SORINTEQ

TARGETED EQUIPMENT INTERFERENCE TACTICS

5-Day
Advanced Technical Course
Government Use Only

- 5 Day Programme
- Specialist Training for Law Enforcement
- All Training Equipment Provided
- In Association With the University of Buckingham

Contact Us

0333 0063248

Sorinteq Academy

SORINTEQ

Course Overview

Modern investigations increasingly require the ability to lawfully obtain intelligence and evidential opportunities directly from digital devices and systems used by subjects of interest. Where conventional investigative methods are limited, Targeted Equipment Interference (TEI) provides a specialist capability to support operational objectives.

The Targeted Equipment Interference Tactics Course is a practical 5-day advanced programme designed for technically competent Government personnel responsible for supporting or conducting Technical Equipment Interference activity and advanced Internet Intelligence & Investigation (I3) operations.

This course provides learners with a structured understanding of TEI planning, deployment considerations, operational tradecraft, legal frameworks, and technical opportunities. Delegates will examine the tactical application of authorised interference activity, operational security requirements, intelligence exploitation opportunities, and how TEI supports wider investigative and intelligence objectives.

The programme is highly operational and designed for experienced practitioners working in sensitive and technically demanding environments.

Who is the course for?

This course is strictly for Government personnel operating in advanced technical or covert investigative roles, including:

- Technical Equipment Interference (TEI) operators
- Cyber investigators and technical surveillance specialists
- Digital intelligence and advanced i3 practitioners
- Government cyber operational support teams
- Intelligence officers supporting covert digital activity
- Specialist law enforcement and national security teams
- Technical operators involved in covert access and evidential recovery

Participants should have strong technical competence and prior experience in digital investigations, Linux, networking, or advanced cyber operational environments.

SORINTEQ

Course Content

The course provides advanced practitioner-led instruction across key operational areas, including:

- Introduction to Targeted Equipment Interference
- Understanding TEI capability, operational purpose, and investigative value
- Legal Authorities and Governance Frameworks
- Necessity, proportionality, authorisation, oversight, and compliance requirements
- Operational Planning and Target Assessment
- Identifying opportunities, threat modelling, and operational decision-making
- Delivery and Deployment Considerations
- Understanding access opportunities, technical delivery pathways, and operational support requirements
- Technical Environment Awareness
- Devices, platforms, operating systems, cloud environments, and subject ecosystems
- Intelligence and Evidential Recovery Opportunities
- Identifying high-value data and supporting investigative outcomes
- Operational Security and Counter-Detection
- Protecting the operation, maintaining covert integrity, and reducing operational risk
- Integration with Wider Investigative Strategies
- Supporting cyber investigations, organised crime enquiries, and national security operations
- Evidence Handling and Reporting
- Continuity, forensic defensibility, reporting standards, and disclosure considerations
- Case Studies and Operational Lessons Learned
- Real-world examples demonstrating TEI success, failure, and best practice

Final Exercise Phase

- Live TEI Operational Planning Scenario
- Participants design and manage a full Targeted Equipment Interference deployment plan
- Technical and Strategic Decision-Making Exercise
- Applying legal, operational, and technical considerations to a realistic investigation
- Debrief and Operational Review
- Structured feedback on planning, governance, execution, and evidential opportunities

SORINTEQ

Aims and Objectives of the Course

By the end of the course, participants will be able to:

- Understand the operational role of Targeted Equipment Interference within modern investigations
- Identify when TEI provides lawful and proportionate investigative opportunities
- Plan and support TEI operations within legal and governance frameworks
- Understand technical delivery methods and deployment considerations
- Apply operational security (OpSec) and risk management principles to TEI activity
- Identify intelligence and evidential recovery opportunities from targeted systems
- Support investigative strategy through structured technical exploitation
- Maintain evidential integrity and defensible operational practice throughout TEI deployments

Why Choose Sorinteq

Sorinteq delivers university-accredited, practitioner-led training trusted by Government agencies. Our specialist technical training develops real operational capability for teams working in high-risk, high-complexity environments where legal compliance, technical precision, and investigative effectiveness are critical. Students undertaking courses provided by Sorinteq may earn credits towards formal academic qualifications such as Post Graduate Certificate, Diploma or MSc at the university of Buckingham.

For further enquiries please email info@sorinteq.com or call Sorinteq on +44 (0)333 0063248.

Sorinteq provide all necessary training equipment including laptop computers, internet connectivity, mobile devices and training material.