Internet of Battle Things (IoBT) Security Training Course

Professional Development Training Course Outline

Category	Defense and Security	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Internet of Battle Things (IoBT) represents a rapidly expanding ecosystem of interconnected autonomous systems, sensors, drones, wearable devices, and intelligent platforms that support next-generation military operations. As armed forces deploy real-time analytics, artificial intelligence, and distributed tactical networks, ensuring IoBT security has become mission-critical. Internet of Battle Things (IoBT) Security Training Course provides a comprehensive framework for securing highly dynamic, cyber-enabled combat environments where data must be trusted, communications must be resilient, and digital systems must operate under extreme adversarial pressures.

Participants will explore advanced cybersecurity strategies, battlefield data protection methods, autonomous system defense, and secure mission-critical communication architectures. The training emphasizes strong keywords such as cyber defense, tactical networks, AI-enabled battlefield systems, adversarial threats, and operational resilience. By blending technical knowledge with practical case studies, the course equips learners with the expertise to secure IoBT environments, mitigate cyberattacks, and strengthen operational readiness across modern defense ecosystems.

Programme Curriculum

Internet of Battle Things (IoBT) Security Training Course

Introduction

Internet of Battle Things (IoBT) represents a rapidly expanding ecosystem of interconnected autonomous systems, sensors, drones, wearable devices, and intelligent platforms that support next-generation military operations. As armed forces deploy real-time analytics, artificial intelligence, and distributed tactical networks, ensuring IoBT security has become mission-critical. Internet of Battle Things (IoBT) Security Training Course provides a comprehensive framework for securing highly dynamic, cyber-enabled combat environments where

data must be trusted, communications must be resilient, and digital systems must operate under extreme adversarial pressures.

Participants will explore advanced cybersecurity strategies, battlefield data protection methods, autonomous system defense, and secure mission-critical communication architectures. The training emphasizes strong keywords such as cyber defense, tactical networks, AI-enabled battlefield systems, adversarial threats, and operational resilience. By blending technical knowledge with practical case studies, the course equips learners with the expertise to secure IoBT environments, mitigate cyberattacks, and strengthen operational readiness across modern defense ecosystems.

Course Objectives

1. Understand the architecture, components, and vulnerabilities of Internet of Battle Things ecosystems.
2. Analyze emerging cyber threats targeting AI-enabled battlefield systems.
3. Apply advanced cybersecurity controls across tactical IoT and autonomous battlefield devices.
4. Strengthen secure communication protocols in contested electromagnetic environments.
5. Implement real-time intrusion detection and threat intelligence for IoBT networks.
6. Protect battlefield sensor data integrity using trending cyber defense strategies.
7. Evaluate interoperability risks across multi-domain and coalition forces.
8. Integrate AI-driven cyber defense tools for adaptive battlefield protection.
9. Develop resilient mission-critical architectures under cyber disruption.
10. Implement secure device lifecycle management for ruggedized military IoT.
11. Conduct risk assessments and battlefield cyber readiness evaluations.
12. Apply encryption, authentication, and zero-trust principles to tactical systems.
13. Strengthen operational resilience through secure system design and continuous monitoring.

Organizational Benefits

- Enhanced protection of mission-critical battlefield systems
- Strengthened cyber resilience against sophisticated adversaries
- Improved interoperability across multi-domain military operations
- Reduced vulnerability of autonomous and AI-enabled combat devices
- Increased operational readiness through proactive threat mitigation
- Improved trust and reliability in battlefield data and analytics
- Stronger defense-wide cybersecurity governance and compliance
- Lower long-term security costs through integrated protection frameworks
- Better alignment with emerging defense technology standards
- Enhanced strategic advantage through secure digital transformation

Target Audiences

- Defense cybersecurity professionals
- Military communications and network engineers
- Tactical operations and battlefield technology teams
- AI and autonomous systems specialists
- Cyber threat intelligence analysts
- Defense technology policymakers and program managers
- Military systems integrators and contractors
- Research institutions working on advanced defense technologies

Course Duration: 10 days

Course Modules

Module 1: Introduction to IoBT Ecosystems

- Define IoBT technologies and battlefield system interconnections
- Explore tactical IoT, autonomous devices, and multi-domain systems
- Identify IoBT vulnerabilities and operational weak points
- Examine adversarial environments and contested zones
- Assess intelligence and data exchange demands
- Case Study: System compromise in a multi-sensor battlefield network

Module 2: Cyber Threat Landscape for IoBT

- Review advanced persistent threats targeting military IoT
- Assess AI-enabled cyberattacks and battlefield malware
- Examine electronic warfare and signal jamming risks
- Understand tactical deception and spoofing techniques
- Analyze attack vectors across autonomous platforms
- Case Study: Cyber intrusion during a joint military exercise

Module 3: Secure Battlefield Communication Networks

- Protect tactical communication channels under hostile conditions
- Implement secure protocols for real-time battlefield data
- Strengthen network resilience in degraded or denied environments
- Apply frequency-hopping and anti-jamming techniques
- Integrate encrypted mission-critical communication flows
- Case Study: Communication disruption in an armored battalion

Module 4: AI-Enabled Systems and Autonomous Platform Security

- Examine AI-driven decision systems in combat settings
- Identify algorithmic vulnerabilities and adversarial AI
- Ensure secure machine-to-machine interactions
- Apply defensive AI to counter enemy cyber infiltration
- Design safe autonomous battlefield workflows
- Case Study: Adversarial AI attack on autonomous drone swarms

Module 5: Zero-Trust Architectures for Tactical Environments

- Apply zero-trust principles to battlefield devices
- Strengthen identity and access controls in tactical systems
- Secure micro-perimeters across distributed combat zones
- Implement least-privilege access for autonomous units
- Monitor device behavior for threat anomalies
- Case Study: Zero-trust implementation in a forward operating base

Module 6: Data Protection & Integrity in Battlefield Systems

- Ensure accuracy and trustworthiness of sensor data
- Apply encryption and secure hashing to tactical information
- Strengthen battlefield data integrity pipelines

- Implement anti-tampering measures on rugged devices
- Mitigate data corruption under cyberattack
- Case Study: Tampered intelligence data during reconnaissance

Module 7: IoBT Device Lifecycle Security

- Establish secure deployment and configuration routines
- Monitor device health in high-risk environments
- Implement ruggedized endpoint protection
- Secure firmware and patch management at scale
- Prevent unauthorized device replacement or modifications
- Case Study: Compromised battlefield device through supply chain infiltration

Module 8: Cloud, Edge, and Fog Computing in Military Operations

- Explore distributed computing models for real-time operations
- Secure tactical edge nodes and fog computing systems
- Ensure resilient connectivity during mobile missions
- Protect data flows between cloud and battlefield devices
- Identify multi-layer processing vulnerabilities
- Case Study: Edge network attack in a battlefield simulation

Module 9: Encryption and Cryptographic Controls

- Implement battlefield-ready encryption methods
- Secure inter-device communication with cryptographic protocols
- Protect sensor data flows with lightweight cryptography
- Apply quantum-resistant encryption strategies
- Mitigate risks of key exposure in combat zones
- Case Study: Encryption failure in intelligence transmission

Module 10: Battlefield Cyber Threat Intelligence

- Develop threat intelligence tailored to combat operations
- Integrate real-time cyber situational awareness
- Identify battlefield threat actors and capabilities
- Map indicators of compromise in tactical devices
- Apply intelligence-driven defensive actions
- Case Study: Tactical threat intelligence revealing enemy cyber posture

Module 11: Intrusion Detection & Real-Time Security Monitoring

- Deploy IDS technologies suitable for battlefield networks
- Monitor autonomous platforms for suspicious activity
- Apply behaviour-based anomaly detection
- Correlate multi-sensor alerts for rapid decision-making
- Integrate monitoring tools with command systems
- Case Study: Intrusion detection success during an urban combat mission

Module 12: Human Factors & Operational Cybersecurity

- Evaluate cyber hygiene practices of deployed personnel

- Address cognitive overload in digital-rich battlefields
- Implement secure user behaviors under stress
- Train forces in rapid cyber response actions
- Mitigate insider threat risks in tactical operations
- Case Study: Human error leading to IoBT compromise

Module 13: Multi-Domain and Coalition Security Integration

- Ensure secure interoperability across allied forces
- Implement unified security standards for joint operations
- Manage data exchange risks in multinational missions
- Align policies for shared battlefield technologies
- Mitigate cross-force vulnerabilities
- Case Study: Coalition cybersecurity gap during joint peacekeeping

Module 14: Resilience Engineering for IoBT Systems

- Build redundancy for mission-critical battlefield assets
- Implement self-healing architectures in IoBT systems
- Strengthen cyber-physical continuity under attack
- Evaluate system recovery in active conflict zones
- Design resilient battlefield technology strategies
- Case Study: Resilient command-and-control system under cyber disruption

Module 15: Strategic Governance & Future Force Modernization

- Establish governance models for secure IoBT operations
- Integrate cybersecurity into modernization programs
- Develop long-term investment frameworks for AI and IoBT
- Align defense policies with emerging battlefield technologies
- Strengthen leadership oversight and accountability
- Case Study: National modernization program for IoBT integration

Training Methodology

- Instructor-led presentations and guided learning
- Group activities using real IoBT security scenarios
- Case study analysis focused on battlefield cyber operations
- Practical demonstrations of tactical security tools
- Structured exercises for threat mapping and risk analysis
- Development of operational action plans for IoBT security

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.com or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to FINESKILL TRAINING CENTER account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
07 Sep 2026	18 Sep 2026	Physical	$3,000
14 Sep 2026	25 Sep 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
28 Sep 2026	09 Oct 2026	Physical	$3,000
05 Oct 2026	16 Oct 2026	Physical	$3,000
12 Oct 2026	23 Oct 2026	Physical	$3,000
19 Oct 2026	30 Oct 2026	Physical	$3,000
26 Oct 2026	06 Nov 2026	Physical	$3,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com