DISC 13

Defence India Startup Challenge

Problem Statements

S. No	Name of Agency	Number of Problem Statements
1.	Indian Army	03
2.	Indian Navy	02
3.	Indian Air Force	02
Total		07

Table of Contents

INDIAN ARMY

PROBLEM STATEMENTS

Problem Statement – 1: Advanced Autonomous AI-Driven Cyber-Security Framework for Isolated LAN Environments

Organization Name	**Indian Army**
Problem Statement/ Challenge title	Advanced Autonomous AI-Driven Cyber-Security Framework for Isolated LAN Environments
Challenge brief/definition	In isolated, air-gapped Local Area Networks (LANs), conventional security methods that rely on external updates and signature-based detection are inadequate against evolving cyber threats, zero-day attacks and insider threats. The lack of internet connectivity restricts real-time updates, rendering these networks vulnerable. Additionally, static security mechanisms, such as password-based authentication, fail to detect ongoing anomalies or insider activities once user sessions are initiated. To address these challenges, a comprehensive AI-driven solution focused on LAN security is essential. This system will operate autonomously in offline environments, leveraging advanced User and Entity Behavior Analytics (UEBA) to continuously monitor user actions, system interactions, LAN traffic, and critical LAN parameters. By detecting deviations from normal behavior in real-time, the solution can identify insider threats, account takeovers, and unauthorized actions. Integrated anomaly detection algorithms will enhance proactive threat identification and risk mitigation. Utilizing techniques like pattern analysis and behavior profiling, the solution will ensure continuous monitoring of network activities, effective USB device tracking, and advanced Next-Generation Antivirus (NGAV) capabilities for comprehensive malware detection within isolated LANs. This AI-based defence mechanism will dynamically secure sensitive data and mission-critical systems against modern cyber threats, including unauthorized USB device connections and malware infiltration, significantly improving the overall security posture of isolated networks.

	The prototype system will be specifically designed for isolated, air-gapped Local Area Networks (LANs), providing robust and autonomous cybersecurity capabilities tailored to closed network environments. Recognizing that conventional security methods relying on external updates and signature-based detection are inadequate against evolving cyber threats, zero-day attacks, and insider threats, this system addresses the vulnerabilities resulting from a lack of internet connectivity, which hinders real-time updates and leaves networks exposed. Central to this prototype is a Next-Generation Antivirus (NGAV) and malware detection module leveraging advanced artificial intelligence and machine learning techniques. The Automated Threat Hunting feature will continuously monitor the LAN for potential threats, vulnerabilities, and signs of compromise, enhancing detection capabilities beyond traditional signature-based methods. Complementing this, an Incident Triage and Automated Mitigation system will assess the severity of detected incidents and initiate automated responses to neutralize threats swiftly, minimizing downtime and reducing reliance on human intervention. Additionally, the system will incorporate User and Entity Behavior Analytics (UEBA) to monitor user actions and system interactions, identifying suspicious anomalies that may indicate breaches or insider threats. Anomaly Detection Algorithms powered by machine learning will track irregularities in data traffic patterns within the LAN, ensuring proactive responses to potential cyber incidents. By continuously monitoring user actions, LAN traffic, and critical LAN parameters, the solution will utilize techniques such as pattern analysis and behavior profiling, ensuring effective USB device tracking and malware detection. This advanced AI-driven defence will dynamically secure sensitive data and mission-critical systems against modern cyber threats, significantly enhancing the overall security posture of isolated networks.

Problem Statement – 2: C-UAS Equipment (Cyber Takeover)

Organization Name	Indian Army
Problem Statement/ Challenge title	C-UAS Equipment (Cyber Takeover)
Challenge brief/definition	Drones have emerged as major challenge for traditional weapon systems to counter and hence require specialized C-UAS equipment. Multitude of C-UAS tech are being explored to counter this threat. Each counter measure also possesses weaknesses which can be exploited by the UAS. Worldwide, the electronic warfare systems including anti-UAS systems rely on spectrum-based detection and RF spectrum as the key means of interdicting the threat. However, jamming (Jx) and spoofing are not precise solutions and will invariably interfere with other nearby communication systems. These options will also adversely impact friendly drone ops. Small sized commercial drones being used en masse to saturate on Air Defences have evolved as major challenge in contemporary battlefield. After almost two and half years of continuous conflict the drones still operate freely in presence of Electronic Warfare (EW) systems like Krasukha, Leer, Pole 21 eqpt used by Russia & EDMGS, LDR 30 & LDR 50 equipment being used by Ukraine. This proves that either these systems are not effective or are being used in a calibrated manner to limit risks of electronic fratricide. Therefore, there is need to leverage the soft kill measures albeit with engagement capabilities. Cyber Takeover tech equipment as part of hybrid C-UAS solution more precise (when deployed with other hard kill measures) will provide precise engagement capability and will exponentially increase the target handling capability of this integrated system. A complete system should have following capabilities: (a) Operational deployment - Tactical, Vehicular, Sty/Tripod-based & man portable. (b) Compact, lightweight and small form factor.

	(c) Interdiction: - (i) Fend Off: Disconnect drone signal from Ground Control Station (GCS). (ii) Take Control/Land: Safe or crash landing of hostile drones at a predefined location. (d) Rs Coverage: - (i) Min 5 km detection range. (ii) Mitigation range between 1.2 – 4 Km. (iii) 360° omni coverage. (e) Technical Specifications: Operating Frequency is 400 MHz-6 GHz or above.

Problem Statement – 3: AI for Adaptive Networks

Organization Name	Indian Army
Problem Statement/ Challenge title	AI for Adaptive Networks
Challenge brief/definition	An Adaptive Network refers to a dynamic and responsive system that can adjust its parameters and behaviour in real-time based on changing conditions or inputs. These Networks often employ machine learning algorithms to optimize performance, allowing them to learn from experience and improve over time. The flexibility of Adaptive Networks makes them valuable where responsiveness to evolving scenario is paramount. **Pre-requisites:** (a) Robust security measures to shield the Network from cyber threats to including firewalls, IDS, secure access control, regular security audits and updates. (b) A well-defined infrastructure with adequate Bandwidth, a stable and high-performance internal Network and low latency for the optimal functioning. (c) Data Governance and Privacy Regulations must be strictly adhered to. Compliance with Regulatory Policies to ensure that sensitive info processed by the Network is handled responsibly. Adequate encryption, integrity, and trust measures should be implemented. (d) A comprehensive Backup & DR strategy is of paramount importance given the critical nature of Adaptive Networks in various applications to safeguard against data loss and system failures. Regular scheduled backups, redundant systems and efficient recovery protocols are imperative to minimize downtime and ensure the continuity. This challenge aims to achieve the following benefits: (a) **Network Planning, Management with Predictive Maintenance:** Enable enhanced predictive maintenance, optimizing Network performance, and automating fault detection and resolution. Intelligent traffic management and resource allocation, facilitated by AI algorithms, ensure efficient Network utilization.

	(b) **Network Security:** Threat detection, identification, segregation & mitigation along with Cyber Threat detection of anomalies and potential security threats within the network emanating from user end. Analysis of unusual traffic behaviour to identify any breaches can be carried out. This predictive analysis helps SOC teams anticipate emerging threats and prioritize their security efforts accordingly. (c) **Improvement:** AI analyses network traffic and user behaviour to optimize Quality of Service (QoS) parameters, ensuring a better user experience by prioritizing critical services and applications. (d) **Resource Management and Intelligent Resource Allocation:** AI algorithms for assistance in optimizing resource allocation, such as bandwidth allocation, spectrum optimization, and energy consumption, leading to more efficient utilization of resources. Allocation of Network resources based on real- time demand and user requirement can be achieved. (e) **Predictive Maintenance for Network Infrastructure:** AI algorithms can analyse data from Network devices and sensors to predict potential failures or performance issues before they occur. This proactive approach can be exploited for preventive maintenance, minimizing downtime and improving overall Network reliability.

INDIAN NAVY

PROBLEM STATEMENTS

Problem Statement – 4: IR Light based Communication System

Organization Name	**Indian Navy**
Problem Statement/ Challenge title	Design and development of IR Light based communication system for marine applications for mobile platform with secure data and voice.
Challenge brief/definition	The IR Light based Communication System aims to develop a secure and efficient means of communication using light signals in environment where radio frequency (RF) transmissions are restricted to undesirable. This system leverages optical communication technologies to ensure robust data transmission while minimizing electromagnetic interference. The challenge is to design and develop IR Light based communication system for marine applications for mobile platform with secure data and voice. These devices are expected to fit on a tripod/ mast using mounting arrangements and remain within the power budgeting of installed equipment. The system should be able to function with full efficiency till at least sea state 4 when deployed on mobile platform. Integration of these devices with existing ship borne systems also is to be undertaken by the system provider. The problem definition statement has deliberately been kept generic and broad based. The features of the IR Light based Communication System are as follows: (a) **Secure Communication.** Establish a reliable method for exchanging communication using light signals to prevent interception or unauthorized access. (b) **RF Silence Compliance.** Develop a communication system that operates without emitting RF signals or being in any dependency upon any other RF signal exchange, adhering to regulatory requirements and mitigating RF pollution.

	(c) **Performance Optimization.** Data transmission rates of at least 20 Mbps and voice communication rates at least 16 Kbps, and reliability through contemporary advancements in optical communication techniques and signal processing algorithms. (d) **Environmental Adaptability.** Design a system capable of functioning effectively in diverse environmental conditions, including both indoor and outdoor settings and marine conditions. (e) **Integration Feasibility.** Explore integration possibilities with existing naval data link systems as well as a standalone solution.

Problem Statement – 5: RADAR Obscurant Cloak for Aircraft

Organization Name	**Indian Navy**
Problem Statement/ Challenge title	RADAR Obscurant Cloak for Aircraft
Challenge brief/definition	1. Avoid detection of aircraft parked on ground from enemy radar. 2. Provision of a roll-on roll-off microwave obscurant cover for aircraft parked on ground to avoid detection from airborne radar.
Future Expectation from the prototype / Technology Developed	The product is expected to provide a light/ roll-on roll-off type canopy which can cover small and medium aircraft parked on ground. The top cover and the support structure is to be designed so as to minimize the radar signature of a parked aircraft.

INDIAN AIR FORCE

PROBLEM STATEMENTS

Problem Statement – 6: IP-based Gateway Interface between different SDR Networks

Organization Name	Indian Air Force
Problem Statement/ Challenge title	Development of Internet Protocol (IP)-based Gateway Interface for bridging inter-communication between two different Software Defined Radio (SDR) Networks.
Challenge brief/definition	The IAF has a long-standing requirement for new-generation radios and data links that can talk to existing IAF SDR. Development of IP Based Gateway Interface will provide solution to establish interoperability between SDRs of different make and hardware without dependency on the interoperable SDR waveform. IAF is in the process of procuring and deploying new generation SDRs for various airborne and C2 platforms. IAF SDRs can operate on L-Band, UHF & SATCOM. The vendor is expected to demonstrate the interoperability through IP Based Gateway Interface between two different SDR networks for voice and data both. **Preliminary scope of solution being developed:** 1. The IP Based Gateway Interface would include an interface for voice and data exchange between the two different SDR networks realised by IAF SDR and any Airborne SDR developed by Indian Industry. 2. The design and demonstration setup will be proposed by the vendor which may include combination of IAF SDR, Airborne SDRs developed by Indian Industry and Gateway Interface hardware. Demonstration for the interoperability through gateway interface would be conducted at Software Development Institute (SDI), Bengaluru. It will be divided in two phases viz. Phase I - Legacy and Secure Voice Communication and Phase II - Data Communication. 3. **Phase I:** It is proposed that voice communication in non-secure mode should be demonstrated as a proof of concept which can be executed without the need of ICD level information. Subsequently, for secure voice communication, the details of IAF SDR required for

	interfacing shall be facilitated through SDI. Based on which voice communication in secure mode should be demonstrated. The Lab evaluation of voice communication over gateway shall be assessed with reference to the quality of speech and delays observed in communication through gateway interface against the existing performance of IAF SDRs. 4. **Phase II:** Once the communication over non-secure and secure voice is proven through gateway interface, the vendor would demonstrate the exchange of defined data. 5. Post successful evaluation of Gateway solution at SDI, the flight trials (with IAF SDR as airborne member) shall be planned. The gateway solution shall be positioned within RT range of aircraft at trial location along with the other SDR at ground with Data and Voice reception end points to evaluate the interoperability. 6. After the successful demonstration during the flight trials, the technology transfer including details of software and electrical interface definitions of gateway interface to be shared with IAF.
Future Expectation from the prototype / Technology Developed	The Gateway solution would ensure interoperability between the SDRs of different make operating on different waveforms on different platforms.

Problem Statement – 7: Development of Battery-Operated Taxi Bots for Aircraft Movement

Organization Name	**Indian Air Force**
Problem Statement/ Challenge title	Development of Battery-Operated Taxi Bots for Aircraft Movement
Challenge brief/definition	Proposed Taxi bots will be used for towing of aircraft from standing start to holding point before take-off and from holding point till parking bay after landing. This will enable push back starts and engine off taxiing resulting in effective increase of available parking space, saving of aircraft fuel, engine hrs and manpower. **<u>Preliminary scope of solution being developed:</u>** 1. The battery-operated taxi bot is to designed to meet the requirement of taxiing the aeroplanes without starting the engines. 2. It should be controlled by the pilot and should not have any adverse effect on life of nose landing gear. 3. An interface mechanism should provide steering mechanism to the pilot for taxiing the aircraft to have similar handling characteristics as with engines running. 4. The system should have own power source and not require any power from the aircraft. 5. The system should not have any adverse effect on the cargo space or cause any increase in weight of the aeroplane. 6. There should not be any modification in the aeroplane. 7. The system should cater to the wide-bodied aircraft of IAF.
Future Expectation from the prototype / Technology Developed	Indigenously developed technology following industrial and environmental norms.