November 19, 2025

IFATSEA- GA25 – Cape Town – Americas Regional Meeting.

🔍 Detailed Cyber Threat Explanations for ATSEP

1. Malware Family Overview

Malware = *Malicious Software*. Its code designed to disrupt, damage, or gain unauthorized access to systems. It can infect laptops, engineering stations, or even embedded equipment if controls fail.

🧩 a. Virus

- **Definition:** A self-replicating program that attaches to legitimate files and spreads when the infected file is executed.
- **Typical behavior:** Modifies or corrupts software, data, or boot sectors.
- **Example:** A radar configuration file infected with a macro virus spreads to multiple engineering PCs.
- **Example:** A virus hidden in a maintenance report template infects other documentation PCs, spreading corrupted configuration data to field laptops during synchronization.
-

🪱 b. Worm

- **Definition:** Like a virus, but it spreads automatically across networks without user action.
- **Impact:** Can quickly saturate a network and overload communication channels or servers.
- **Example:** A worm propagates via shared drives, slowing down surveillance data transfer between centers.

🕵️ c. Trojan (Trojan Horse)

- **Definition:** A malicious program disguised as legitimate software or a useful tool.
- **Mechanism:** The user installs or runs it, unknowingly granting access or control to an attacker.
- **Example:** A “firmware update tool” that secretly installs remote access malware on a navigation aid control computer.

- ***Example:*** A counterfeit “frequency calibration utility” downloaded from an unofficial supplier site installs a hidden remote-access Trojan that gives the attacker access to VHF transceiver settings.

💣 d. Ransomware

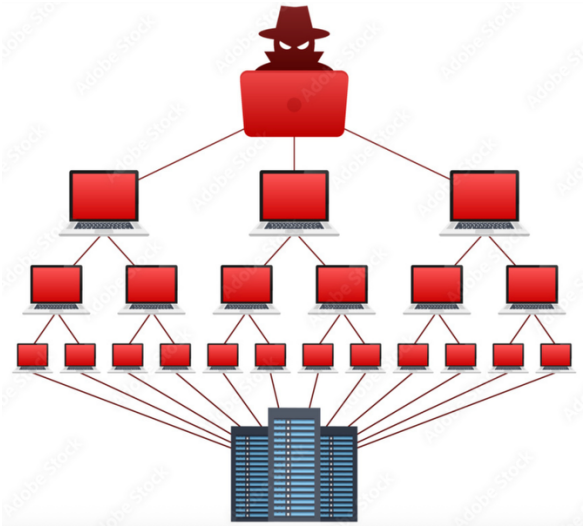
- **Definition:** Malware that encrypts data or systems and demands payment to restore access.
- **Impact:** Can paralyze operational systems if backups or redundancy are not properly secured.
- **Example:** A maintenance PC infected with ransomware locks configuration files used for critical equipment.

🎭 e. Spyware / Keylogger

- **Definition:** Software that secretly records activity (keystrokes, screens, or data) and sends it to an external actor.
- **Example:** Credentials captured from a system login used to access restricted networks later.
- ***Example:*** Spyware installed through malicious browser extension records credentials of engineers logging into the CNS monitoring interface and sends them to an external command server.

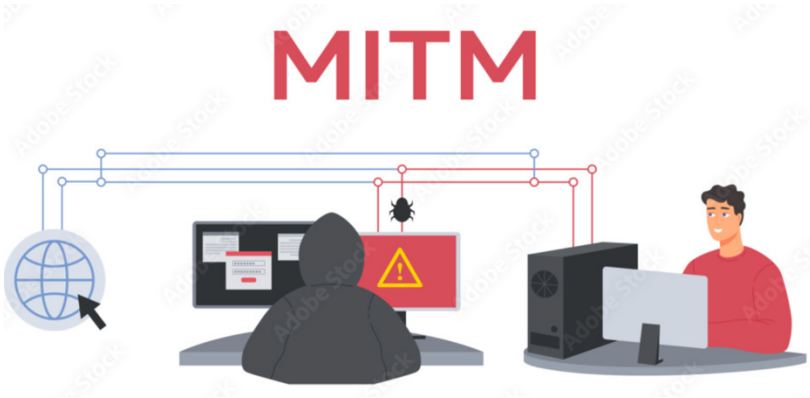
2. Denial-of-Service (DoS) and Distributed DoS (DDoS)

- **Definition:** Attackers intentionally overload a system, network, or service with excessive requests, making it unavailable to legitimate users.
- **How it works:**
  - **DoS:** A single source sends continuous traffic or commands to exhaust system resources.
  - **DDoS:** Many compromised computers ("botnet") simultaneously flood the target from different origins.
- **Example:** A DDoS against a remote ATC data gateway causes delays in radar data updates.
- **Why it matters to ATSEP:** These attacks can simulate "technical faults," masking cybersecurity incidents as normal outages.



3. Man-in-the-Middle (MitM) Attacks

- **Definition:** The attacker secretly intercepts or alters communication between two systems or users.
- **Example:** A malicious actor intercepts SNMP or FTP traffic between a monitoring station and a radar, altering data in transit.
- **Impact:** False system readings, corrupted configuration uploads, or data leakage.
- **Mitigation concept:** Encryption (TLS, VPN), authentication, and network segmentation.



4. Spoofing and Data Manipulation

- **Definition:** Faking legitimate data or signals to deceive systems.
- **Types:**
  - **IP Spoofing:** Pretending to be another IP address to gain access.
  - **GNSS Spoofing:** Broadcasting fake satellite signals to alter navigation data.
  - **Radar Spoofing:** Injecting false targets or modifying plots.
- **Example:** Spoofed GNSS data misleading aircraft positioning systems or tower displays.
- **Impact:** Misleading operational data, flight safety risk.

5. SQL Injection and Code Exploits

- **Definition:** Inserting malicious code into applications that interact with databases.
- **Example:** A web-based monitoring interface exploited to reveal system credentials or modify configurations.
- **Relevance:** Increasingly important as maintenance interfaces become web-enabled.
- **Prevention concept:** Input validation, regular patching, and software hardening.

6. Zero-Day Vulnerabilities

- **Definition:** Newly discovered security flaws that are exploited before developers issue a patch.
- **Example:** Attackers use an unpatched flaw in a Windows service to gain access to an engineering workstation.
- **Why critical:** ATSEP systems often run long-term configurations where updates are rare, creating long windows of exposure.

---

7. Supply Chain Attacks

- **Definition:** Compromise introduced through trusted software or hardware sources.
- **Example:** A third-party maintenance tool containing hidden malicious code that is installed across multiple radar sites.
- **Impact:** Hidden infiltration deep inside trusted systems, often hard to detect.
- **Lesson:** Even official updates must come through validated and verified channels.

---

8. Credential Theft and Session Hijacking

- **Definition:** Stealing authentication data (passwords, tokens, certificates) to impersonate users.
- **Example:** Capturing a session cookie to gain access to the ATC management interface.
- **Mechanism:** Phishing, malware, or network sniffing.
- **Impact:** Full access to control systems under a legitimate identity.

---

9. Data Exfiltration

- **Definition:** Unauthorized copying or transfer of data from a system.
- **Example:** System configuration files, operational plans, or maintenance logs extracted to an external site.
- **Relevance:** Even non-safety data can help attackers map your network.

---

10. Advanced Persistent Threats (APT)

- **Definition:** Long-term, stealthy campaigns by organized groups (often state-sponsored) targeting critical infrastructure.
- **Phases:**
    1. Initial access (phishing, exploit, or supply chain).
    2. Lateral movement through networks.
    3. Data exfiltration or disruption.
- **Example:** A coordinated attempt to monitor or manipulate surveillance systems without triggering alarms.
- **Example:** Over several months, a stealthy attacker infiltrates an ANSP's administrative network through a contractor's account, laterally moves to engineering servers, and silently monitors configuration uploads to identify system vulnerabilities.
- **Key feature:** Persistence — they hide and remain active for months or years.

---

11. Physical-Layer Cyber Threats

- **Definition:** Physical actions with cyber consequences.
- **Examples:**
    - Plugging an infected USB into a console.
    - Replacing hardware with compromised devices (e.g., router with modified firmware).
- **Relevance:** ATSEP often work directly on physical systems; security must include physical controls.

---

12. Emerging and Hybrid Threats

- **AI-Driven Attacks:** Automated phishing, intelligent password cracking, or adaptive intrusion tools.
- **ICS/SCADA-specific Attacks:** Target operational technology (e.g., radar controllers, ILS, VOR).
- **Quantum Threats (future):** Potential to break current encryption algorithms.

Sincerely,

Michel Gaulin
IFATSEA Regional Director of the Americas

www.ifatsea.org
www.ifatsea-aar.org