Foundation of AI for Secure and Responsible Military Systems

5-Day Intensive Bootcamp Syllabus

Program Overview

The *Foundation of AI for Secure and Responsible Military Systems* bootcamp provides a structured, non-coding introduction to artificial intelligence as applied to modern military and defense environments. The program emphasizes **security, responsibility, governance, and operational readiness**, ensuring participants understand both the capabilities and risks of AI-enabled systems.

This course is designed to prepare participants to **evaluate, support, and oversee AI systems** in military contexts while maintaining human accountability, mission assurance, and ethical compliance.

Target Audience

- Military personnel (officers, enlisted, analysts)
- Defense contractors and systems integrators
- Cybersecurity and IT professionals
- Systems engineers and architects
- Policy, acquisition, and program management staff

Prerequisites

- General understanding of IT, cybersecurity, or military systems
- No programming or data science experience required

Learning Outcomes

By the end of this bootcamp, participants will be able to: - Explain foundational AI and machine learning concepts in a military context - Identify security risks and adversarial

threats to AI systems - Apply responsible and ethical principles to AI-enabled military operations - Understand AI governance, risk management, and oversight requirements - Evaluate AI systems for operational readiness and mission alignment

---

Day 1 – Foundations of Artificial Intelligence in Military Systems

Objectives

- Understand core AI concepts and terminology
- Identify current and emerging AI applications in military systems
- Distinguish operational reality from AI hype

Topics

- Artificial Intelligence vs Machine Learning vs Deep Learning
- Narrow AI vs General AI
- AI lifecycle: data, model development, deployment, monitoring
- AI use cases in military environments:
    - Intelligence, Surveillance, and Reconnaissance (ISR)
    - Logistics and predictive maintenance
    - Cyber defense and threat detection
    - Decision-support systems

Practical Activity

- Mapping AI capabilities to military missions

Day 2 – Secure AI Systems and Adversarial Threats

Objectives

- Understand vulnerabilities unique to AI-enabled systems
- Identify adversarial threats and attack vectors
- Learn defensive strategies for securing AI pipelines

Topics

- AI attack surface overview
- Adversarial machine learning:
    - Data poisoning
    - Model evasion
    - Model extraction and inversion

- AI supply chain risks (models, datasets, vendors)
- Securing AI systems:
  - Data integrity and validation
  - Model testing and assurance
  - Secure deployment environments

Practical Activity

- Threat modeling an AI-enabled military system

Day 3 – Responsible, Ethical, and Lawful Use of Military AI

Objectives

- Understand ethical risks and operational consequences of AI misuse
- Apply responsibility principles to military decision-making
- Reinforce human accountability in AI-supported operations

Topics

- Responsible AI principles:
  - Human-in-the-loop and human-on-the-loop
  - Transparency and explainability
  - Bias, fairness, and unintended outcomes
- AI-assisted decision-making vs autonomous action
- Rules of engagement and command responsibility
- Automation bias and over-reliance on AI outputs

Case Studies

- Ethical dilemmas in AI-assisted targeting
- Misidentification and escalation risks

Day 4 – Governance, Policy, and AI Risk Management

Objectives

- Understand AI governance in defense environments
- Learn how AI systems are reviewed, approved, and monitored
- Apply structured risk management to AI programs

Topics

- AI governance frameworks and oversight models
- Risk classification of AI systems
- Model testing, validation, and auditability
- Documentation and lifecycle management
- AI considerations in acquisition and procurement
- Internal review boards and approval processes

Practical Activity

- AI risk assessment checklist for military systems

Day 5 – Operational Readiness and the Future of Military AI

Objectives

- Evaluate AI systems for operational deployment
- Understand future trends shaping AI-enabled warfare
- Prepare organizations for responsible AI adoption

Topics

- AI maturity models for military organizations
- Integration with legacy systems
- Training personnel to work effectively with AI tools
- AI in joint, coalition, and allied operations
- Emerging trends:
    - Edge AI and battlefield systems
    - Autonomous logistics
    - AI-enabled cyber operations

Capstone Exercise

- End-to-end evaluation of a hypothetical AI-enabled military system:
    - Security considerations
    - Ethical and legal alignment
    - Governance and oversight
    - Operational fit