DefAI: Cyber & AI Frontiers for Defence

(Schedule)

Brief Outline of the Cybersecurity and AI for Defence Applications Program

1. Understanding the intersection of cybersecurity and artificial intelligence through real-world defence scenarios.
2. Exploring AI-enabled cyber threat analysis, network defence strategies, and automated response systems tailored for defence.
3. Gaining expertise in protecting AI models from adversarial manipulation and using AI for malware detection and incident response.
4. Discussing ethical considerations, data security, and regulation in the context of AI in military systems.

The objectives include:

1. Understand AI and cybersecurity fundamentals for military applications.
2. Learn how AI can enhance threat detection and response.
3. Identify vulnerabilities in AI systems used in defence.
4. Study case studies involving AI in cyber warfare.
5. Discuss ethical, operational, and regulatory frameworks.

Duration of Program

The duration is based on client requirements (2 weeks). Tentative Dates are as follows
Dates: 14 July - 25 July 2025
Time: 2:00 PM- 4:00 PM (2 Hrs)

Expected outcome:

- Enhanced Security Posture: Defence systems are better prepared for AI-driven attacks.
- Secure AI Workflows: Understanding and deploying secure ML pipelines.
- Threat Prediction: Leveraging AI for threat intelligence.
- Rapid Incident Handling: AI-assisted SOC and automated remediation.
- Future Preparedness: Recognizing trends like deep fakes, LLMs, and quantum threats.

Tentative Schedule (Subject to Change)

Sr. No	Day	Topics	Subtopics
1	Day 1	Introduction to Cybersecurity and AI in Defence	• Overview of AI's role in cybersecurity • Defence applications of AI in cyber operations • Ethical implications and limitations
2	Day 2	Creation of Custom AI Models	• Fundamentals of Models • Data Preparation and Model Training • Model Deployment and Optimization
3	Day 3	Local LLM Setup with custom knowledge	• Deploying a Local LLM • Configuring OpenWebUI for Frontend • Integrating Custom • Knowledge Bases specific to use cases
4	Day 4	Using AI for Red Teaming : Part 1	• Automating Subdomain and Asset Enumeration • AI-Enhanced OSINT Techniques • Effective Content Discovery
5	Day 5	Using AI for Red Teaming: Part 2	• Leveraging AI for Reconnaissance • AI-Powered Fuzzing and Exploit Generation • Bypassing WAFs and Defensive Controls

6	**Day 6**	**Offensive Use of AI**	• AI-generated phishing campaigns • Malware generation and polymorphism • Red team automation using AI • Case: AI tools in the Ukraine cyber conflict
7	**Day 7**	**Cyber Threat Intelligence Augmented by AI**	• Automating threat hunting with AI • Correlation of logs and alert prioritization • Case: Indian military SOC enhancement using AI
8	**Day 8**	**Defensive Use AI**	• Malware Detection with AI • AI for Log Analysis • AI for Network Analysis • AI for threat detection
9	**Day 9**	**Emerging AI Threats**	• LLM misuse and prompt injection • Deepfakes in information warfare • Quantum threats to AI model confidentiality • Detection and mitigation strategies
10	**Day 10**	**Tabletop Simulation**	• AI System Locked by Ransomware • Fake AI Email Scam
11	**Day 11**	**Assessment for Grading (Online form MCQ Based)**	

Tabletop Exercise / Discussion Details:

Scenario 1: AI System Locked by Ransomware

Situation: Your organization's AI-powered automation system suddenly becomes unresponsive. A ransom note appears on all AI interfaces, demanding payment in cryptocurrency to unlock your data and restore services. The attack has halted key operations, including customer support and internal task automation.

Key Questions:

- What are the first steps your team should take to contain and investigate the incident?
- How do you determine if secure backups are available and viable for restoration?
- What factors will influence the decision to pay or refuse the ransom?
- How do you inform leadership, staff, and potentially affected customers about the situation?

Outcome: Participants should demonstrate an understanding of ransomware response plans, including containment, recovery, communication strategies, and legal considerations related to ransom payments.

Scenario:2 Fake AI Email Scam

Situation: Multiple employees report receiving personalized emails that appear to come from your company's AI assistant, instructing them to click a link for a "system update." Some employees clicked the link and now notice strange behavior on their systems. Your IT team suspects a phishing attack exploiting trust in your internal AI systems.

Key Questions:

- How do you quickly identify how many employees were targeted and who clicked the link?
- What steps should be taken immediately to contain and investigate potential infections?

- How will you verify whether your AI systems or email servers have been compromised?

- What training or technical measures can you introduce to prevent similar attacks in the future?

Outcome: Participants should showcase effective phishing response protocols, understand the risks of AI-generated phishing, and develop strategies for improving staff awareness and technical defenses.

Background Information

Brief Biodata of Chief Instructor:

Dr. Rohit Gautam has been working in cyber security for more than a decade and is serving as CISO at Hacktify Cyber Security. He has a PhD in Cyber Security and is the author of the book - **"Ultimate Web Pentesting Guide"** which is five star rated on amazon. He has also authored various best-selling courses in the field of cyber security on various online platforms. He is the board of studies member of Mandsaur University and reviews the curriculum for industry trends. He has actively found many zero days on various open source and commercial software's and his contributions has helped organizations patch critical vulnerabilities. He also works as a tactical instructor for the defence sector and imparts training for various service cyber groups.

He has been awarded as Cyber Security Samurai of the Year 2024 and Year 2023 by Bsides Bangalore. He actively speaks at various conferences like VULNCon, California Summit, Bsides Bangalore, OWASP Jaipur, Hakon etc. He was a mentor for CTF category for Indian Army Hackathon 2021. He has credentials like NCPT, NCBBR, NCFI and CCIO.