The Invisible Battlefield: Cybersecurity & the Armed Forces

Duration of Program on

10 Days (2 weeks)

Dates: 13 - 25 January 2025

Time: 11:00 AM- 1:00 PM (2 Hrs)

The Training Program is to deliver the following outcomes:

1. **Enhanced Network Security:** Improved defence mechanisms against cyber-attacks
2. **Real-Time Threat Detection:** Implementation of monitoring and alerting systems to detect suspicious activities, relying on established methodologies and tools
3. **Secure Communication:** Development of encrypted communication systems for defence.
4. **Incident Response:** Creation of robust response plans for cyber incidents.
5. **Operational Efficiency:** Proactive detection and patching of vulnerabilities.

S. No	Day	Topic	Subtopic
1.	Day 1	The Strategic Importance of Cybersecurity in Defence	• Overview of cybersecurity challenges in the defense sector. • Case Study: Cyberattacks on military infrastructure (e.g., Stuxnet and its implications). • Understanding the cyber kill chain in defense scenarios. • Practical: Simulate identifying vulnerabilities in a defense network.
2.	Day 2	Cyber Threat Intelligence for Defence Operations	• Types of cyber threats targeting defense systems (Apts, ransomware, supply chain attacks). • Role of threat intelligence in mitigating attacks. • Case Study: Attacks on Indian defense networks (e.g., foreign espionage). • Practical: Analyze simulated threat intelligence feeds.
3.	Day 3 & 4	Securing Critical Defence Infrastructure and Communications	• Cybersecurity frameworks for critical defense systems (NCIIPC, Zero Trust). • Protecting communication channels: Satellite, RF, IoT in military use. • Lessons from SCADA system attacks.

			• Practical: Secure Modbus-based PLCs and mitigate risks in military IoT.
4.	Day 5 & 6	Offensive Cybersecurity for Defence	• Understanding cyber operations: reconnaissance, exploitation, payload delivery. • Cyber warfare strategies: Defensive vs Offensive doctrines. • Case Study: Cyber warfare analysis (e.g., Ukraine conflict). • Practical: Red team exercise targeting a mock defense network.
5.	Day 7	Cybersecurity for Artificial Intelligence in Defence	• Understanding vulnerabilities in AI systems used in defense: Adversarial attacks, poisoning, and bias. • Case Study: Adversarial AI used to manipulate image recognition systems in drones. • Best practices for securing AI pipelines. • Practical: Perform an adversarial attack on a simple AI model and implement defenses.
6.	Day 8	Building Cyber Resilience in the Defence Ecosystem	• Cyber resilience strategies: Redundancy, incident response, and recovery. • Economic and operational considerations. • Case Study: Analysis of India's cybersecurity preparedness. • Discussion: Balancing cybersecurity costs with operational capability. • Case Study: Resilient architectures used in NATO and their applicability in Indian defense.
7.	Day 9	Emerging Threats and Trends in Defence Cybersecurity	• Threats from quantum computing, deepfakes, and AI in cyber warfare. • Case Study: Deepfake disinformation campaigns. • Role of cyber diplomacy in defense. • Practical: Detecting deepfake content in military communications.
8.	Day 10	Tabletop Exercise /Discussions & Assessment	• Insider Threat with Sensitive Data Exfiltration • Supply Chain Attacks • Ransomware Attack on Base IT Infrastructure