

Geo-Intelligence & Network-Centric Warfare

The convergence of geospatial intelligence, AI, cyber systems, satellites, and autonomous platforms is reshaping national power. Modern conflicts now span communication networks, data systems, satellites, financial systems, and civilian infrastructure — far beyond physical battlefields.

STRATEGIC OVERVIEW

Vipin Tyagi

Track 2.2: Data Sovereignty & Strategic Autonomy,



The New Warfare Ecosystem

Modern conflict is defined by a set of interconnected doctrines and technologies that blur the boundaries between physical and digital domains.

Network-Centric Warfare

The network becomes the weapon system — resilient comms and real-time awareness drive military effectiveness.

Multi-Domain Operations

Simultaneous action across land, sea, air, space, cyber, and information domains.

Cognitive & Hybrid Warfare

Targeting perception, decision-making, and social ecosystems alongside physical infrastructure.

AI-Enabled Battlespace

AI fuses satellite imagery, telecom metadata, sensor networks, cyber intelligence, and behavioral analytics.



Key Technologies of the New Warfare Ecosystem

GEOINT

Satellite imaging, radar mapping, thermal sensing, terrain analytics, maritime tracking, and location intelligence.

AI Decision Systems

Threat prediction, autonomous target recognition, swarm drone coordination, misinformation detection, and predictive logistics.

Civilian Infrastructure

Telecom networks, power grids, payment systems, GPS/GNSS, ports, and AI cloud infrastructure are now contested domains.

How Geo-Intelligence Actually Works

"How to reliably convert photons, radio reflections, thermal signatures, and movement patterns into actionable truth."

Modern geo-intelligence systems do not "see" like humans — they **infer**. What appears to be precise identification of tanks, ships, or troop movement is the result of layered probabilistic processing across sensors, AI models, metadata fusion, and contextual reasoning.



Each stage introduces uncertainty. The final output is a confidence estimate, not a certainty — making human judgment and verification essential at every level.

Why Misinterpretation Happens — and How to Mitigate It

Sources of Error

- Resolution illusions
- Contextual bias
- Adversarial camouflage & deception
- Sensor fusion conflicts
- Deepfake geospatial intelligence
- Algorithmic overconfidence

Reliability Techniques

- Multi-Source Verification
- Red Team Analysis
- Explainable AI (XAI)
- Human-in-the-Loop Systems
- Physics-Based Constraints

⚠ Geo-intelligence is not truth extraction — it is **uncertainty management under incomplete information.**



Multi-Modal Sensing & Object Detection

Sensor Modalities

- Optical (visible imagery)
- Infrared / Thermal
- SAR (Synthetic Aperture Radar)
- Hyperspectral
- LiDAR
- RF sensing & SIGINT fusion

AI Detection Architectures

Deep neural systems power object recognition using:

- CNNs & Vision Transformers
- Multi-scale feature pyramids
- Semantic & instance segmentation
- Graph-based scene understanding

Geo-registration anchors every pixel to precise Earth coordinates using GPS, inertial systems, star trackers, and terrain correction.

HAPS: Airborne Trust Infrastructure

High Altitude Platform Systems (HAPS) occupy the critical altitude gap between drones, aircraft, and satellites — typically **20–50 km** — providing persistent line-of-sight, lower latency than satellites, and broader coverage than terrestrial towers.

Defensive Surveillance


Verify missile launches, troop movement, electronic emissions, GNSS anomalies, and drone swarms as persistent airborne trust nodes.

Distributed Resilience

Airborne mesh networking, communication rerouting, alternate command links, and adaptive beam steering replace centralized vulnerable systems.

Cyber & Anti-Spoofing

Neural-network-based hijacking detection, anti-jamming response, spoofing immunity, and navigation control transfer during attack scenarios.

 Persistent sensing + AI inference risks automated threat perception, rapid autonomous response, and algorithmic conflict escalation.

HAPS Strategic Shift: Protecting Decision Authenticity

Defense increasingly means protecting **data integrity, network continuity, timing synchronization, geospatial truth, and decision authenticity** — not just physical territory. HAPS may ultimately become the backbone of sovereign airborne trust infrastructure.

Decoy & Redundancy

Distributed HAPS architectures provide fallback nodes that absorb and diffuse attacks on centralized systems.

Communications Continuity

HAPS maintain command links and civilian broadband during terrestrial or satellite disruption.

Strategic Situational Awareness

Persistent coverage enables real-time monitoring of electronic emissions, spoofing events, and kinetic activity.



ITU Frequency Allocations for HAPS

The ITU has progressively identified frequency bands for HAPS through World Radiocommunication Conferences (WRC-97 through WRC-19), enabling integrated terrestrial–airborne–space networking.

Key Frequency Bands

Band	Frequency	Primary Use
Core HAPS	47.2–48.2 GHz	High-capacity backhaul & gateway
WRC-19	31–31.3 GHz	Broadband feeder links
WRC-19	38–39.5 GHz	Dense airborne networking
IMT-HAPS	1885–2170 MHz	Airborne cellular base stations
Gateway	6440–6640 MHz	Core network connectivity
Americas	21.4–27.5 GHz	Regional directional links

Architecture Flow

User Devices – IMT Bands (~2 GHz)

↓ HAPS Platform ↓

Backhaul / Feeder Links (31 / 38 / 47 GHz)

↓ Core Network / Satellite / Fiber

This layered architecture supports civilian broadband, emergency resilience, military networking, persistent surveillance, and sovereign communication continuity.

Strategic Takeaways

The Network IS the Weapon

Military and national power now depend on data integrity, low-latency communications, and distributed command — not just kinetic force.

Intelligence is Probabilistic

Geo-intelligence is uncertainty management. Catastrophic misinterpretation remains possible without human-in-the-loop verification and explainable AI.

HAPS as Sovereign Infrastructure

HAPS are evolving from surveillance tools into airborne trust infrastructure — protecting timing, geospatial truth, and decision authenticity.

Spectrum is Strategic

ITU HAPS allocations signal a global transition toward integrated terrestrial–airborne–space networking for both civilian and military resilience.

