# Master Dashboards Template: Red List WiFi

**Training Board Purpose: WiFi Redlist DFP**

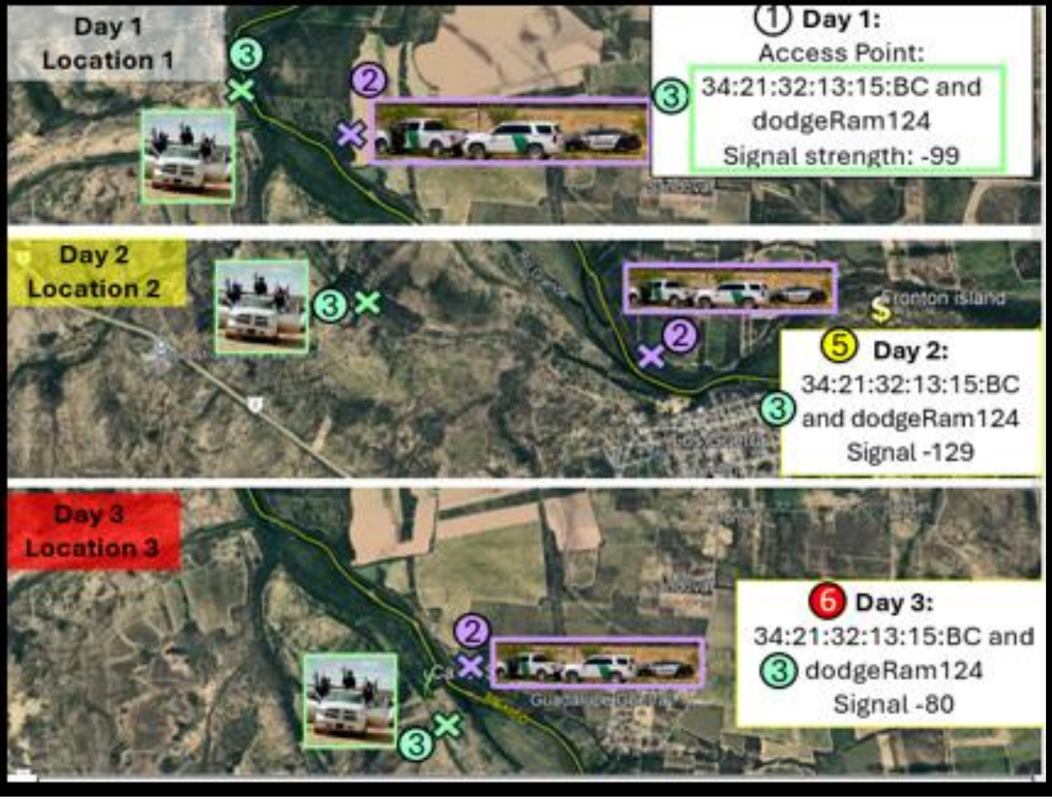
•**Network Survey Role** – Identifies WiFi access points (APs) in the Area of Interest (AOI) using:

- **BSSID** (Device MAC)
- **SSID** (WiFi Name)

•**Team Visualization** – Maps display team routes to monitor survey coverage and highlight APs of interest.

•**Data Exploration** – Visualizations and maps stream records from survey devices, with filters applied to:

- Focus on APs of interest
- Detect adversary movement
- Highlight anomalies in signal strength and AP activity



| Threat Detection | Operations and Planning |
|---|---|
| Identify WiFi/BT devices co-traveling | Identify areas with less secure encryption in access points |
| Identify SDRs, SBCs, SDKS  or other devices of interest | Monitor blue force digital footprint |
| Detect when Network Survey Device is near known AdTech WiFi or Bluetooth threat | |

SEME Tactical Mission Network

# Red List DFP Dashboard for Wardrive Analysis

## Wardrive: Survey Points of Interest Brief

**Actionable Intelligence:**

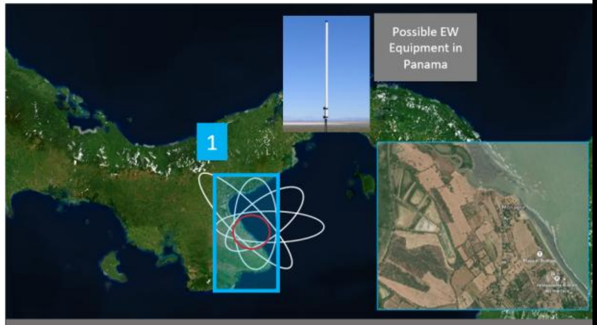
**Objective 1:** Suspected Enemy EW equipment has been identified using Hawkeye 360 data. The EW is potentially a rogue tower that identifies the cell global identity (MCC, MNC, LAC, CI that this device is broadcasting.

Located in AOI-1

**Objective 2:** Intel reports that 2 two rogue networks have been identified ssid: **"Hotel_Free_1244"** and **"Van9321"**. Identify any BSSIDs connected to those networks within the area.

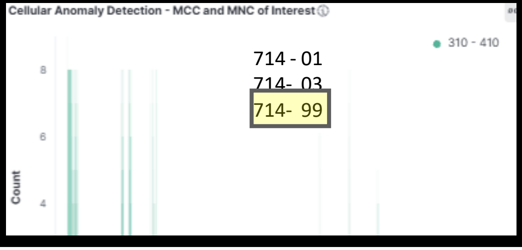
**Ground teams are tasked:**

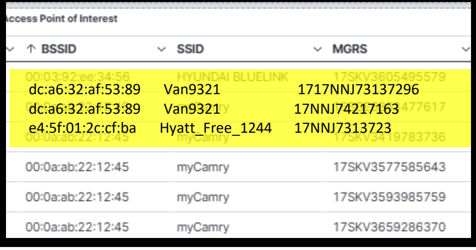
To wardrive with passive NS surveys of the area to identify: rogue tower & locate networks TOC "Hotel_Free_1244" or "Van9321" are sighted.



Ellipse Center Point Panama IVO: MGRS 17NNJ73437458

## Master Dashboard Template: WiFi DFP Redlist Device





Access Point of Interest

| BSSID | SSID | MGRS |
|---|---|---|
| dc:a6:32:af:53:89 | Van9321 | 1717NNJ73137296 |
| dc:a6:32:af:53:89 | Van9321 | 17NNJ74217163 |
| e4:5f:01:2c:cf:ba | Hyatt_Free_1244 | 17NNJ7313723 |
| 00:0a:ab:22:12:45 | myCamry | 17SKV3577585643 |
| 00:0a:ab:22:12:45 | myCamry | 17SKV3593985759 |
| 00:0a:ab:22:12:45 | myCamry | 17SKV3659286370 |

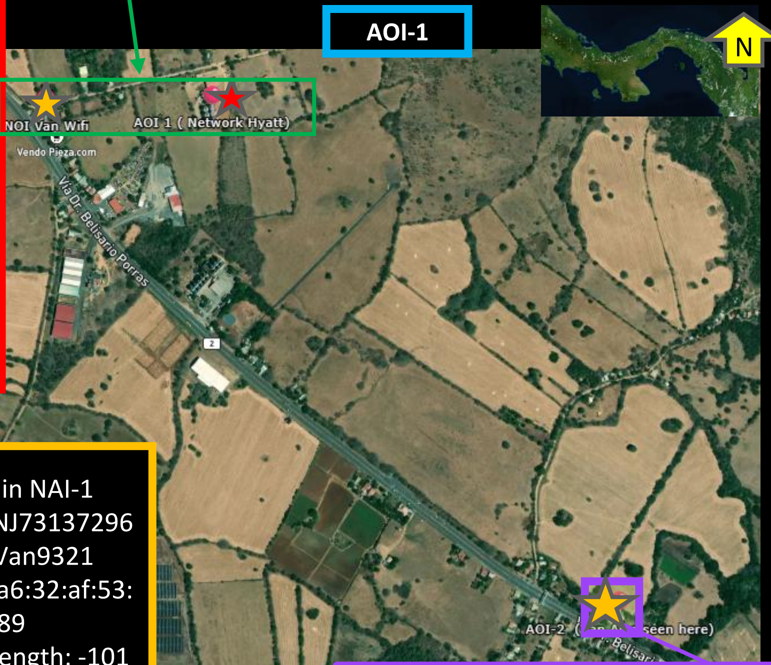
### Post Analysis- Named Area of Interest Development:

- Narrowed down area of interest to 2 named areas of interest where the wifi networks were surveyed as well as a cell tower that had not been seen before
- **NAI-1 located: IVO** 17NNJ7313723
  - ★ ssid: Hotel_Free_1244 bssid: e4:5f:01:2c:cf:ba OUI vendor:Raspberry Pi
  - ★ ssid:Van9321 bssid dc:a6:32:af:53:89 OUI vendor Raspberry Pi at street entrance.
- **NAI-2 located 17NNJ74217163**
  - ★ ssid : Van9321 bssid dc:a6:32:af:53:89is also seen in this location
- Surveyed Potential Rogue Tower within AOI-1 7 times
  - Cell global identity: MCC: 714 MNC: 99 LAC: 104 CI: 111111
  - Panama MCC is 714 Networks 1-4 and CGI was broadcasting MNC 99

**NAI-1:** 17NNJ7313723

**Potential Rogue Tower**
AOI-1: IVO: 17NNJ731372
Cell tower technology: GSM 2G
MCC: 714 MNC: 99 LAC: 104 CI: 111111
Signal Strength: Range -83 to -98

★NOI-1 in NAI 1: IVO: 17NNJ7313723
SSID: Hyatt_Free_1244
BSSID: e4:5f:01:2c:cf:ba
Signal Strength: -60 Encryption: Open



★ NOI-2 in NAI-1
IVO: 17NNJ73137296
SSID: Van9321
BSSID:dc:a6:32:af:53:89
Signal Strength: -101
Encryption: Open

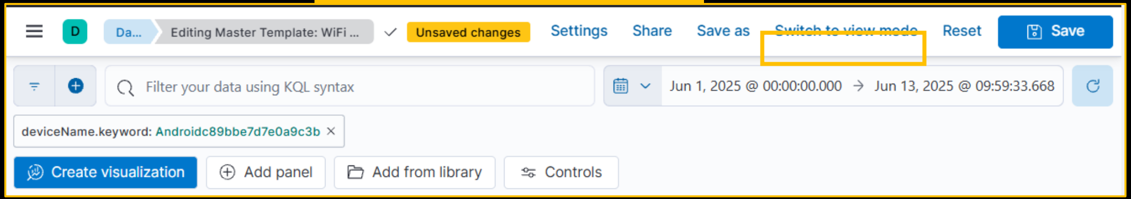
**NAI-2: 17NNJ74217163**

AOI-2 (Van Also seen here)
Via Dr. Belisario Porras
2

★ NOI-2 in NAI 2-
IVO: 17NNJ74217163
SSID: Van9321
BSSID:dc:a6:32:af:53:89
Signal Strength: -82
Encryption: Open

# Master Dashboards Template: WiFi Redlist DFP

Dashboard Functions



Filter your data using KQL syntax

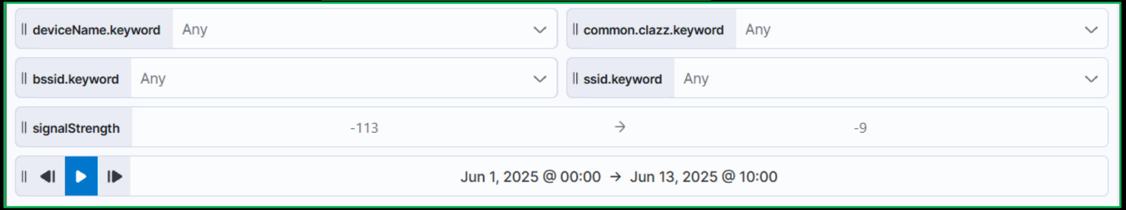
Jun 1, 2025 @ 00:00:00.000 → Jun 13, 2025 @ 09:59:33.668

deviceName.keyword: Androidc89bbe7d7e0a9c3b ×

## Dashboard Functions

- Starting point for filtering data in the Master Template
- Analysts can query by device, set time ranges, and begin shaping results
- Template can be cloned, shared, and modified for specific analysis

Controls



deviceName.keyword: Any

common.clazz.keyword: Any

bssid.keyword: Any

ssid.keyword: Any

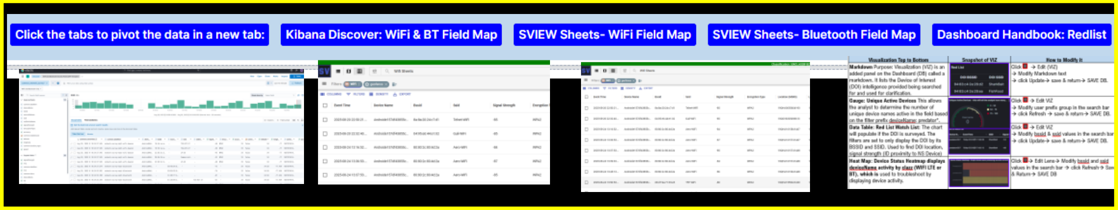
signalStrength: -113 → -9

Jun 1, 2025 @ 00:00 → Jun 13, 2025 @ 10:00

## Controls

- Interactive filters for refining results in the Master Template
- Narrow data by device name, BSSID/SSID, classification, & signal strength
- Filter for specific devices or access points for deeper analysis

Pivot Data

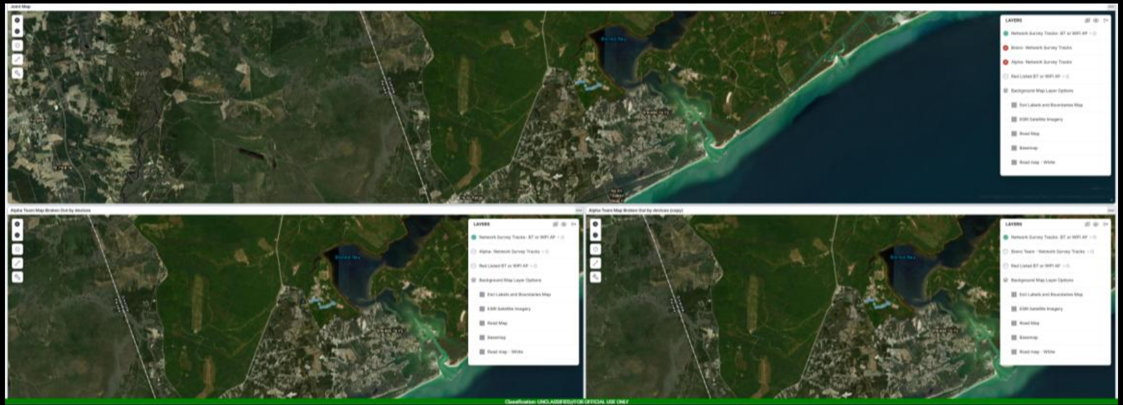


Click the tabs to pivot the data in a new tab:
Kibana Discover: WiFi & BT Field Map
SVIEW Sheets- WiFi Field Map
SVIEW Sheets- Bluetooth Field Map
Dashboard Handbook: Redlist

## Pivot Data

- Provides **pivot URLs** with predefined field maps in both **SVIEW** (WiFi & Bluetooth) and **Kibana** (Sheets View & Discover)
- Enables data exploration without rebuilding filters or re-selecting fields
- Includes a **Dashboard Handbook link** explaining how to modify visualizations and explain DFP purpose.

Maps

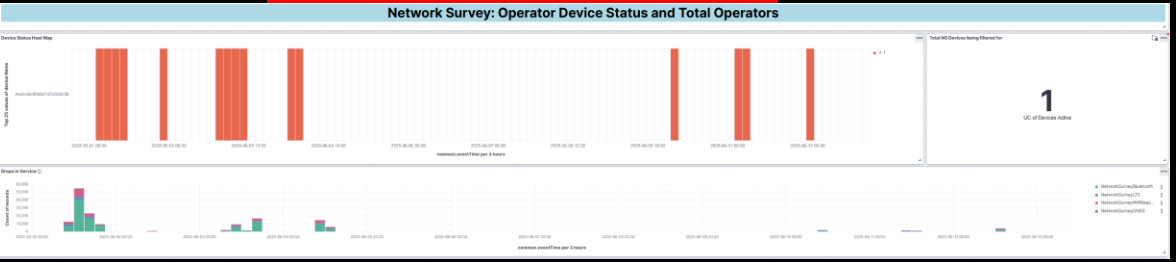


## Maps: Three included maps:

- **Map 1** – Full operations view: shows all teams surveying, collected access points, and highlights access points of interest
- **Map 2** & **3** – Alpha &Bravo team view: breaks out survey data by team for separate mission tracking, enabling TOC to run multiple missions simultaneously and track data by end user

# Master Dashboards Template: WiFi Redlist DFP

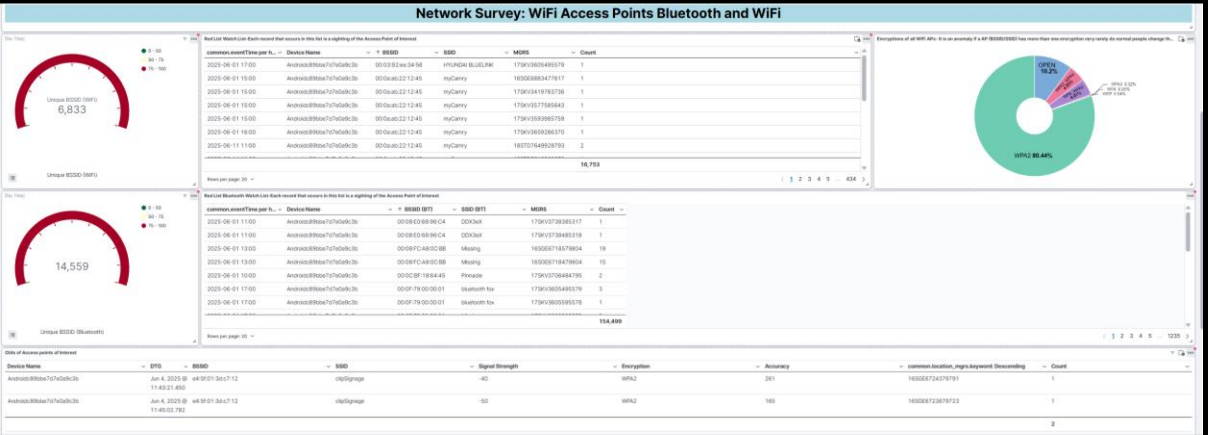
Device Status Graphs



Network Survey: Operator Device Status and Total Operators

Device Status Heat Map
Total NS Devices being Filtered for
1
UC of Devices Active
common.eventTime per 3 hours
Drops in Service

Access Points of Interest WiFi and Bluetooth



Network Survey: WiFi Access Points Bluetooth and WiFi

Red List Watch List-Each record that occurs in this list is a sighting of the Access Point of interest

| common.eventTime per h... | Device Name | BSSID | SSID | MGRS | Count |
|---|---|---|---|---|---|
| 2025-06-01 17:00 | Androidc89bbe7d7e0a9c3b | 00:03:92:ea:34:56 | HYUNDAI BLUELINK | 17SKV3605495579 | 1 |
| 2025-06-01 15:00 | Androidc89bbe7d7e0a9c3b | 00:0a:ab:22:12:45 | myCamry | 16SGE6883477617 | 1 |
| 2025-06-01 15:00 | Androidc89bbe7d7e0a9c3b | 00:0a:ab:22:12:45 | myCamry | 17SKV3419783736 | 1 |
| 2025-06-01 15:00 | Androidc89bbe7d7e0a9c3b | 00:0a:ab:22:12:45 | myCamry | 17SKV3577585643 | 1 |
| 2025-06-01 15:00 | Androidc89bbe7d7e0a9c3b | 00:0a:ab:22:12:45 | myCamry | 17SKV3593985758 | 1 |
| 2025-06-01 16:00 | Androidc89bbe7d7e0a9c3b | 00:0a:ab:22:12:45 | myCamry | 17SKV3659286370 | 1 |
| 2025-06-11 11:00 | Androidc89bbe7d7e0a9c3b | 00:0a:ab:22:12:45 | myCamry | 18STD7649928793 | 2 |
| | | | | | 16,753 |

Rows per page: 20   1 2 3 4 5 ... 434

Red List Bluetooth Watch List-Each record that occurs in this list is a sighting of the Access Point of interest

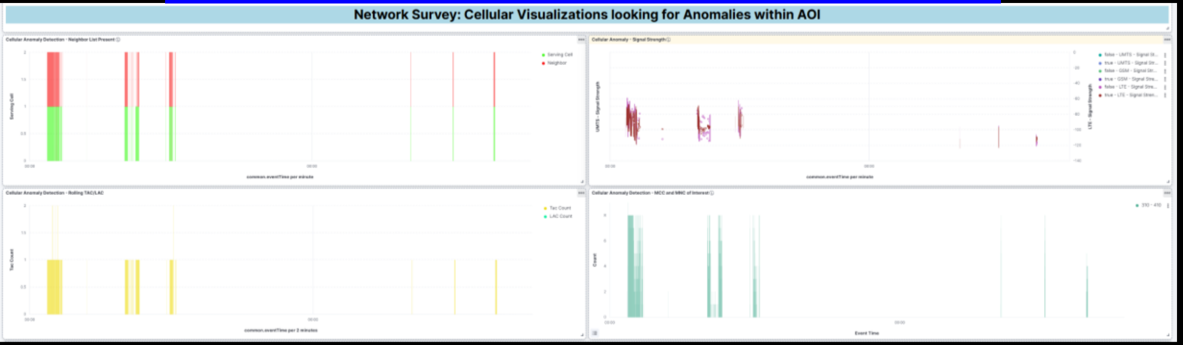
| common.eventTime per h... | Device Name | BSSID (BT) | SSID (BT) | MGRS | Count |
|---|---|---|---|---|---|
| 2025-06-01 11:00 | Androidc89bbe7d7e0a9c3b | 00:08:E0:68:96:C4 | DDX3eX | 17SKV3738385317 | 1 |
| 2025-06-01 11:00 | Androidc89bbe7d7e0a9c3b | 00:08:E0:68:96:C4 | DDX3eX | 17SKV3738485318 | 1 |
| 2025-06-01 13:00 | Androidc89bbe7d7e0a9c3b | 00:08:FC:A8:0C:BB | Missing | 16SGE6718579804 | 19 |
| 2025-06-01 13:00 | Androidc89bbe7d7e0a9c3b | 00:08:FC:A8:0C:BB | Missing | 16SGE6718479804 | 15 |
| 2025-06-01 10:00 | Androidc89bbe7d7e0a9c3b | 00:0C:BF:18:64:45 | Pinnacle | 17SKV3706484795 | 2 |
| 2025-06-01 17:00 | Androidc89bbe7d7e0a9c3b | 00:0F:79:00:00:01 | bluetooth fox | 17SKV3605495579 | 3 |
| 2025-06-01 17:00 | Androidc89bbe7d7e0a9c3b | 00:0F:79:00:00:01 | bluetooth fox | 17SKV3605595578 | 1 |
| | | | | | 154,499 |

Rows per page: 20   1 2 3 4 5 ... 1235

OUIs of Access points of Interest

| Device Name | DTG | BSSID | SSID | Signal Strength | Encryption | Accuracy | common.location_mgrs.keyword: Descending | Count |
|---|---|---|---|---|---|---|---|---|
| Androidc89bbe7d7e0a9c3b | Jun 4, 2025 @ 11:43:21.450 | e4:5f:01:3d:c7:12 | clipSignage | -40 | WPA2 | 261 | 16SGE6724379791 | 1 |
| Androidc89bbe7d7e0a9c3b | Jun 4, 2025 @ 11:45:02.782 | e4:5f:01:3d:c7:12 | clipSignage | -50 | WPA2 | 165 | 16SGE6723679723 | 1 |
| | | | | | | | | 2 |

Cellular Tower Measurements



Network Survey: Cellular Visualizations looking for Anomalies within AOI

Cellular Anomaly Detection - Neighbor List Present
Serving Cell
Neighbor
common.eventTime per minute
Cellular Anomaly - Signal Strength
Cellular Anomaly Detection - Rolling TAC/LAC
Tac Count
LAC Count
common.eventTime per 2 minutes
Cellular Anomaly Detection - MCC and MNC of Interest
Event Time

**Device Status Graphs- current end users- deviceNames activity**

- **Device Heat Map:** Displays criteria filtered end users in the dashboard, great tool for operations pre-check devices are operational.
- **Devices in AOI Metric Display** – Shows the total number of end users
- **Service Drop Detection Histogram**–IDs gaps in records or service that may indicate anomalies

**APs (Access Points) of Interest (WiFi & Bluetooth)**

- **Gauges** – Show the total number of **unique BSSIDs** detected along the survey route (both WiFi (BSSID MAC) and Bluetooth (sourceaddress).
- **Data Tables** – Break down each access point with:
  - DTG, Device Name, Signal Strength, Encryption Type & Location
- **OUI Filter Table** – Flags **manufacturers of interest** (e.g., Raspberry Pi, Rock Pi), which may indicate a DFP threat in certain AOIs

**Cellular Tower Measurements** – Used to ID anomalous cell tower activity

- **Neighbor List Histogram)** – Shows serving vs. neighbor cells; normally equal (red/green), anomalies if only red or green.
- **Signal Strength Line Chart** – Compares serving cell vs. neighbor cell; serving cell should usually be stronger.
- **Rolling TAC/LAC Chart** – Detects anomalies when rapidly changing
- **MCC/MNC Histogram** – Identifies country and carrier codes; only the expected MCC (country code) should appear.

SEME Tactical Mission Network