DEPARTMENT OF SPACE STUDIES
MERI
धराशक्तिक: व्योमशक्तिक:
Empowerer of the Earth, Empowerer of Space.

CENTRE FOR LAND WARFARE STUDIES
CLAWS
अन्वेषणं ज्ञानस्य मुख्यम्।

MERI
GROUP OF INSTITUTIONS

CYBER FRONTIER 2026

From Defence Manufacturing to Tactical Operations: Build the resilience to shield national security architectures from state-sponsored threats.

5th Oct to 16th Oct 2026

Core Learning Pillars

Strategic Doctrine

Understand the geopolitics of cyberspace, state-sponsored cyber operations, and cognitive warfare doctrines.

Net-Centric Security

Master securing Software-Defined Radios (SDRs), military satellite communications, and C4ISR systems.

Operational Defence

Implement Zero-Trust Architecture, coordinate military incident response, and conduct digital forensics.

Why Cyber Frontier 2026

- ☑ Joint collaboration between CLAWS and MERI, combining military insight with academic rigor.
- ☑ Intensive 10-day (40-hour) program with 65% hands-on practical lab content.
- ☑ Specifically designed for Indian Army officers and professionals in the defence industry ecosystem.

About the Course

This specialized executive certificate course equips participants with a comprehensive understanding of cyber warfare dynamics and advanced defensive technical capabilities necessary to secure critical military infrastructure. By bridging high-level defence policy with operational execution, the program provides Indian Army officers and industry professionals with technical foresight and tactics to shield national security architectures.

FOR CONTACT / CLARIFICATION

+91 93119 50041 (Whatsapp Active)

itmanager.claws@gmail.com

About the Programme

The Executive Certificate Course in Cyber Security for Defence provides a distinct advantage through its strategic collaboration between the MERI Group of Institutions and CLAWS, directly bridging high-level military doctrine with operational execution. The program's strongest asset is its rigorous hands-on methodology, dedicating 65% of the 40-hour curriculum (26 hours) to practical laboratory work within an isolated, air-gapped sandbox environment. Designed specifically for Indian Army officers and defence industry professionals, the curriculum moves beyond theory by requiring participants to deploy Zero-Trust Architectures, train AI models for predictive threat hunting, and conduct live malware reverse-engineering. Additionally, the training uniquely addresses the security of indigenised defence manufacturing (Atmanirbhar Bharat) through targeted supply chain vulnerability management. The comprehensive experience culminates in a live tabletop wargame using MITRE's Caldera, ensuring participants can seamlessly translate technical engineering into tactical crisis management under simulated operational stress.

10 Days | 40 Hours | Online Mode | 4 Core Academic Modules

The 40-hour curriculum is divided into 4 core academic modules to ensure a progressive learning curve from theory to hands-on applications:

Module I: Cyber Warfare & Strategic Doctrine (10 Hours)

- Geopolitics of cyberspace, state-sponsored cyber operations, and information warfare.
- National Cyber Security Strategies and integration into conventional military planning.

Module II: Tactical Net-Centric Security (10 Hours)

- Securing Software-Defined Radios (SDRs), military SATCOM, and IoT/C4ISR systems.
- Supply chain vulnerability management for defence manufacturing.

Module III: Operational Cyber Defence & Emerging Tech (12 Hours)

- Zero-Trust Architecture (ZTA) implementation and Quantum Key Distribution (QKD) protocols.
- AI and Machine Learning frameworks for predictive threat hunting and anomaly detection.

Module IV: Incident Command, Forensics & Compliance (8 Hours)

- Military Incident Response Procedures (IRP) and digital forensics for breach investigation.
- Legal frameworks including the IT Act, DPDP Act 2023, and international cyber laws.

Technical Stack Blueprint

Category	Key Tools & Libraries
Network Security & COMSEC	Wireshark, Tshark, GNU Radio, Nmap, Zenmap, OpenVPN, WireGuard
AI/ML & Threat Hunting	Scikit-Learn, TensorFlow, PyTorch, Hugging Face Transformers, YOLOv8, OpenCV
Threat Intel & SIEM	Open Search Elastic Security (ELK Stack), MISP, Zeek
Digital Forensics & IR	Ghidra, Volatility Framework Autopsy, Sleuth Kit, YARA
DevSecOps & Supply Chain,	Trivy, Grype, OWASP Dependency-Check,OpenScap
Simulation & Wargaming	Caldera (by MITRE), Docker, Kubernetes

Assessment & Certification

Assessment Component	Weightage	Format
Continuous Lab Assessments	30%	Execution of daily practical exercises (e.g., ZTA configuration, malware isolation)
Capstone Project & Defence	40%	Problem-solving execution (Whitepaper & Prototype) + Panel Presentation (15 mins) & Q&A
Tabletop Wargame Performance	20%	Strategic decision-making and collaborative threat containment during Day 10 simulation
Aptitude & Viva Voce	10%	Individual oral examination evaluating legal frameworks, ethics, and tactical sovereignty

Registration Fee & Payment

The fee for the programme is 5,000 /- which should be paid via NEFT/ Or UPI, the applicants must use the form (Scan QR code) to complete the Registration

Name : Centre for Land Warfare Studies

Branch : Canara Bank, Delhi Cantt

Bank Account No : 91162010005981

IFSC Code : CNRB0019008

MICR No : 110015357

Payments can be made via Army Training Grant (ATG) for the course