Contribution ID: **4** Type: **Poster**

Open-Source Multi-Domain CubeSat Architecture for Search and Rescue

CubeSats are increasingly used as low-cost communication relays, but their convergence with drones, trail-side environmental IoT sensors, and ground control stations creates new challenges in security, resilience, and interoperability. Search and Rescue (SAR) missions provide a compelling case where these systems must interoperate under constrained and adversarial conditions. Rapid intervention can mean the difference between life and death for victims. Yet, operations in mountainous regions or disaster-stricken zones face obstructed terrain, poor cellular coverage, and the limited reach of Visual Line of Sight (VLOS) drones.

This work proposes an open-source Beyond Visual Line of Sight (BVLOS) architecture. Trail-side IoT sensors detect motion, sound, and pressure, transmitting data via LoRa to guide drone waypoints. Drones execute autonomous SAR surveillance with AI-assisted human detection. Telemetry and commands are managed via lightweight MQTT-SN over SDR. CubeSats provide resilient LEO links between drones and ground control stations, which coordinate mission planning, telemetry aggregation, and victim rescue.

To evaluate the system's security posture, traditional frameworks such as MITRE ATT&CK, STRIDE, and SPARTA were considered. While effective for enterprise networks or isolated domains, they are limited in capturing complex interdependencies in modern space-enabled architectures. Applying them to this system would provide incomplete threat visibility and limited resilience analysis.

METEORSTORM™, an open-source framework developed by ethicallyHackingspace, was used for multi-domain threat modeling, offering comprehensive system decomposition and enabling exposure assessment, adversarial simulation, and resilience planning across the full CubeSat–Drone–IoT sensors–Ground Control Station chain.

Simulated attacks, including MQTT-SN injection, telemetry spoofing, and RF interference, revealed critical attack surfaces. Detection engineering, combining rule-based logic and machine learning, achieved strong anomaly detection despite resource constraints.

The system was implemented with open-source tools such as ArduPilot (SITL), Gazebo, MQTT-SN, GNU Radio, and Flask. It provides the CubeSat community a multi-domain architecture for resilient, interoperable systems, enabling life-saving missions in communication-limited regions.

Keywords: CubeSat, BVLOS, Trail-Side Environmental IoT, LoRa, MQTT-SN, SDR, Ground Control Stations, METEORSTORM, Multi-Domain Threat Modeling, Anomaly Detection, Open Source, SAR, Victim Detection, Secure Communications

Author: ADJEI, Ernest (Erasmus Mundus Masters Student in IoT Cybersecurity)

Presenter: ADJEI, Ernest (Erasmus Mundus Masters Student in IoT Cybersecurity)

Session Classification: Poster Tea Time