- Additional services upon request

Conclusion

This brochure is designed to provide an overview of the courses available for delivery by Mercury EW Ltd. A detailed breakdown of each course syllabus and provisional costings can be provided on confirmation of the customer training requirement.

Radar Theory and Electromagnetic Intelligence [ELINT] Course

Introduction

This course provides an overview of the background, history, and key operating principles in modern radar technology. It covers both earlier legacy systems and more recent developments, including Quantum radar and the integration of AI. Participants will learn about the role of radar in both military and civilian applications. The course includes theoretical instruction and practical demonstrations. Attendees will gain knowledge of the parameters used in modern radar systems and examine how adjustments to these parameters and physical components can affect performance and operational capabilities.

What you will learn:

- Introduction to the History of Radar
- Principles of Operation
- Antenna Theory in Radar
- Introduction to Electromagnetic Intelligence
- Types of Radars
- Radar Functions
- Interpulse Modulation Techniques
- Pulse Compression Techniques
- Measurable Radar Pulse Parameters
- Radar Calculations
- Radar against Modern Electromagnetic Support Measure (ESM) & Electromagnetic Counter Measure (ECM) Technology
- Radar in Modern Warfare
- Artificial Intelligence (AI) integration in Radar
- Quantum Radar

Who should attend?

Military and government civilian EW practitioners engaged in the technical analysis of Electromagnetic Intelligence (ELINT) data. Ideally suited for experienced ELINT technical data analysts.

Key Organisations

Ministry of Defence

HQ Joint, Army, Navy and Air Force ELINT operators/Analysts

All Government agencies, industries and organisations interested in operational and technical aspects ELINT

Course Duration

1 Week

Location

Mercury EW Ltd – Training Facility

Electromagnetic Intelligence (ELINT) Technical Analysis Course [Foundation]

Who should attend?

Military and government civilian EW practitioners engaged in the technical analysis of ELINT data. Ideally suited for experienced ELINT technical data analysts.

Key Organisations

Ministry of Defence

HQ Joint, Army, Navy and Air Force ELINT operators/Analysts

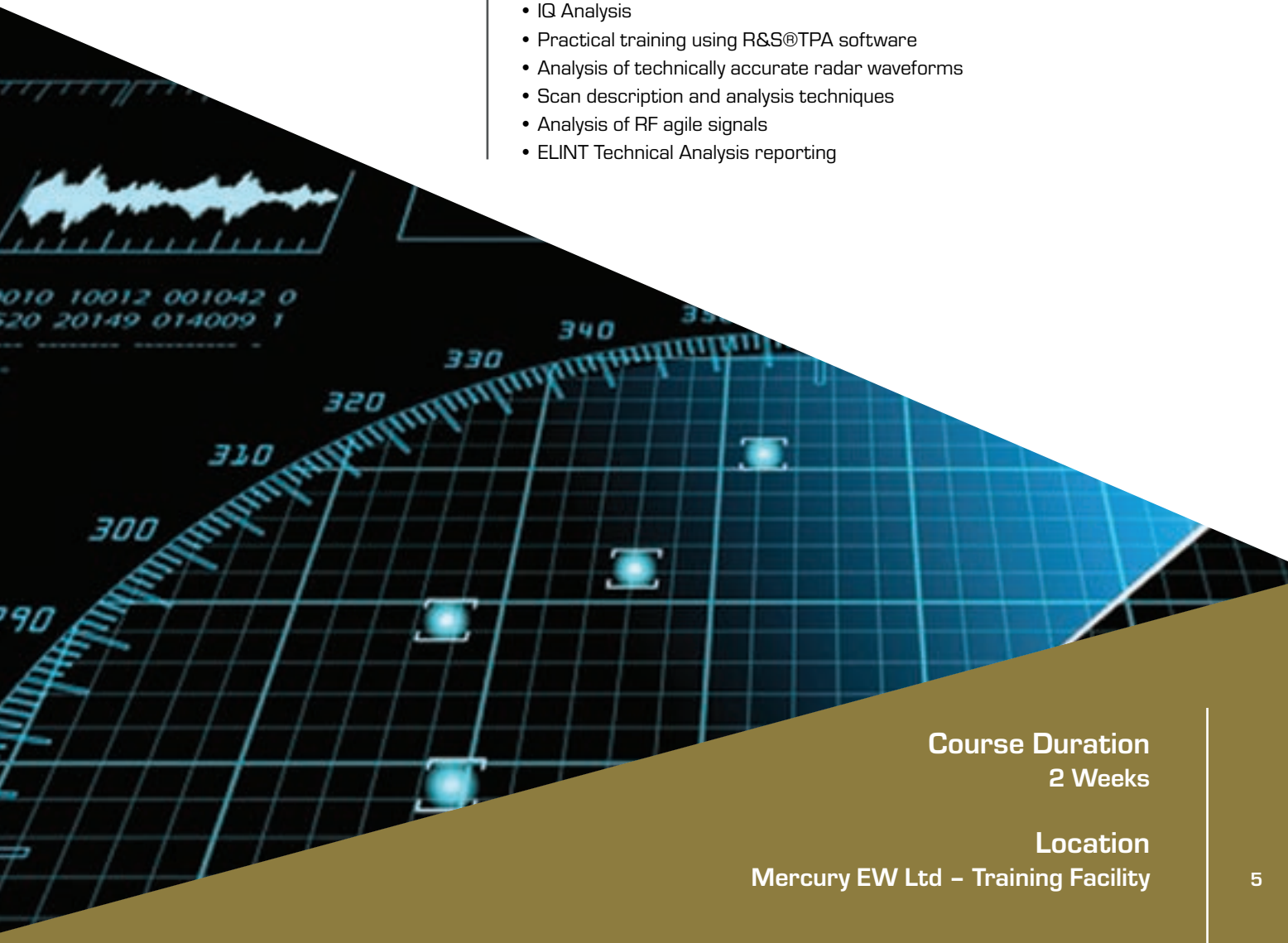
All Government agencies, industries and organisations interested in operational and technical aspects ELINT

Introduction

This course covers the principles from our theoretical course and progresses to focus on key components of ELINT Technical Analysis, aiming to provide participants with an operational overview of ELINT and its function in modern warfare. The curriculum includes both theoretical and practical lessons. Practical sessions utilise the R&S®TPA software suite, which allow participants to perform technical analysis of ELINT data. By combining theoretical instruction with the application of the R&S®TPA software, participants can develop knowledge of radar system parameters and the skills necessary for ELINT analysis and reporting.

What you will learn:

- Major ELINT Signal Parameters
- Radar theory and Electronic Intelligence [ELINT]
- Radar equations and constraints
- ELINT interception system characteristics
- Characteristics of a pulse
- Intrapulse modulation description and analysis techniques
- Pulse Train Deinterleaving
- Introduction to ELINT Technical Analysis procedures
- Introduction to Pulse Analysis Tool – real time Pulse Descriptor Word (PDW) collection and analysis tool
- PDW Analysis
- IQ Analysis
- Practical training using R&S®TPA software
- Analysis of technically accurate radar waveforms
- Scan description and analysis techniques
- Analysis of RF agile signals
- ELINT Technical Analysis reporting



Course Duration
2 Weeks

Location
Mercury EW Ltd – Training Facility

Electromagnetic Intelligence [ELINT] Technical Analysis [Advanced]

Introduction

This comprehensive course is designed for delegates aspiring to achieve a high level of proficiency in the field of technical Electronic Intelligence (ELINT) analysis. The curriculum begins by establishing a solid foundation in the essential theories that underpin ELINT. From this base, the training progresses to explore the advanced features of the R&S®TPA software using a modular approach that will start with simple waveforms and culminate in the practical analysis of modern, highly complex radar systems and techniques.
The learning journey is structured to guide delegates from the analysis of basic waveforms through to the complexities of modern, complex radar signals. Throughout the course, a detailed examination of all common radar modulation techniques and types will be conducted. A significant emphasis is placed on practical application; delegates will have extensive hands-on opportunities to analyse each type of signal. This practical experience is further enhanced by training that focuses on operational ELINT collection, utilising ERA's synthetic radar simulator.

Upon completion, participants will not only possess a deep theoretical understanding but will also have honed the practical skills necessary to produce industry-recognised analysis reports, marking them capable and proficient ELINT analysts.

Who should attend?

Military and Civilian Radar and EW practitioners from both Operational and Engineering backgrounds. Programme & Project Managers, Systems Engineers and Technical Staff.

Key Organisations

Ministry of Defence

Defence Science and Technology Agencies

Defence Research Lab/Institutes

All Government agencies, industries and organisations interested in development of EW capability

What you will learn:

- Radar theory and Electronic Intelligence (ELINT)
- Major ELINT signal parameters
- Radar equations and constraints
- ELINT interception system characteristics
- Characteristics of a pulse
- Interpulse modulation description and analysis techniques
- Intrapulse modulation description and analysis techniques
- Pulse train deinterleaving
- Introduction to ELINT technical analysis procedures
- Introduction to Pulse Analysis Tool – Realtime Pulse Descriptor Word (PDW) collection and analysis tool
- Advanced PDW analysis
- Advanced IQ analysis
- Analysis of Frequency-Modulated Continuous Wave (FMCW) signals
- Practical training using R&S®TPA software
- Analysis of technically accurate radar waveforms
- Scan description and analysis techniques
- Analysis of RF agile signals
- ELINT technical Analysis reporting
- Introduction to ELINT parametric databases

Course Duration
3 Weeks

Location
Mercury EW Ltd – Training Facility

Mission Data Engineering Course

Who should attend?

Military and civilian radar and EW practitioners from both operational and engineering backgrounds. Programme & project managers, systems engineers and technical staff. Anyone involved in formulating strategy, policy, doctrine, processes or procedures for EW reprogramming capability in a deployed, operational context.

Key Organisations

Ministry of Defence

HQ Joint, Army, Navy, and Air Force EW operators/Analysts

All Government agencies, industries and organisations interested in operational and technical aspects of EW reprogramming

All Government agencies, industries and organisations interested in development of EW capability. development of COMINT/EW capability

Introduction

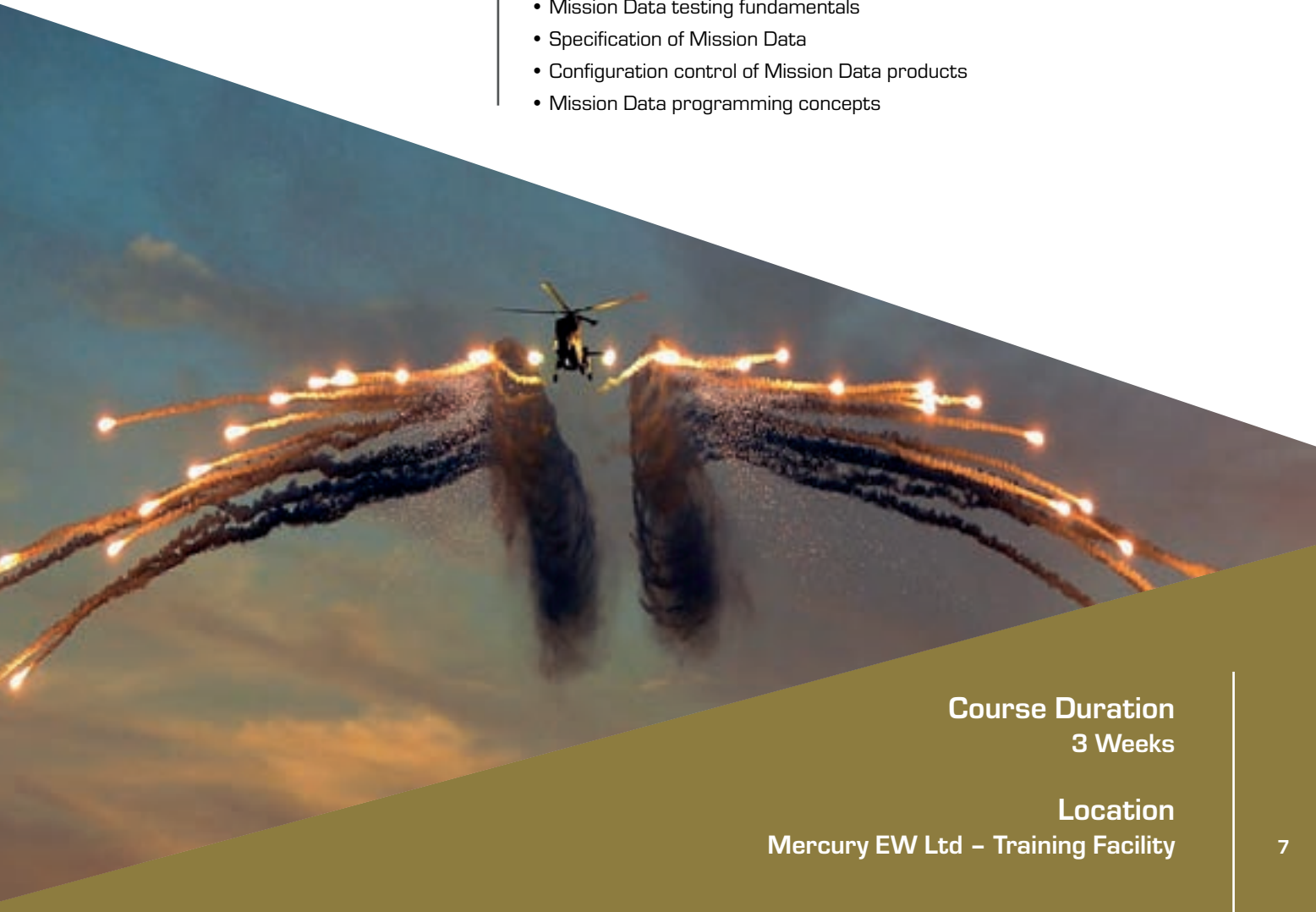
The Mission Data Engineering course is designed to inform and introduce students to the key principles of Mission Data Engineering along with the development of an Agile lifecycle process. This includes gathering your organisational requirements with regards to the Mission Data lifecycle along with implementing and evolving the processes and procedures to meet these requirements through a variety of methods.

This is an interactive experience using a combination of lecture, hands-on practical exercises, and student-instructor interaction. The course will also facilitate a number of practical based exercises designed around realistic scenarios in order to consolidate student learning. It is this combination of skills that will enable your organisation to keep pace with this fast-moving arena and develop an indigenous capability toward the future.

The course is designed to allow your operational personnel to apply and manage the principles of Mission Data Engineering in a practical way. It is desirable to have completed basic radar theory / radar fundamentals prior to this course.

What you will learn:

- Overview of an Agile Mission Data Development Lifecycle (MDDLC)
- Introduction to MDDLC Management
- Developing Mission Data requirements
- Mission Data testing fundamentals
- Specification of Mission Data
- Configuration control of Mission Data products
- Mission Data programming concepts



Course Duration
3 Weeks

Location
Mercury EW Ltd – Training Facility

Cyber and Electromagnetic Activities [CEMA] Awareness Course

Introduction

The foundation course provides a comprehensive introduction to Cyber and Electromagnetic Activity [CEMA] for defence professionals who may find themselves operating within or in parallel to the CEMA environment. It covers the key principles, risks, and capabilities associated with the cyber domain and the electromagnetic spectrum, including operational contexts and strategic implications. Participants will gain critical awareness of how CEMA impacts command, control, communications, intelligence, and mission success across the modern battlespace.

What you will learn:

- Cyber and Electromagnetic Activity [CEMA] components
- Strategic importance of CEMA in complimentary military operations
- Common threats, vulnerabilities, and adversary capabilities in the cyber and electromagnetic domains
- The role of CEMA in force protection, command assurance, and operational planning
- Awareness of NATO and allied CEMA frameworks, tools, and terminologies
- Application of CEMA awareness to improve resilience and collaboration in joint operations

Who should attend?

Personnel from international Ministries of Defence (MODs), operators or managers newly assigned to CEMA-related roles, leaders requiring situational awareness of CEMA's influence on operations and Defence contractors or support staff working in CEMA-enabled environment.

Key Organisations

Ministry of Defence

HQ Joint, Army, Navy and Air Force EW operators/Analysts

All Government agencies, industries and organisations interested in operational and technical aspects of EW

Course Duration
1 Week

Location
Mercury EW Ltd – Training Facility

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.

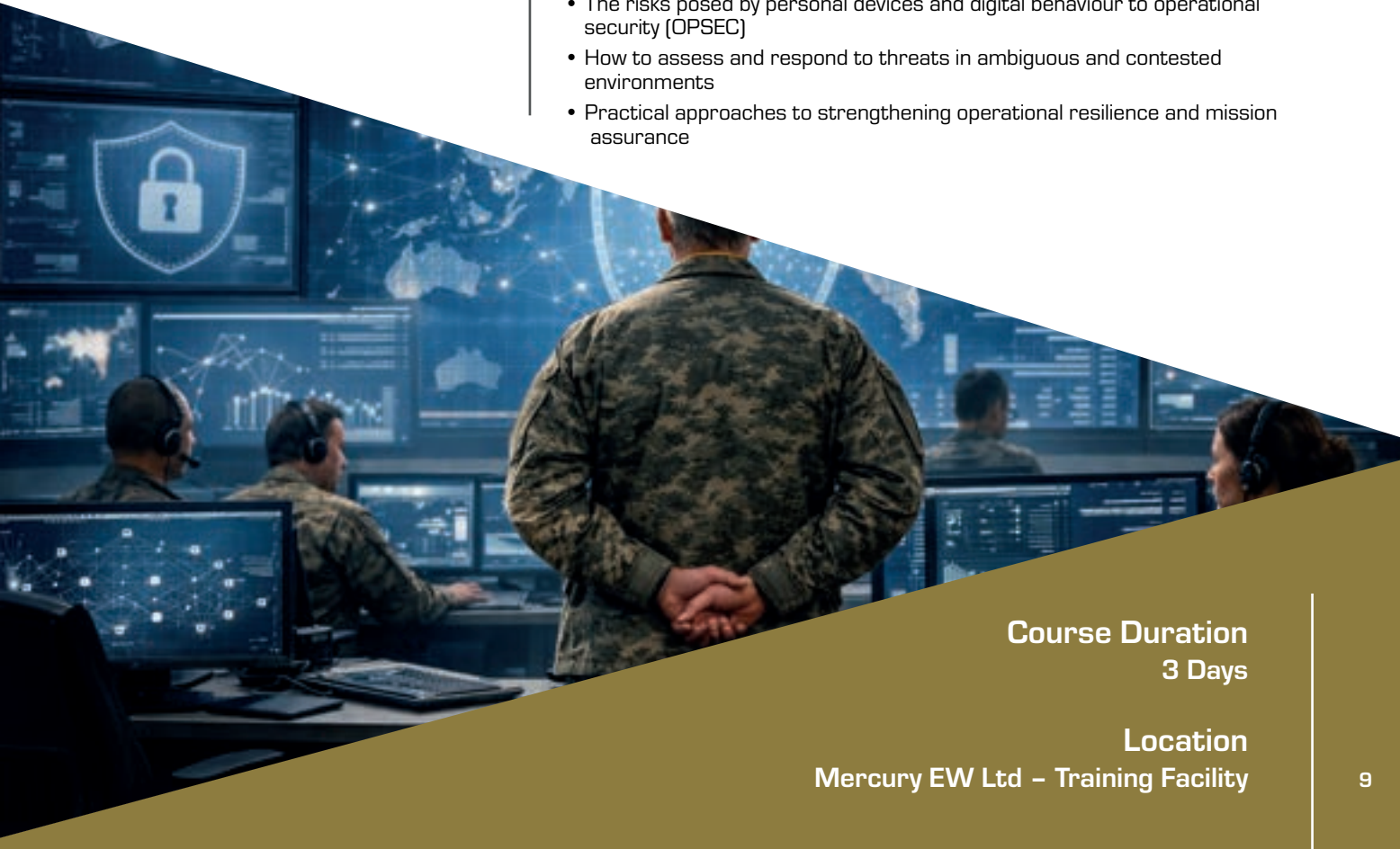
This programme develops operational cyber and information warfare awareness, enabling personnel to understand how hybrid conflict, deception, artificial intelligence, and influence operations shape the modern battlespace.

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

Executive Cyber Threat and Risk Leadership Course

Introduction

Cyber threats are no longer isolated technical events, they operate across crime, espionage, and state-level conflict, exploiting technology, human behaviour, and global interconnectivity.

This programme develops strategic cyber literacy, enabling leaders to understand how ransomware, deception, artificial intelligence, cyber law, and emerging conflict dynamics shape the modern threat environment.

Delivered through real-world case studies, structured debate, and scenario-based exercises, the course challenges participants to think critically, operate in ambiguity, and make informed decisions under pressure.

The focus is not on technical detail, but on understanding the bigger picture, improving organisational resilience, and enabling leadership to respond effectively to evolving cyber threats.

What you will learn:

- The structure and impact of modern cyber threats (criminal, state, and hybrid)
- How ransomware and cyber crime operate as strategic business models
- The role of deception, influence, and trust exploitation in cyber attacks
- Legal, ethical, and attribution challenges in cyberspace
- The impact of artificial intelligence and synthetic media on trust and security
- How cyber warfare and hybrid conflict affect organisations beyond the military domain
- The concept of "shadow security" and hidden organisational risk
- How to make effective decisions in uncertain and rapidly evolving situations
- Practical approaches to improving organisational resilience and governance

Who should attend?

This course is designed for senior leaders, decision-makers, and professionals responsible for organisational risk, strategy, and governance in an increasingly complex cyber landscape.

It is particularly relevant for:

- **Executives and senior managers**
- **Risk, compliance, and governance leads**
- **Cybersecurity and IT leaders**
- **Intelligence and analysis professionals**
- **Policy and strategy advisors**

No deep technical expertise is required. The course focuses on strategic understanding, decision-making, and risk judgement.

Key Organisations

Government Departments and Agencies

Critical National Infrastructure (CNI)

Financial Services, Healthcare, and Legal Sectors

Defence Industry and Commercial Enterprises

Any organisation operating in high-risk or regulated environments

Course Duration
3 Days

Location
Mercury EW Ltd – Training Facility

Networking to Security Operations Centre [SOC] Operations Course

Introduction

Cybersecurity capability depends on more than awareness alone. Organisations need personnel who understand how networks operate, how security controls fit together, how threats are detected, and how incidents are escalated within a Security Operations Centre (SOC) environment.

The 10-Day Networking to SOC Pathway provides a structured development route for individuals entering the cybersecurity field or strengthening their technical foundations. Delivered by Mercury EW in collaboration with SudoCyber, the course uses SudoCyber's technical course material to provide a practical and progressive learning experience aligned to recognised cybersecurity pathways.

The programme bridges the gap between networking fundamentals, security operations, incident response thinking, and the realities of working in or alongside a SOC. It is designed to support learners as they develop the confidence, vocabulary, and technical understanding required to contribute more effectively within cyber security environments.

A key feature of this course is its progression towards CompTIA accreditation, giving learners a recognised development pathway while ensuring the training remains practical, relevant, and grounded in real-world cyber operations.

Throughout the course, learners will explore how networks function, how threats move through systems, how logs and alerts support detection, and how analysts investigate, escalate, and communicate cyber incidents. The course is particularly valuable for organisations seeking to grow internal cyber capability, reduce reliance on external recruitment, and create a clearer pathway into SOC and cybersecurity roles.

What you will learn:

- Core networking principles, including OSI model, TCP/IP, ports, protocols, DNS, DHCP, routing, and segmentation
- How common network services and infrastructure support business operations
- Security fundamentals, including authentication, access control, endpoint protection, email security, and secure configuration
- How cyber threats exploit networks, users, systems, and misconfigured environments
- The purpose and function of a SOC
- How alerts, logs, and indicators of compromise are used to support investigation
- Introduction to incident response, escalation, containment, and recovery thinking
- How frameworks such as the cyber kill chain and MITRE ATT&CK support analyst understanding
- The role of communication, prioritisation, and decision-making within SOC operations
- How technical knowledge supports progression towards recognised CompTIA accreditation
- Practical approaches to building confidence for entry-level cyber and SOC roles

Who should attend?

This course is designed for individuals moving into cybersecurity, technical support, SOC operations, or cyber-adjacent roles who require a structured foundation in networking, security concepts, and operational cyber awareness. It is particularly relevant for:

- **Junior cyber security analysts**
- **IT support and service desk personnel**
- **Network technicians and administrators**
- **Personnel transitioning into cyber roles**
- **Graduates, apprentices, and early-career cyber professionals**
- **Organisations developing internal cyber talent pipelines**

The course is suitable for learners with limited cybersecurity experience, although a basic familiarity with IT systems would be beneficial. The programme is designed to build confidence progressively, moving from core networking principles through to practical SOC awareness and incident response thinking.

Key Organisations

Ministry of Defence

Government Departments and Agencies

Defence and Security Organisations

Critical National Infrastructure (CNI) Providers

Managed Service Providers and SOC Teams

Commercial Organisations developing internal cyber capability

Any organisation seeking to build technical cyber skills and support progression towards recognised accreditation

Course Duration
2 Weeks

Location
Mercury EW Ltd – Training Facility

Protecting What Matters: Human-Centric Cybersecurity Course

Introduction

Cybersecurity is no longer solely a technical problem, it is a human one. The majority of successful cyber attacks exploit human behaviour rather than technical vulnerabilities, targeting how individuals think, feel, and make decisions.

This course provides a powerful and engaging insight into the psychological and behavioural drivers behind cyber risk. It explores how individuals are influenced by social engineering, online environments, and cognitive biases, both inside and outside the workplace.

Delivered through a combination of real-world examples, interactive discussion, and scenario-based learning, this course moves beyond traditional "tick-box" training and explicitly links personal digital behaviour with organisation risk, reflecting modern working practices such as remote and hybrid working. It equips participants with the awareness and practical understanding required to recognise manipulation, challenge assumptions, and make more secure decisions in both their professional and personal lives.

What you will learn:

- How cyber attacks exploit human behaviour rather than technology
- Networking fundamentals for everyone
- The psychology behind phishing, social engineering, and manipulation techniques
- The role of cognitive biases (e.g. optimism bias, normalcy bias, authority bias) in decision-making
- How social media, online activity, and "echo chambers" influence perception and behaviour
- Real-world examples of insider threat development and behavioural exploitation
- How to recognise suspicious activity and respond appropriately
- The link between personal digital habits and organisational risk
- Practical steps individuals can take to protect themselves and their organisation
- How small behavioural changes can significantly reduce cyber risk

Who should attend?

This course is designed for personnel at all levels within an organisation, from frontline staff to senior leadership. It is particularly relevant for individuals who interact with digital systems, handle sensitive information, or are responsible for maintaining organisational security in day-to-day operations.

No prior technical cyber security knowledge is required, making it suitable for both technical and non-technical audiences.

Key Organisations

Ministry of Defence

Government Departments and Agencies

Critical National Infrastructure (CNI) Organisations

Financial Services, Healthcare and Legal Sectors

Defence Industry and Commercial Organisations

Any organisation seeking to reduce human cyber risk and strengthen security culture

Course Duration
1 Day

Location
Mercury EW Ltd – Training Facility or Customer Site

Driving Behavioural Change in Cybersecurity Course

Who should attend?

No prior technical cyber knowledge is required for this course, which focuses on leadership, decision-making, and behavioural risk management. This is designed for senior leaders, managers, and decision-makers responsible for people, process, and risk within an organisation; it is particularly relevant for:

- **Department heads and team leaders**
- **Programme and project managers**
- **Risk, compliance, and governance professionals**
- **Security leaders and non-technical executives**

Key Organisations

Ministry of Defence

Government Departments and Agencies

Defence and Security Organisations

Critical National Infrastructure (CNI) Providers

Large Commercial Enterprises and SMEs

Any organisation seeking to improve cyber resilience through leadership and culture

Introduction

Organisations invest heavily in cybersecurity technology and breaches still occur. Why? Because security failures are rarely caused by a lack of tools, but by a lack of alignment between people, process, and behaviour.

This course is designed to equip management with the knowledge and practical tools required to drive meaningful behavioural change in cybersecurity. It challenges traditional approaches that rely solely on policy enforcement and technical controls, and instead focuses on how leadership decisions shape organisational behaviour both positively and negatively.

Through a combination of real-world case studies, behavioural models, and scenario-based exercises, participants will learn how to identify hidden risks, reduce friction, and create an environment where secure behaviour becomes the default, not the exception.

A key feature of this course is its practical application. Throughout the day, participants will work collaboratively to develop a tailored cyber security action plan, aligned to their organisational context. By the end of the course, attendees will leave with a structured model and clear, actionable steps that can be immediately implemented to initiate meaningful change within their organisation.

What you will learn:

- Why traditional cybersecurity approaches (People, Process, Technology) often fail in practice
- How behavioural biases influence decision-making and create hidden vulnerabilities
- The impact of organisational culture on cyber security outcomes
- How to identify and reduce “shadow security practices” within teams
- How to interpret technical risk (e.g. CVSS reporting) in a business context
- The role of management in bridging the gap between security teams and operations
- How to design and implement effective behavioural change strategies
- Practical frameworks for improving adoption of security controls (e.g. ADKAR, behavioural models)
- How to communicate cyber risk in a way that drives action and accountability
- Techniques for building a security-conscious culture without creating friction or resistance

Course Duration
1 Day

Location
Mercury EW Ltd – Training Facility or Customer Site

Counter-Uncrewed Aerial Systems [C-UAS] Course

Introduction

This course is designed for delegates seeking a robust technical and analytical understanding of uncrewed aerial threats and the systems used to counter them. The course establishes a strong foundation in UAS architectures, operational concepts and threat methodologies, before progressing through communications, RF fundamentals, waveforms, observables and exploitation techniques relevant to modern C-UAS environments. From this base, the training expands into detection, classification and response methodologies, highlighting the strengths, limitations and trade-offs of different C-UAS approaches.

The learning journey culminates in realistic, scenario driven analysis, where delegates apply structured threat assessment, sensor selection and response decision making within operational constraints. Practical activities are embedded to reinforce theory and develop analytical confidence. On completion, participants will have developed both a deep technical understanding of C-UAS concepts and the analytical skills required to support operations, system design, capability development and informed decision making in complex environments.

What you will learn:

- UAS Terminology, components and system architectures
- How UAS function as integrated operational systems.
- Emerging UAS threats and employment methodologies
- UAS communications and control link concepts
- RF fundamentals relevant to C-UAS environments
- Waveforms and signal characteristics associated with UAS
- Observable signatures across RF, radar, EO/IR and acoustic domains
- Detection, tracking and layered C-UAS architectures
- CEMA and EW concepts applied to C-UAS
- Kinetic and non-kinetic C-UAS response methodologies
- Limitations, trade-offs and constraints in C-UAS solutions
- Application of C-UAS principles to realistic operational scenarios
- How emerging UAS employment concepts are driving changes in C-UAS design
- Identification of likely failure modes and fallback behaviours in UAS
- How threat dependencies and system design affect C-UAS effectiveness

Who should attend?

Military CEMA Operators.

Civilian EW Practitioners.

Systems and Capability Engineers.

Programme and Project Managers.

Technical staff supporting UAS and C-UAS activities.

Key Organisations

Ministry of Defence

Defence Science and Technology Agencies

All Government agencies, industries and organisations interested in development and employment of C-UAS capabilities

Course Duration
1 Week

Location
Mercury EW Ltd – Training Facility

Advanced Electromagnetic Warfare (EW) Managers' Course

Who should attend?

Military and Civilian Radar and EW practitioners from both Operational and Engineering backgrounds. Programme & Project Managers, Systems Engineers and Technical Staff.

Key Organisations

Ministry of Defence

HQ Joint, Army, Navy and Air Force EW operators/Analysts

All Government agencies, industries and organisations interested in operational and technical aspects of EW

Introduction

This course is designed to inform and introduce delegates to the key principles of EW Management. The course will be delivered with a blend of theory and practical syndicate-based scenarios. Using the theory-based knowledge and practical lesson delegates will increase their understanding of the EW Management principles within a joint environment and an all source approach to EW in modern warfare.

What you will learn:

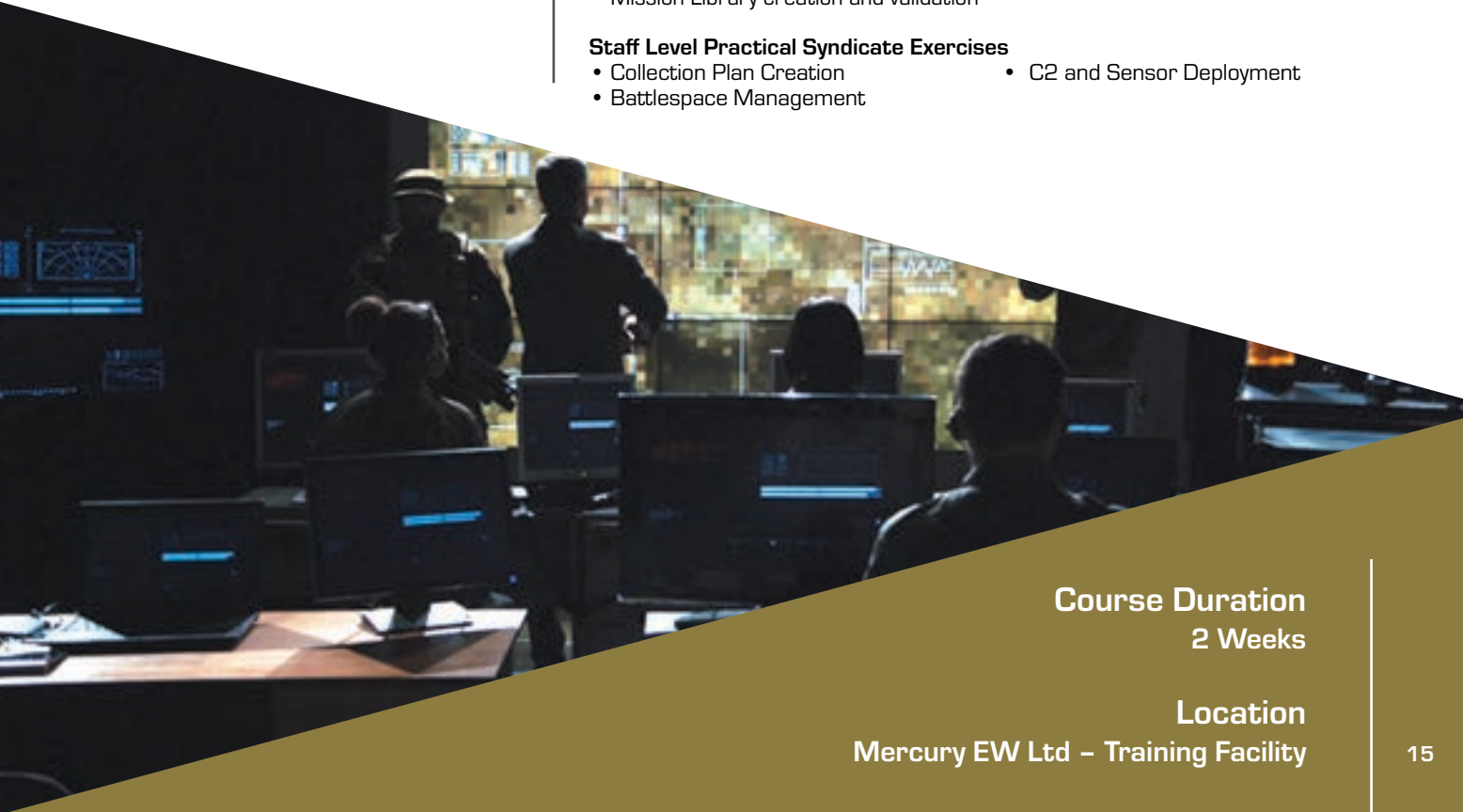
EW Collection Management
- CCIRM Process
- Command and Control
- ISTAR Capabilities
- Intelligence Cycle

EW in Joint Operations
- EW in Land, Sea & Air Domains
- ES, EA and EP
- EW Threats (inc The Drone Threat)
- EW Command Control
- EW Mutual Support
- EW Operational Support
- Overview of and ISTAR Organisation

EW Analysis
- Information & Intelligence Analysis
- Definition of information and Intelligence
- Objective Analysis
- Reasoning, interpretation and decision making
- Intelligence as a Force Multiplier
- Intelligence Exploitation & Analysis Techniques
  - Pattern Analysis
  - Statistical Analysis
  - Data Mining Techniques
- Introduction to OSINT Analysis

Data Management and Data Fusion
- Principles of Database Management
  - Basic Relational Database Structure
  - Validation
  - Security
- EOB Filtering
- Mission Library creation and validation
- Post Mission Analysis
- Intelligence Sources
- Correlation and Fusion Techniques
- All source Analysis
- Confidence/Reliability grading

Staff Level Practical Syndicate Exercises
- Collection Plan Creation
- Battlespace Management
- C2 and Sensor Deployment



Course Duration
2 Weeks

Location
Mercury EW Ltd – Training Facility

Land Electromagnetic Warfare [EW] Course

Introduction

This course addresses the key management functions regarding the planning, preparation, deployment and sustainment of Land EW capability in a deployed operational context. This includes the processes and procedures required to effectively manage EW capability. It will focus on the employment of EW assets and how best to utilise these assets in a variety of operational environments.

There will be a detailed focus on Counter Radio Controlled Improvised Explosive Devices (RCIEDs) covering threats, equipment, technology cycle and interoperability. It will also address key subjects that EW has significant influences upon; Intelligence Surveillance Target Acquisition and Reconnaisance
(ISTAR), Information Operations and Battlespace Spectrum Management as well as the roles and responsibilities of military personnel involved in EW Equipment Procurement, specifically; Procurement Cycle, Capability Integration, Statements of Requirement, Requirements Capture and the various associated key document outputs. The course will also facilitate a number of practical based exercises designed around realistic deployed scenarios in order to consolidate student learning.

What you will learn:

- The Electromagnetic Threat
- Electromagnetic Surveillance (ES) principles and techniques - Search, Intercept, Direction Finding and Analysis of signals at radio and RADAR frequencies
- Electromagnetic Attack (EA) principles and techniques - Jamming, Deception and Neutralisation.
- Electromagnetic Defence (ED) principles and techniques - Active and passive measures
- The capabilities and limitations of Land EW equipment
- The deployment principles and cycle relating to EW capability and operations
- Counter Radio Controlled Improvised Explosive Device principles
- EW in Information Operations
- ISTAR principles
- Duties of the User Representative in the procurement of EW capability

Who should attend?

Anyone involved in formulating strategy, policy, doctrine, processes or procedures for Land EW capability in a deployed, operational context. Anyone involved in the practical application, delivery and conduct of Land EW in a deployed, operational context.

Key Organisations

Ministry of Defence

HQ Army

Defence Science and Technology Agencies

Defence Research Lab/Institutes

All Government agencies, industries and organisations intersted in the development of Land EW capability

Course Duration
2 Weeks

Location
Mercury EW Ltd – Training Facility

Communications Intelligence / Electromagnetic Warfare Intercept Operator Course

Who should attend?

Military and civilian COMINT/ EW practitioners from Strategic, Operational and Tactical backgrounds. Anyone involved in the practical application, delivery and conduct of EW in a deployed, operational context.

Key Organisations

Ministry of Defence

HQ Joint, Army, Navy and Air Force

All Government agencies, industries and organisations interested in the development of EW capability

Introduction

This course addresses the underpinning knowledge and generic practical skills required of a COMINT/EW Intercept Operator. Delegates will be provided with a thorough appreciation of the principles, practices and application of COMINT/ EW in modern warfare. Specifically, the practical elements of the course include: receiver search and intercept skills, activity logging, locating (through Direction Finding), analysis and exploitation of information, and reporting methods. Practical training realism is enhanced through the use of a market leading COMINT Simulator (EXERCISE RF), which is capable of generating relevant tactical scenarios through simulating threat emitters at any distance and direction of arrival from training EW Mission Systems. The training EW Mission Systems comprise sophisticated wideband software defined intercept and DF systems that enable Intercept Operators to consolidate their skills. Increasingly complex scenarios are used to ensure training is both intuitive and progressive. The course will also focus on the employment of COMINT/EW assets and how best to utilise these assets in a variety of operational environments.

What you will learn:

- Introduction to EW Terminology
- The Electromagnetic Threat
- Electromagnetic Surveillance (ES) principles and techniques - Search, Intercept, Direction Finding and Analysis of radio frequency signals of interest
- Electromagnetic Attack (EA) principles and techniques - Jamming, Deception and Neutralisation
- Electromagnetic Protect (EP) principles and techniques - Active and passive measures
- The capabilities and limitations of Land EW equipment
- The deployment principles and cycle relating to EW capability and operations
- Receiver search and intercept techniques
- Logging methods and processes, and recording of activity
- Analysis techniques and exploitation
- Activity Reporting

Course Duration
2 Weeks

Location
Mercury EW Ltd – Training Facility

Communication Intelligence [COMINT] Technical Analysis Course

Introduction

This course addresses key elements of COMINT Technical Analysis and will provide delegates with a sound operational understanding and appreciation of the complexities of technical signals analysis and its value within modern warfare. The course will be delivered with a blend of theory and progressive practical lessons to consolidate knowledge, skills and experience in the configuration and application of the PROCITEC Go2 monitoring and analysis tools against pre-recorded or live Signals of Interest (SOIs).

What you will learn:

- Basic Communications Theory Consolidation
- The Fundamentals of Radio Data Transmissions
  - Telegraph Speed, Bit Rate, Baud Rate Symbol Rates
  - Formatting and Source Coding
  - Encryption
  - Modulation
    - ASK (Amplitude Shift Keying)
    - FSK (Frequency Shift Keying)
    - PSK (Phase Shift Keying)
    - OFDM (Orthogonal Frequency Division Modulation)
  - Bandwidth-efficient Modulation
  - Indirect Frequency Modulation (FM) & Amplitude Modulation (AM)
- Introduction to Common Transmission Modes and their composition
- Classifier and Automatic Code Check usage
- Introduction to PROCITEC go2Signals Monitoring and Analysis Tools
  - Fast Fourier Transform (FFT) and Sonogram analysis mode
  - Waterfall
  - Oscilloscope
  - Frequency Shift Keying (FSK) Analysis
  - FSK Code Check
  - Phase Shift Keying (PSK) Symbol Rate, Phase Plane and Code Check
  - Multiple Frequency Shift Keying (MFSK) Analysis and Code Check
  - Auto Correlation & Identification
  - Bit Correlation and Bit Length Analysis
- Practical Signals Collection Principles in a Live and simulated environment
- Digital Mobile Radio (DMR) & Terrestrial Trunked Radio (TETRA) Interception
- Remote Keyless Entry (RKE) Theory & Practical manipulation
- Wideband Monitoring and Analysis (Export Control Licence Dependant)
  - TETRA & MPT 1327 practical band search and Interception
  - Frequency Hopper Theory with practical collection and Interception techniques
- HF Military Signals Applications (Export Control Licence Dependant)

Who should attend?

Military and government civilian Electromagnetic Warfare (EW) practitioners engaged in the technical analysis of COMINT data. Ideally suited for experienced COMINT technical data analysts.

Key Organisations

Ministry of Defence

HQ Joint, Army, Navy and Air Force COMINT operators/Analysts

All Government agencies, industries and organisations interested in operational and technical aspects COMINT

Course Duration
2 Weeks

Location
Mercury EW Ltd – Training Facility

Communications Jamming Course

Who should attend?

Military and government civilian EW practitioners engaged in communication jamming activities.

Key Organisations

Ministry of Defence

HQ Joint, Army, Navy, and Air Force EW operators Analysts.

All Government agencies, industries and organisations interested in operational and technical aspects of EW

Introduction

This course addresses key elements of communications jamming and will provide delegates with a sound understanding and appreciation of the complexities of communications jamming in a range of operational scenarios and against various signal types. The course will be delivered with a blend of theory and progressive practical lessons to consolidate knowledge and skills.

What you will learn:

- Introduction to Electromagnetic Attack within EW
- Mathematics related to communications jamming
  - Exponents, metric prefixes, logarithms and decibels
- Space/direct wave propagation including:
  - Propagation losses using the line-of-sight and two-ray propagation loss models
  - Fresnel zones
- Communications and Electromagnetic Attack antennas
  - Principles and terminology associated with electromagnetic radiation
  - Principles of various communications and jamming antennas: half-wave dipole, monopole, Logarithmic Periodic Array, discone and parabolic reflector
- Principles of communications jamming
  - Jamming networks
  - Jamming analogue and digital signals
  - Jamming-to-Signal (J/S) ratio including operational calculations
  - Burn-through range including calculations
- Types of jamming and systems
  - Including: spot, barrage, swept, partial band, responsive and follower jamming
  - Different jamming techniques including: self-protection, stand-off and stand-in jamming
  - Different types of jamming systems
- Ground-based and airborne communication jamming
  - Man-portable, vehicle-based, mast elevated, expendable and airborne
- Jamming of Low Probability of Intercept (LPI) threat signals
  - Basics of Frequency Hopping Spread Spectrum and Direct Sequence Spread Spectrum
  - Jamming methods used against LPI signals
- Satellite communications jamming and GSM jamming
  - Introduction to SATCOM and GSM communications
  - Methods of SATCOM jamming and GSM jamming
  - Spoofing and GPS jamming
- Jamming planning process – tasks involved during each stage of the jamming planning process
- Electromagnetic Protect and anti-jamming
  - Active methods of EP (technical and tactical)
  - Passive methods of EP (technical, tactical and training)
- Radar jamming
  - Jamming and deception techniques
- Counter-Radio Controlled Improvised Explosive Device (C-RCIED) Jamming
  - The RCIED threat, principles of ECM, jamming techniques, interoperability, development cycle
- Various syndicate based practical exercises to consolidate knowledge

Course Duration
2 Weeks

Location
Mercury EW Ltd – Training Facility

Electromagnetic Warfare [EW] Analysis Course

Introduction

This course addresses key elements of EW Analysis and will provide delegates with a sound operational understanding and appreciation of EW Analysis, Data Fusion and the need for sound EW Threat Library Management.

What you will learn:

Information Analysis

- All source information analysis
- Pattern analysis
- Open Source Intelligence (OSINT)
- Statistical analysis
- Semantic intelligence
- Data mining techniques

Data Fusion COMINT/ELINT

- Overview of the intelligence process
- Intelligence sources
- Correlation and fusion techniques
- Intelligence cycle
- All source analysis
- Confidence /reliability grading

Library Threat Management COMINT/ELINT

- How to create a database abstract
- Mission Library fundamentals
- Creating and Filtering Electromagnetic Order of Battle (EOBs)
- Library Distribution

Who should attend?

Military and Civilian Radar and EW practitioners from both Operational and Engineering backgrounds. Programme & Project Managers, Systems Engineers and Technical Staff.

Key Organisations

Ministry of Defence

HQ Joint, Army, Navy and Air Force Electromagnetic Intelligence (ELINT) operators/Analysts

Defence Science and Technology Agencies

Defence Research Lab/Institutes

All Government agencies, industries and organisations interested in the technical aspects of ELINT analysis

Course Duration

2 Weeks

Location

Mercury EW Ltd – Training Facility

Maritime Electromagnetic Warfare [EW] and Intelligence Course

Who should attend?

Military and government civilian EW practitioners engaged in Maritime EW and Intelligence.

Key Organisations

Ministry of Defence

HQ Joint, Army, Navy and Air Force EW operators/Analysts

All Government agencies, industries and organisations interested in operational and technical aspects of Maritime EW

Introduction

This course addresses key elements of Maritime Electromagnetic Warfare (EW) and Intelligence in today's modern maritime environment. The course is designed to provide the foundations of Maritime EW and Intelligence using a mixture of theory and practical based training addressing key areas covering a variety of subjects related to Maritime EW and Intelligence.

What you will learn:

Maritime EW

- EW Theory Overview
- Radar Foundation
- Radar and EW Weapons, Threats and Platforms
- EW Planning and Preparation
- Employment of Maritime EW systems
- Optimisation of ESM Systems
- Weapon Systems and Countermeasures

Maritime Intelligence

- Introduction to Intelligence
- Fundamentals of Intelligence
- Intelligence Sources and Agencies
- Sources of Intelligence and Agencies
- The Intelligence Estimate
- Intelligence Reporting and Products
- Maritime Staff Intelligence Scenario
- Ships Intelligence Collection Management (SICM)

Course Duration
2 Weeks

Location
Mercury EW Ltd – Training Facility

Electromagnetic Warfare [EW] for Programmers & Product Owners Course

Introduction

This course addresses a range of operational functions regarding the planning, preparation, deployment and sustainment of Electromagnetic Warfare (EW) capability in a deployed operational context. It will cover all doctrinal aspects of EW but from a tactical EW operator and manager's perspective. This includes the processes and procedures required to effectively manage EW capability as well as the functional requirements of various EW equipment. It will focus on the employment of EW assets and how EW managers would best utilise these assets in a variety of operational environments. There will also be a detailed focus on Counter Radio Controlled Improvised Explosive Devices (RCIEDs) covering threats, equipment, technology cycle and interoperability. The course will also facilitate a number of practical based exercises designed around realistic deployed scenarios in order to consolidate student learning.

What you will learn:

- Electromagnetic Surveillance (ES) principles and techniques - Search, Intercept, Direction Finding and Analysis of signals at radio and RADAR frequencies
- Electromagnetic Attack (EA) principles and techniques – Jamming, Deception and Neutralisation
- Electromagnetic Protect (EP) principles and techniques - Active and passive measures
- The capabilities and limitations of Land EW equipment
- The deployment principles and cycle relating to EW capability and operations
- An introduction to Maritime EW
- An introduction to Air EW
- Counter Radio Controlled Improvised Explosive Device principles.

Who should attend?

Engineers or project managers working for Defence sector EW organisations who require a detailed understanding of EW from a military and operational perspective.

Key Organisations

Ministry of Defence

HQ Army

Defence Science and Technology Agencies

Defence Research Lab/Institutes

All Government agencies, industries and organisations interested in development of EW capability

Course Duration
1 Week

Location
Mercury EW Ltd – Training Facility

Counter Radio Controlled Improvised Explosive Device [C-RCIED] Workshop

Who should attend?

Anyone involved in formulating strategy, policy, doctrine, processes or procedures for Counter RCIED capability in a deployed, operational context. Anyone involved in the practical application, delivery and conduct of Counter RCIED in a deployed, operational context.

Key Organisations

Ministry of Defence

HQ Army

Defence Science and Technology Agencies

Defence Research Lab/Institutes

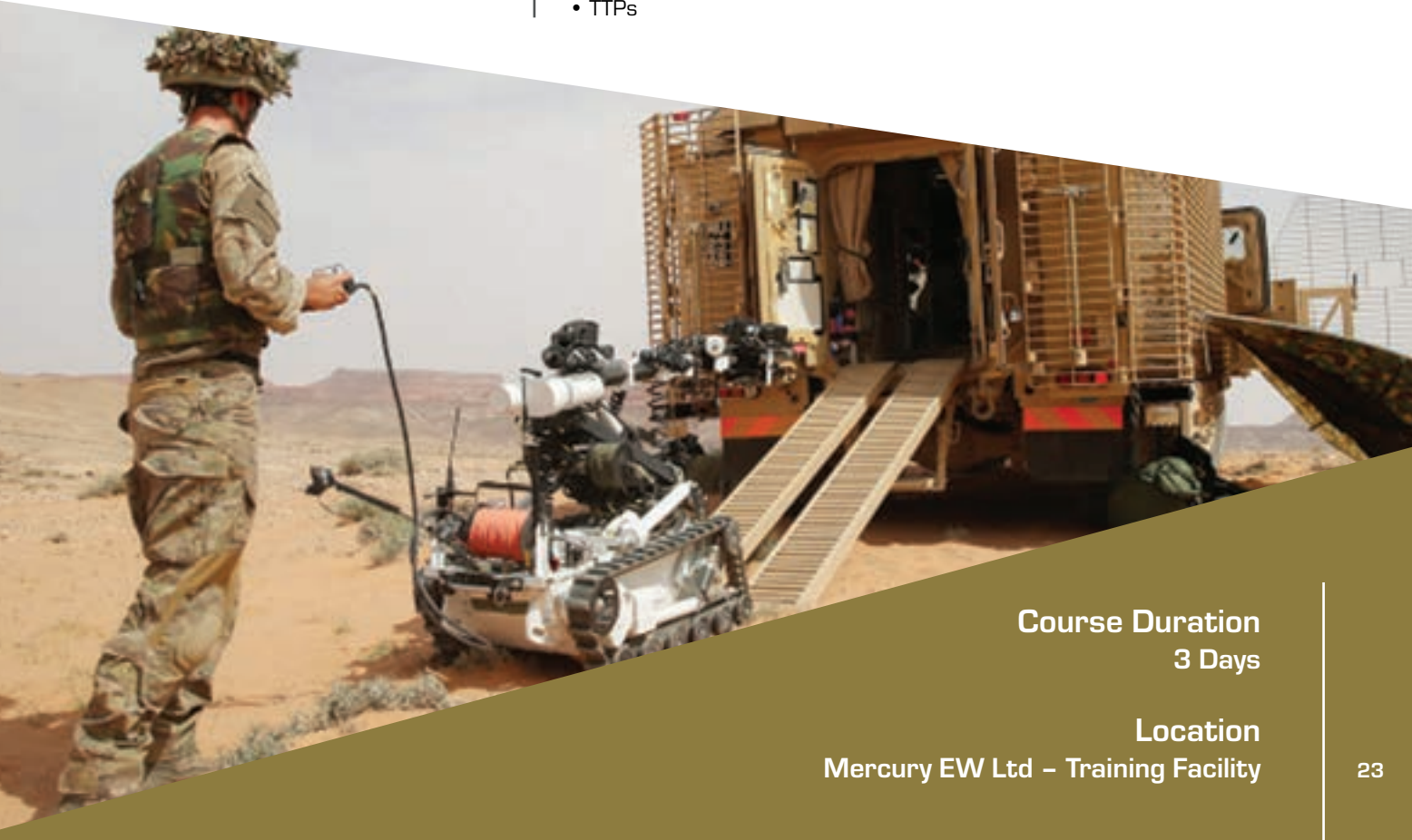
All Government agencies, industries and organisations interested in development of Counter RCIED capability

Introduction

This workshop addresses key areas regarding the planning, preparation, deployment and sustainment of Electromagnetic Counter Measures (ECM) used specifically to inhibit Radio Controlled Improvised Explosive Devices (RCIEDs) in a deployed operational context. This includes the processes and procedures required to effectively manage ECM capability. It will cover the RCIED threat; an historical insight into how devices have developed in different environments. Different types of IEDs will be discussed, focusing on the requirements of an RCIED. The workshop will focus in detail on the requirements of ECM equipment and the various methods of jamming that can be used to inhibit RCIEDs. It will also concentrate on the Technology Cycle; exploiting emerging threats and developing new waveforms or new equipment as a timely response to the threat. Interoperability between national and other nations ECM equipment will be addressed as well as ECM interoperability with communications. There will also include a session analysing Tactics, Techniques and Procedures relating to ECM usage by both dismounted patrols and vehicle convoys. The workshop will also facilitate practical based exercises designed around realistic deployed scenarios in order to consolidate student learning.

What you will learn:

- The RCIED threat
- Principles of RCIEDs
- Principles of ECM
- ECM equipment requirements
- Jamming techniques
- Technology Cycle – Exploitation, waveform/equipment development, TTP analysis
- Interoperability
- TTPs



Course Duration
3 Days

Location
Mercury EW Ltd – Training Facility

Advanced Anti-Submarine Warfare & Underwater Analysis Course

Introduction

This course addresses key elements of underwater analysis by introducing Acoustic Intelligence (ACINT) in the context of Anti-Submarine Warfare (ASW). The Underwater Analysis phase of the course will include a mixture of theory and practical based training addressing key areas covering a variety of subjects related to ACINT.

What you will learn:

- Understanding the Submarine Threat
  - Tasks
  - Capabilities
  - Effects
- Oceanography 1 – Understand the Submarine environment
- Oceanography 2 – How the Submarine exploits the environment
- Nuclear Submarines
- Diesel Submarines
- Visual recognition features of submarines to identify nationality, type and class
- Periscope/mast recognition
- Submarine design features and how to exploit them
- Understanding noise sources, their implications and how to exploit them
- Tracking theory and practical exercises
- Special Forces Submarines, Midget Submarines and Merchant Vessels
- Acoustic Theory for ASW
- Acoustic Sensors
- Fixed Wing Maritime Patrol Aircraft in ASW
- Rotary Wing and Ships in ASW
- Practical ASW Exercise – Diesel Target
- Practical ASW Exercise – Nuclear Target
- Maritime Patrol Aircraft SME Guest Speaker
- Visit to RN Submarine Museum Portsmouth (COVID-19 permitting)
- Discussion with ex-RN Submarine Commander

Who should attend?

Military and government civilian practitioners engaged in ASW operations and/or those engaged in the underwater analysis.

Key Organisations

Ministry of Defence

HQ Joint, Army, Navy and Air Force ASW operators/Analysts

All Government agencies, industries and organisations interested in operational and technical aspects of ASW

Course Duration
3 Weeks

Location
Mercury EW Ltd – Training Facility

Open Source Intelligence [OSINT] Course

Who should attend?

Military and Civilian from an Intelligence, Research or Investigation background who already have a fundamental understanding of All Source Intelligence Analysis.

Key Organisations

Ministry of Defence

HQ Joint, Army, Navy and Air Force EW operators/Analysts

All Government agencies, industries and organisations interested in operational and technical aspects of open source intelligence

Introduction

This course is designed to inform and introduce delegates to the key principles of OSINT. The course will provide a strong foundational knowledge and understanding. The course will enable delegates to effectively and safely exploit the vast Open Source Information landscape and understand how this can be fused with other Intelligence gathering platforms to inform decision making of key stakeholders. The course will be delivered in a practical and exercise focussed manner, allowing students to gain hands-on experience, following short theory-based sessions.

What you will learn:

Introduction to OSINT

- History of Open Source Information
- Overview of the Internet
  - History
  - Architecture
  - Size
  - Regulation
- Collection Planning and Management
- Limitations and Considerations
  - 4 V's of Data
- OSINT Within the Intelligence Cycle
- Online Security Awareness
  - Digital Footprint
  - Organisational and Personal security
- Legal and Ethical Constraints

Online Resources, Effective Searching and Information Exploitation

- Framing the Question - Effective Direction
- Web Browsers
- Investigation Tools
- Understanding Search Engines
  - Basic Search Principles
  - Search Results and Variations
  - Different Types of Search Engines
- Advanced Search Techniques
  - Search Planning
  - Search Operators
- Deep Web Exploitation
- Monitoring and Alert Services
- Global News Resources
- Databases, Archives and Public Records
- Metadata
- Mapping
- Personal Identifiers
  - Email Addresses
  - Usernames
  - Telephone Numbers
- Language Translation
- Object and Device Identifiers
- Dark Web overview
  - History
  - Tor Privacy and Security
  - Other Dark Webs
- IP Address and Domain Exploitation
- Image and Video Exploitation

Social Media Intelligence (SOCMINT)

- Global Trends
- Limitations and Other Considerations
- Investigation Methods for Social Media
- Alternative Social Media Platforms
- Facebook, Twitter and LinkedIn
- Image-based platforms (Instagram, Flickr etc.)
- Social Media Analysis Tools and Platforms
- Creating and Maintaining False Personas

OSINT Analysis Fundamentals

- Combining OSINT with other Intelligence Collection Capabilities
- Source Validation and Credibility
  - Types of Sources
  - Motivations and Bias
- Reliability of Information
- Critical Thinking
- Effective information Processing and Analysis
- Adding Value - Applying the 'So What?'
- Creating Professional OSINT Products
- Dissemination Principles
- Managing Intelligence Gaps

Course Duration
2 Weeks

Location
Mercury EW Ltd – Training Facility

Basic Imagery Intelligence [IMINT] Analysis Course

Introduction

This course is to provide foundation training for the analysis of imagery in areas related to defence and security. The course is designed to attendees with limited background in imagery analysis and provides imagery exploitation using recognised tools, interpretation techniques and analysis of critical infrastructures and military forces. All theoretical training is complimented with practical exercises.

What you will learn:

- Role IMINT has in defence and security domains
- Knowledge in remote-sensing including platforms, sensors and imagery
- How to assess and report the composition and capacity of strategic infrastructures
- How to analyse and report significant features and activity of strategic infrastructures
- Knowledge in the structures of Air, Ground, Naval Forces
- How to assess and report the composition and capability of military forces
- How to analyse and report significant features and activities at military installations
- How to analyse and report on the status and activity of deployed military deployed forces
- Create IMINT products to support decision makers

Who should attend?

Military and Civilian Imagery Intelligence practitioners from both Operational and Engineering backgrounds. Programme & Project Managers, Systems Engineers and Technical Staff.

Key Organisations

Ministry of Defence

HQ Joint, Army, Navy and Air Force EW operators/Analysts

All Government agencies, industries and organisations interested in operational and technical aspects of imagery intelligence

Course Duration
2 Weeks

Location
Mercury EW Ltd – Training Facility

Space Intelligence, Surveillance & Reconnaissance [ISR] - Fundamentals Course

Who should attend?

Military and civilian EW and ISR practitioners and managers from operational, planning and engineering backgrounds. Capability programme & project managers, systems engineers and technical staff. Personnel involved in formulating strategy, policy, doctrine, processes or procedures for ISR and EW operations in space.

Key Organisations

Ministry of Defence

HQ Space, Joint, Army, Navy and Air Force EW operators/analysts/

All Government agencies, industries and organisations interested in operational and technical aspects of EW in space

All Government agencies, industries and organisations interested in development of EW capability in spaceand technical aspects COMINT

Introduction

The Space Fundamentals course is designed to inform and introduce students to the key fundamentals of operations (primarily military ISR) in space. This includes international definitions, recognised satellite orbits with benefits and disadvantages with regards to ISR, space operations doctrine and policy and technological considerations.

This is an instructor led tutorial experience using a combination of lecture, explanations and demonstrations of theory, and examples relevant to military ISR operations in space. The course will Include analysis and explanation of current space ISR capability and Its utility in support of military operations, In war and peace time. The fundamentals delivered will enable your organisation to develop a sound foundational knowledge of planning and operations in the space domain.

The course is designed to complement the basic communication and EW fundamentals, allowing your planning, operational and management personnel to understand space theory fundamentals and apply and manage the principles as applied to military and civilian operations in space.

What you will learn:

- Overview of the space environment
- Understanding of different types of satellite orbit
- Advantages and disadvantages of orbits
- Satellite coverage
- Use of satellites - ISR, PNT, communications
- Indicators, warnings and tracking of events
- Satellites - payloads, launch, operation and optimisation
- Satellite planning
- Risks of space operations
- International space policy and doctrine
- Space definitions

Course Duration
2 Weeks

Location
Mercury EW Ltd – Training Facility

Antenna Course

Introduction

This ten-day course addresses the key fundamentals of antennas.

What you will learn:

- Basic Mathematics
- Properties of Electricity
- Basics of Communication
- Sinusoidal Waveforms
- Capacitance and Inductance
- Transmission lines
- Antenna Terminology
- Antenna Types
- Antenna Propagation
- Electromagnetic Defence
- Direction Finding Antennas
- Antenna Practical Exercises

Who should attend?

Anyone involved in the practical application, delivery and conduct of CEMA/EW in a deployed, operational context.

Key Organisations

Ministry of Defence

HQ Joint Forces

Defence Science and Technology Agencies/Defence Research Lab/ Institutes

All Government agencies, industries and organisations interested in developing CEMA/EW capability

Course Duration
2 Weeks

Location
Mercury EW Ltd – Training Facility

Communications Principles Course

Who should attend?

Military and civilian Communications Intelligence (COMINT) Electromagnetic Warfare (EW) practitioners from Strategic, Operational and Tactical backgrounds. Anyone involved in the practical application, delivery and conduct of EW in a deployed, operational context.

Key Organisations

Ministry of Defence

HQ Joint, Army, Navy and Air Force

All Government agencies, industries and organisations interested in the development of COMINT/EW capability

Introduction

This course is used to teach delegates new to the Electronic Warfare (EW) environment the underpinning communications knowledge required prior to enrolling on other Mercury EW Ltd courses. It addresses the basics of communications, including: common terminology, properties of electricity, Electromagnetic (EM) radiation and the EM Spectrum, how different forms of communications are created and propagated through various mediums, as well as the properties and functions of different types of antenna. A range of practical exercises are used to compliment the theoretical training. On completion of the course delegates will be well placed to understand communications and their effect on EW operations.

What you will learn:

- Basic mathematics associated with communications
- Properties of electricity
- Basics of communications
- Antenna theory
- Waveforms
- Modulation techniques (Amplitude Modulation (AM), Frequency Modulation (FM), Pulse Modulation (PM)
- Propagation
- Direction Finding (DF) Theory

Course Duration
1 Week

Location
Mercury EW Ltd – Training Facility

Battlespace Spectrum Management [BSM] Course

Introduction

This course addresses the key elements of spectrum management in a deployed operational context. This includes the organisation, policy, processes and procedures required to effectively manage the electromagnetic spectrum. It will address the principles of effective spectrum management including acquisition, planning and deployment of spectrum dependent capability; the spectrum management process from mission preparation to deployment, sustainment and recovery; multinational doctrine and proposed national, joint and single service policy, doctrine, organisation and procedures; examples of good practice and operational anecdotes; practical exercises based on realistic deployed scenarios.

What you will learn:

- The principles of spectrum management
- The spectrum management process
- Spectrum management considerations during the plan/prepare phase of an operation
- Spectrum management considerations during the operate/sustain phase of an operation
- Spectrum management considerations during the recover/transition phase of an operation
- The importance of spectrum monitoring and spectrum situational awareness
- The use of technology to assist the spectrum manager
- An awareness of spectrum dependent systems and key stakeholders
- How spectrum management can be integrated into the mission planning cycle
- How to produce a spectrum management plan
- How to coordinate the spectrum requirements with all key stakeholders
- How to mitigate and resolve radio-frequency interference

Who should attend?

Anyone involved in formulating strategy, policy, doctrine, processes or procedures for spectrum management in a deployed, operational context.

Anyone involved in the practical application, delivery and conduct of spectrum management in a deployed, operational context.

Key Organisations

Ministry of Defence

HQ Joint, Army, Navy and Air Force

Defence Science and Technology Agencies

Defence Research Lab/Institutes

All Government agencies, industries and organisations interested in development of Electromagnetic spectrum management

Course Duration
1 Week

Location
Mercury EW Ltd – Training Facility

Satellite Communications [SATCOM] Course

Who should attend?

Military and government civilian EW practitioners engaged in the exploitation of satellite communications.

Key Organisations

Ministry of Defence

HQ Joint, Army, Navy and Air Force intelligence operators/Analysts

All Government agencies, industries and organisations interested in operational and technical aspects of intelligence collection

Introduction

This SATCOM course will provide instruction on the introduction to the basics in electromagnetic wave propagation and antennas, introduction to Signals Intelligence (SIGINT) and key areas that impact on satellite communications.

What you will learn:

Basics in Electromagnetic wave propagation and antennas

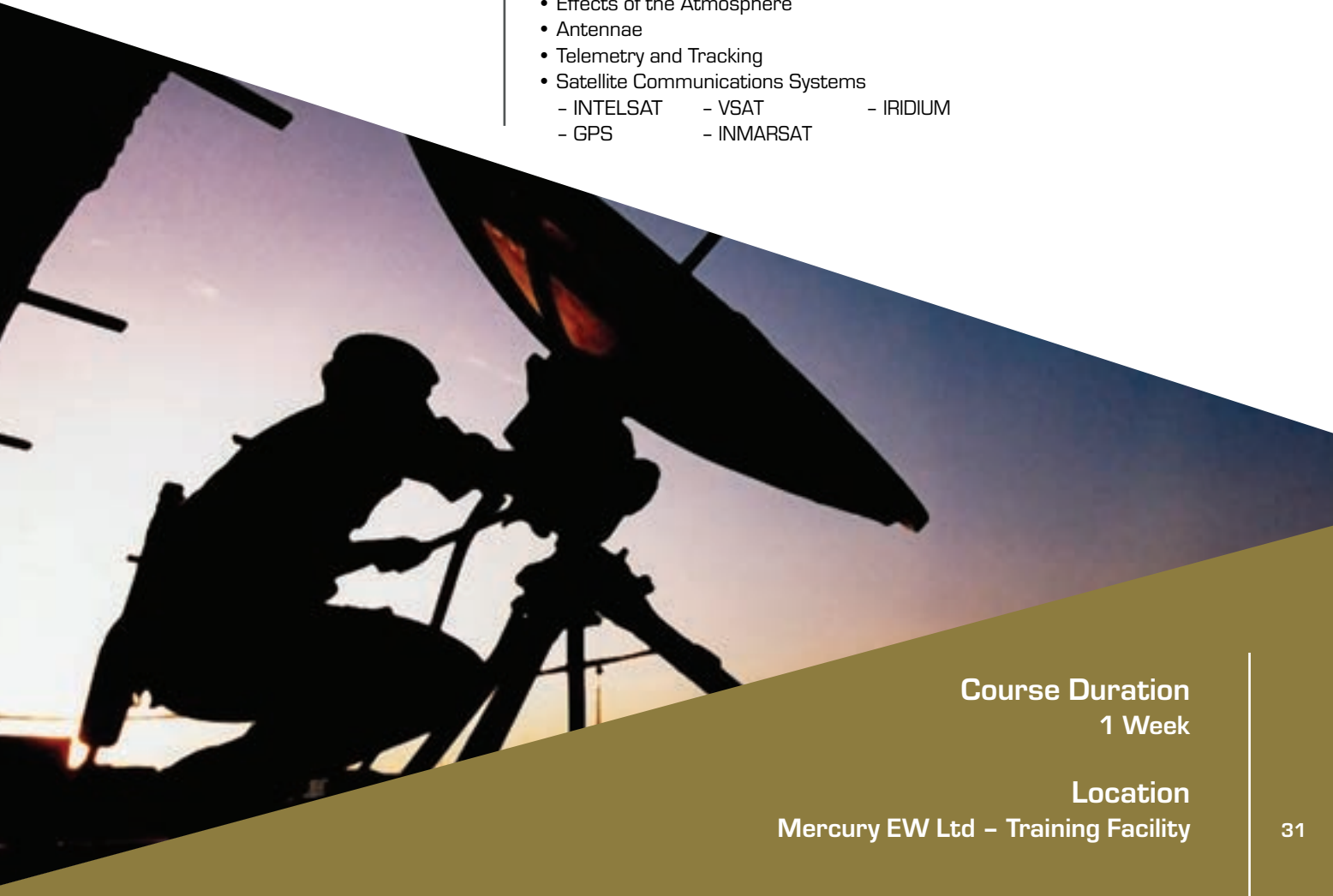
- Perform basic mathematics calculations relating to communications
- Explain the principles and properties of electricity
- Explain the fundamental principles of communications
- Explain the principles of electromagnetic radiation
- Explain various radio wave propagation

Introduction to Signal Intelligence (SIGINT)

- Introduction to Communications Intelligence (COMINT)
- Introduction to Electromagnetic Intelligence (ELINT)
- Introduction to Foreign Instrumentation Signals Intelligence (FISINT)
- SIGINT within Intelligence Collection
- Differences between SIGINT and Electromagnetic Warfare (EW)

Satellite Communications

- Satellite Communications History
- Orbits
- Space segment
- Propagation & Modulation
- Effects of the Atmosphere
- Antennae
- Telemetry and Tracking
- Satellite Communications Systems
  - INTELSAT
  - VSAT
  - IRIDIUM
  - GPS
  - INMARSAT



Course Duration
1 Week

Location
Mercury EW Ltd – Training Facility

Cellular Technology Overview Course

Introduction

This cellular technology training package provides delegates with an introduction to GSM, UMTS, LTE, and 5G technologies, providing foundational knowledge that can be applied to the utilisation of cellular sensing and effect capabilities.

What you will learn:

- Network Architecture/Components/Interfaces
- Frequency Bands
- Air Interfaces
- GSM Services
- Network Identities (IMEI, IMSI, MSISDN etc.)
- Network Coverage
- Cell Sectorisation
- Cell Capacity and Azimuth
- Signalling and Transaction Processing (Text, Voice & Data)
- UMTS (3G) Overview
- LTE (4G) Overview
- NR (5G) Overview

Who should attend?

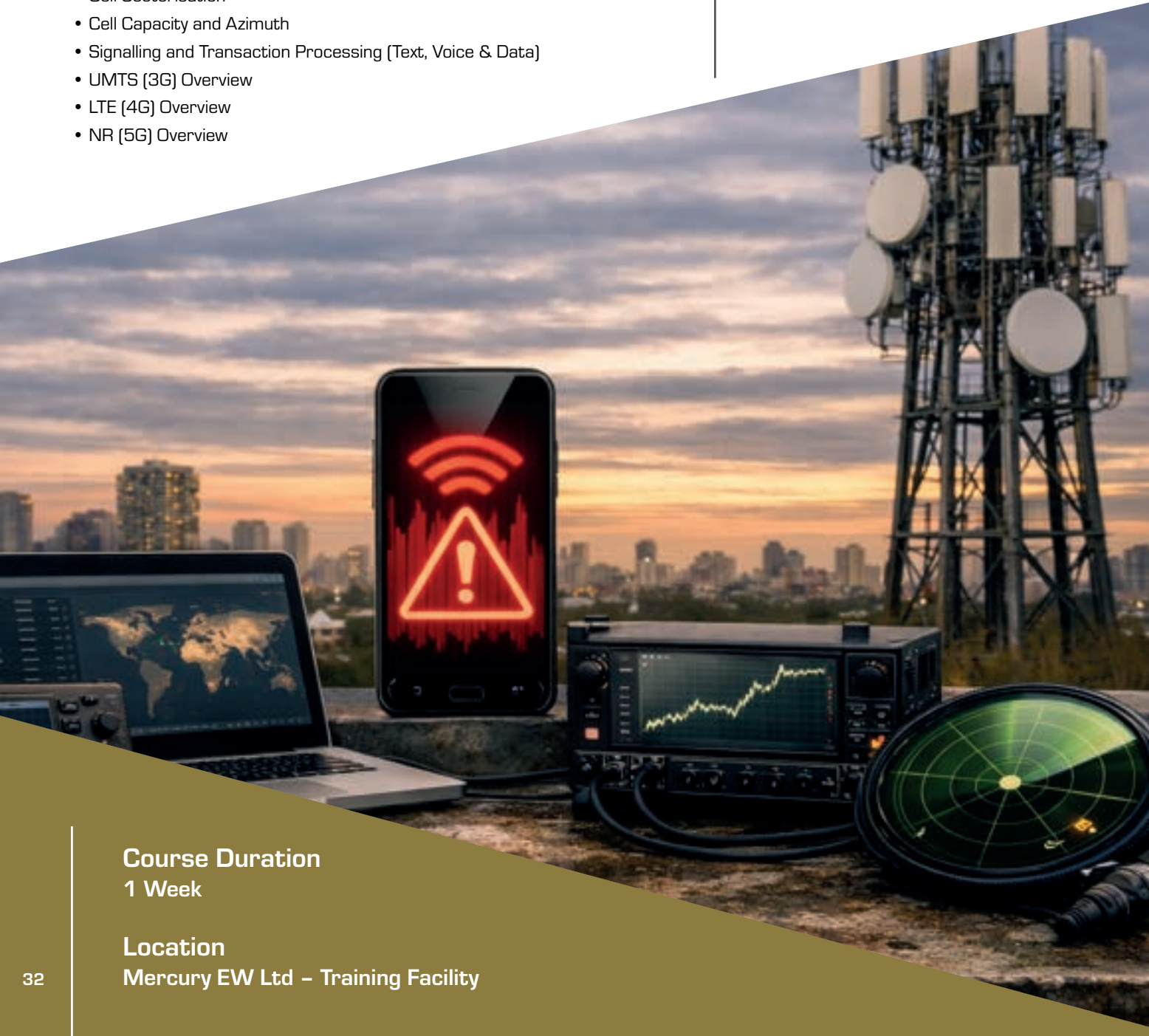
Military and government civilian Electonic Warfare (EW) practitioners engaged in the sensing and exploitation of cellular systems.

Key Organisations

Ministry of Defence

HQ Joint, Army, Navy and Air Force EW operators/Analysts

All Government agencies, industries and organisations interested in operational and technical aspects of EW



Course Duration
1 Week

Location
Mercury EW Ltd – Training Facility

Glossary of Terms

AM	Amplitude Modulation
ASMD	Anti-Ship Missile Defence
CATS	Credit Accumulation Transfer Scheme
CCIRM	Collection Coordination Intelligence Requirements Management
CDS	Course Document Set
CEMA	Cyber and Electromagnetic Activites
CNI	Critical National Infrastructure
COMINT	Communications Intelligence
C-RCIED	Counter Radio Controlled Improvised Explosive Device
C-UAS	Counter Uncrewed Aerial Systems
CVSS	Common Vulnerability Scoring System
DSAT	Defence Systems Approach to Training
DF	Direction Finding
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ELINT	Electromagnetic Intelligence
EA	Electromagnetic Attack
ED	Electromagnetic Defence
EO	Electro-Optical
EOB	Enemy/Electronic Order of Battle
ES	Electromagnetic Support/Electromagnetic Surveillance
EW	Electromagnetic Warfare
ESM	Electromagnetic Support Measure
ECM	Electromagnetic Counter Measure
EPM	Electromagnetic Protection Measure
FTS	Formal Training Statement
FM	Frequency Modulation
GPS	Global Positioning System
GSM	Global System for Mobile Communications
IMINT	Imagery Intelligence
IMEI	International Mobile Equipment Indentity
IMSI	International Mobile Subscriber Indentity
IQ	In-phase and Quadrature
ISTAR	Intelligence, Surveillance, Target Acquisition, Reconnaissance
JSP	Joint Service Publication
LTE	Long Term Evolution
MoD	Ministry of Defence
MSISDN	Mobile Station International Subscriber Directory Number
NR	New Radio
OPSEC	Operational Security
OSINT	Open Source Intelligence
PDW	Pulse Descriptor Word
PM	Phase Modulation
RCIED	Radio Controlled Improvised Explosive Device
RF	Radio Frequency
SOC	Security Operations Centre
TCP	Transmission Control Protocol / Internet Protocol
TTP	Tactics, Techniques & Procedures
UMTS	Universal Mobile Telecommunications System

Notes

+ 44 (0) 1526 830688

info@mercuryew.com

Haverholme Priory Offices
Haverholme Park, Ewerby, Sleaford, Lincolnshire NG34 9PF

mercuryew.com

CYBER ESSENTIALS PLUS

EMPLOYER RECOGNITION SCHEME GOLD AWARD

AUDITED IASME CYBER ASSURANCE LEVEL TWO

JOSCAR REGISTERED