

The Nine Layers of Intelligence Framework

Version: 1.0

Author: PixelatedDwarf

Purpose: A comprehensive overview of the full intelligence spectrum for building a complete Battlespace Assessment.

Introduction

The previous guides focused on the **Core Triad**: SIGINT (Signals), OSINT (Open Source), and HUMINT (Human). These are the most accessible layers for immediate action. However, a true **Commander's View** requires understanding the full spectrum.

This document outlines all **Nine Layers of Intelligence**. You do not need to master all nine today. Use this as a reference guide to expand your analysis as your skills and resources grow. Each layer adds a new dimension to your Threat Map, transforming it from a flat list of cameras into a dynamic, 3D model of your environment.

Layer 1: SIGINT (Signal Intelligence)

Definition: The collection and analysis of electromagnetic emissions.

- **What it maps:** Wi-Fi networks, Bluetooth beacons, cellular towers, RFID tags, and proprietary sensor signals.
 - **Tools:** Kismet, Wireshark, SDR (RTL-SDR, HackRF).
 - **Key Insight:** Tells you *where* the digital eyes are looking and where the "dead air" zones are.
 - **Status: Mastered** in the War-Walk guide.
-

Layer 2: OSINT (Open Source Intelligence)

Definition: Information collected from publicly available sources.

- **What it maps:** Municipal contracts, camera registries, news reports, social media posts, and public records.
 - **Tools:** Google Dorks, FOIA requests, public databases, news archives.
 - **Key Insight:** Reveals the "Silent Nodes"—hardwired cameras and infrastructure that do not broadcast signals.
 - **Status: Mastered** in the OSINT Deep Dive guide.
-

Layer 3: HUMINT (Human Intelligence)

Definition: Information gathered from human sources through interaction.

- **What it maps:** Intent, monitoring habits, community trust, and "ground truth" about camera angles and maintenance.
 - **Tools:** Conversations with neighbors, local business owners, and first responders.
 - **Key Insight:** Answers *who* controls the data and *how* it is used. Turns neighbors from passive subjects into potential allies.
 - **Status: Mastered** in the HUMINT section.
-

Layer 4: GEOINT (Geospatial Intelligence)

Definition: The analysis of terrain, elevation, and physical geography to determine visibility and movement.

- **What it maps:** Sight lines, elevation changes, building heights, vegetation density, and "viewsheds" (what a camera can actually see).
 - **Tools:** Google Earth Pro, QGIS, OpenStreetMap with elevation data, "Viewshed Analysis" tools.
 - **Key Insight:** A camera on a pole might be listed in OSINT, but GEOINT tells you if a hill or a tree blocks its view of the sidewalk. It defines the **physical blind spots**.
 - **Action:** Import your camera locations into Google Earth Pro. Use the "Ruler" tool to measure distances. Use the "Sunlight" tool to see how shadows affect camera coverage at different times of day.
-

Layer 5: IMINT (Imagery Intelligence)

Definition: Analysis of photographs and satellite/aerial imagery.

- **What it maps:** Physical camera mounts, lens types, pole heights, and recent construction changes.
 - **Tools:** Google Earth Historical Imagery, Bing Maps, Maxar, Drone footage (if legal).
 - **Key Insight:** Allows you to spot a new camera mount that hasn't been activated yet. Historical imagery can show when a camera was installed, helping you track the expansion of the grid.
 - **Action:** Compare current satellite images with images from 6 months ago. Look for new poles, new wiring, or new camera housings on rooftops.
-

Layer 6: MASINT (Measurement and Signature Intelligence)

Definition: Detection of non-traditional signatures (acoustic, seismic, thermal, chemical).

- **What it maps:** Acoustic gunshot detectors (ShotSpotter), seismic sensors on bridges, thermal imaging cameras, and air quality monitors.
- **Tools:** Specialized SDRs, acoustic spectrum analyzers, thermal cameras.
- **Key Insight:** These are the "invisible tripwires." They don't record video, but they trigger alerts when specific signatures (like a gunshot or a specific vibration) are detected.
- **Action:** If you suspect ShotSpotter coverage, listen for the distinct "ping" of the sensors or check city contracts for "acoustic monitoring."

Layer 7: Infrastructure Intelligence

Definition: Analysis of the physical backbone that supports the surveillance network.

- **What it maps:** Power grids, fiber optic routes, cell tower locations, water/sewer lines, and backup generators.
 - **Tools:** Utility maps, FCC databases, power outage maps, engineering permits.
 - **Key Insight:** Tells you the **resilience** of the grid. A camera on solar power has downtime at night. A camera on a fiber line is always on. Knowing where the power substations are helps you predict where the grid is strongest or most vulnerable.
 - **Action:** Map the location of cell towers and fiber junction boxes. These are the "nodes" that keep the cameras online.
-

Layer 8: Temporal Intelligence

Definition: The analysis of time-based patterns and schedules.

- **What it maps:** When cameras are monitored live vs. recorded, when data batches upload, shift changes at police stations, and peak traffic times.
 - **Tools:** City work schedules, traffic pattern data, news reports on "live monitoring" hours.
 - **Key Insight:** A camera that records but is only reviewed the next morning is far less dangerous than one watched in real-time. Knowing the "watch schedule" allows you to time your movements.
 - **Action:** Observe when security guards change shifts. Note when traffic cameras seem to "go dark" (often during maintenance windows).
-

Layer 9: Legal Intelligence

Definition: Understanding the laws, regulations, and policies governing surveillance.

- **What it maps:** Local ordinances, data retention policies, privacy laws, and oversight committees.
 - **Tools:** City codes, state statutes, ACLU reports, legal databases.
 - **Key Insight:** Defines the **rules of engagement**. What are the cameras legally allowed to do? How long is data kept? Who can access it? This layer tells you your rights and the limits of the system.
 - **Action:** Read your city's "Surveillance Ordinance." If one doesn't exist, that is a critical finding (no limits).
-

Integrating the Layers: The Common Operating Picture

The power of this framework is not in the individual layers, but in their **synthesis**.

- **SIGINT + GEOINT:** You know a camera is there (SIGINT), and you know exactly what it can see based on the terrain (GEOINT).
- **OSINT + Temporal:** You know a camera exists (OSINT), and you know it is only monitored live from 9 AM to 5 PM (Temporal).
- **HUMINT + Legal:** You know a neighbor has a camera (HUMINT), and you know the local law prohibits pointing it at public sidewalks (Legal).

Your Path Forward

1. **Start with the Core Triad** (Layers 1-3). This gives you 80% of the actionable data.
2. **Add GEOINT and IMINT** (Layers 4-5) to refine your map with physical reality.
3. **Expand to Infrastructure and Temporal** (Layers 7-8) to understand the system's behavior.
4. **Use MASINT and Legal** (Layers 6 & 9) for high-level strategic analysis.

Conclusion The Nine Layers Framework is your roadmap to total situational awareness. You do not need to climb every mountain today. But knowing the mountains exist allows you to plan your ascent.