Problem 1: Secure Communication Channel for Defense Networks

Problem Statement

- Secure transmission of sensitive defense data is critical.
- Existing communication channels are vulnerable to cyberattacks and interception.
- Need for reliable, real-time, and tamper-proof communication in hostile environments.

More About the Problem

- Communication spans land, air, sea, satellite, and cyber networks.
- Threats include eavesdropping, jamming, spoofing, and insider attacks.
- Systems must ensure confidentiality, integrity, authentication, and availability.
- Balancing strong security with low latency and limited device resources is challenging.

What Companies Are Doing Now to Solve the Issue

- Implementing end-to-end and quantum-resistant encryption.
- Using secure software-defined radios with frequency hopping.
- Adopting Zero Trust security models for continuous authentication.
- Deploying AI-based monitoring for real-time threat detection.

Problem 2. Classified Data Leakage Prevention Engine

Problem Statement

- Prevent unauthorized leakage of classified or sensitive data.

More About the Problem

- Data leaks occur via emails, USBs, cloud uploads, or insider misuse.
- Traditional controls fail to detect contextual or intentional leaks.

What Companies Are Doing Now

- Data Loss Prevention (DLP) tools with rule-based monitoring.
- Endpoint and email security solutions.
- Manual audits and access restrictions.

Problem 3. Supply Chain Integrity Checker for Defense Hardware/Software

Problem Statement

- Ensure defense components are not tampered with during procurement.

More About the Problem

- Hardware backdoors and compromised software pose national risks.
- Global suppliers increase attack surface.

What Companies Are Doing Now

- Vendor audits and certifications.
- Firmware validation and checksum verification.
- Limited blockchain-based tracking.

Problem 4. AI-based Anomaly Detection for Radar/Telemetry Systems

Problem Statement

- Detect abnormal behavior in radar and telemetry data in real time.

More About the Problem

- Subtle anomalies may indicate spoofing or system failure.
- Manual monitoring is slow and error-prone.

What Companies Are Doing Now

- Rule-based alert systems.
- AI/ML models trained on historical sensor data.
- Offline post-event analysis.

Problem 5. Post-Quantum Cryptography Implementation Challenge

Problem Statement

- Protect systems from future quantum computing attacks.

More About the Problem

- Quantum computers can break current encryption.
- Migration without performance loss is difficult.

What Companies Are Doing Now

- Testing NIST-approved PQC algorithms.
- Hybrid cryptographic models.
- Research-stage deployments.

Problem 6. Digital Evidence Integrity Validator

Problem Statement

- Ensure digital evidence remains untampered and admissible.

More About the Problem

- Evidence can be altered during storage or transfer.
- Chain-of-custody is hard to maintain digitally.

What Companies Are Doing Now

- Hash-based verification.
- Timestamping and secure storage.
- Blockchain pilots for audit trails.

Problem 7. Dark Web Marketplace Monitoring Dashboard

Problem Statement

- Track illegal cybercrime activities on the dark web.

More About the Problem

- Threat actors trade malware, exploits, and stolen data.
- Dark web is dynamic and anonymized.

What Companies Are Doing Now

- Threat intelligence crawlers.
- Manual analyst monitoring.
- Subscription-based intelligence feeds.

Problem 8. Automated Metadata Removal Tool

Problem Statement

- Prevent sensitive information leaks via file metadata.

More About the Problem

- Metadata reveals author, location, device details.
- Often shared unknowingly.

What Companies Are Doing Now

- Manual metadata cleaning.
- Basic document sanitization tools.
- Policy-based file sharing controls.

Problem 9. Secure e-Government File Transfer Protocol

Problem Statement

- Securely transfer sensitive government documents.

More About the Problem

- Email and public cloud tools are insecure.
- Compliance and auditability are mandatory.

What Companies Are Doing Now

- Encrypted file transfer systems.
- VPN-based sharing.
- Government-specific secure portals.

Problem 10. Automated Log Correlation Tool for SOC Operations

Problem Statement

- Identify attacks by correlating logs from multiple systems.

More About the Problem

- Massive log volume overwhelms SOC teams.
- Isolated alerts miss advanced threats.

What Companies Are Doing Now

- SIEM platforms.
- Rule-based correlation.
- Limited AI-assisted analysis.

Problem 11. Cyber Threat Intelligence (CTI) Sharing Platform

Problem Statement

- Enable secure sharing of threat intelligence across organizations.

More About the Problem

- Delayed sharing increases attack impact.
- Trust and standardization issues exist.

What Companies Are Doing Now

- ISACs and closed sharing groups.
- STIX/TAXII-based platforms.
- Manual validation of intelligence.

Problem 12. Zero-Trust Access Control Model Simulator

Problem Statement

- Demonstrate and test Zero Trust security models.

More About the Problem

- Legacy perimeter security is ineffective.
- Organizations struggle to adopt Zero Trust.

What Companies Are Doing Now

- Zero Trust frameworks.
- Identity-based access control.
- Limited simulation or visualization tools.

Problem 13. AI-Powered Online Harassment Detector

Problem Statement

- Automatically detect harassment and abuse online.

More About the Problem

- Manual moderation does not scale.
- Language, sarcasm, and context are challenging.

What Companies Are Doing Now

- NLP-based content moderation.
- Keyword and sentiment analysis.
- Human-in-the-loop review systems.

Problem 14. Fake News / Deepfake Detection System

Problem Statement

- Detect manipulated media and misinformation.

More About the Problem

- AI-generated deepfakes are highly realistic.
- Rapid spread impacts public trust and security.

What Companies Are Doing Now

- Media forensics tools.
- AI-based image and video analysis.
- Platform-level fact-checking.

Problem 15. Cyber Incident Volunteer Coordination Platform

Problem Statement

- Coordinate cybersecurity volunteers during major incidents.

More About the Problem

- Skilled volunteers are underutilized.
- Lack of centralized task assignment and validation.

What Companies Are Doing Now

- Informal response groups.
- Ad-hoc communication platforms.
- Limited government-backed initiatives.