Intel Collection Simulator

Multi-INT Physics-Based Intelligence Cycle Simulation with Adversary Modeling and Bayesian Fusion

STS Gym Research

Document Version: 1.0

Date: April 30, 2026

Project: intel-collection-sim

Repository: idm.wezzel.com/crab-meat-repos/intel-collection-sim

Classification: UNCLASSIFIED

SIGINT HUMINT MASINT IMINT OSINT FININT Intelligence Cycle Bayesian Fusion Adversary Modeling Covert Action

Abstract

We present **intel-collection-sim**, a comprehensive, physics-based simulation platform for the full intelligence cycle spanning six intelligence disciplines (SIGINT, HUMINT, IMINT, MASINT, OSINT, and FININT). The simulator implements over 90 physics validation tests across 551 total tests, grounded in established international standards including ITU-R P.525 (free-space path loss), ITU-R P.676 (atmospheric absorption), ITU-R P.838 (rain fade), CTBT IMS seismic discrimination, and FATF financial intelligence frameworks. The system models the complete intelligence cycle from planning through collection, processing, analysis, dissemination, and feedback, with dynamic adversary reactions including denial and deception,

counterintelligence operations, and source degradation. A Bayesian evidence integration engine provides multi-INT fusion with cross-discipline corroboration tracking. The collection management hierarchy (SEF → ON → SIR → RFI) is paired with game-theoretic asset tasking to optimize collection against adaptive adversaries. Six built-in scenarios demonstrate the system's capability to simulate complex intelligence operations including nuclear monitoring, signals intelligence sweeps, and financial crime investigation. The 13-package architecture (12 discipline packages plus a cycle engine) provides cross-simulation integration hooks for the FORGE-SIMS constellation, enabling multi-domain operations research at scale.

Table of Contents

1. Introduction

The intelligence community faces a fundamental challenge in training analysts and testing collection strategies: real-world intelligence operations are inherently adversarial, classified, and resistant to controlled experimentation. Wargames and table-top exercises provide limited fidelity, while live collection exercises are expensive, operationally constrained, and impossible to repeat under controlled conditions.

Intel-collection-sim addresses this gap by providing a comprehensive, physics-grounded simulation of the complete intelligence cycle across six disciplines. Unlike simplified analytical models, the simulator implements the actual physical processes governing each collection modality—from the Friis transmission equation governing SIGINT receiver

sensitivity to the MICE framework governing HUMINT source recruitment—ensuring that collection outcomes emerge from authentic physical and behavioral dynamics rather than prescribed results.

The system is designed around three core principles:

- **Physics fidelity:** Every collection discipline is grounded in established physical models validated against international standards (ITU-R, CTBT, FATF). Signal propagation follows ITU-R recommendations; seismic discrimination follows CTBT monitoring protocols; financial detection follows FATF red flags.
- **Adversary awareness:** The intelligence collection process is inherently adversarial. The simulator models adversary denial and deception, counterintelligence operations, source compromise, and adaptive OPSEC responses, ensuring that collection strategies must account for an intelligent opponent rather than a static target.
- **Cycle completeness:** The simulator covers the full intelligence cycle—planning, collection, processing, analysis, dissemination, and feedback—rather than merely modeling individual collection events. This enables end-to-end studies of how collection planning decisions propagate through the analytic process.

1.1 Key Metrics

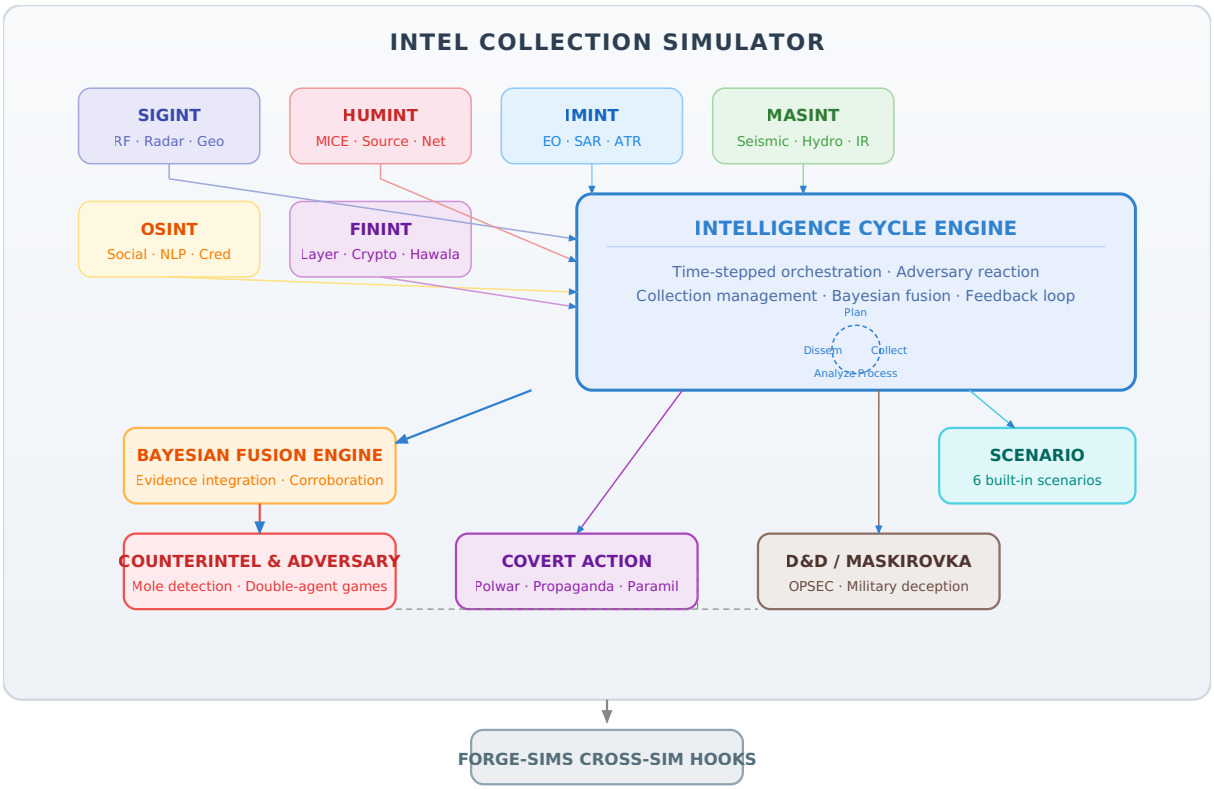
Metric	Value
Repository Size	20 MB
Commits	16
Total Tests	551
Physics Validation Tests	90+
INT Disciplines	6 (SIGINT, HUMINT, IMINT, MASINT, OSINT, FININT)
Packages	13 (12 discipline + 1 cycle engine)
Built-in Scenarios	6
Intelligence Cycle Phases	

	6 (Planning → Collection → Processing → Analysis → Dissemination → Feedback)
Collection Management Hierarchy	SEF → ON → SIR → RFI

2. System Architecture

2.1 Overview and Design Philosophy

The architecture follows a discipline-modular design: each INT discipline is encapsulated in its own package with well-defined interfaces for cross-discipline fusion. A separate cycle engine orchestrates the time-stepped simulation, manages adversary reactions, and coordinates the intelligence cycle phases.



2.2 Package Structure

The 13-package architecture separates concerns along two axes: discipline specificity and cycle phase. Each discipline package contains its own physics models, collection state,

processing algorithms, and analytic outputs. The cycle engine package provides the temporal orchestration, adversary modeling, and fusion infrastructure.

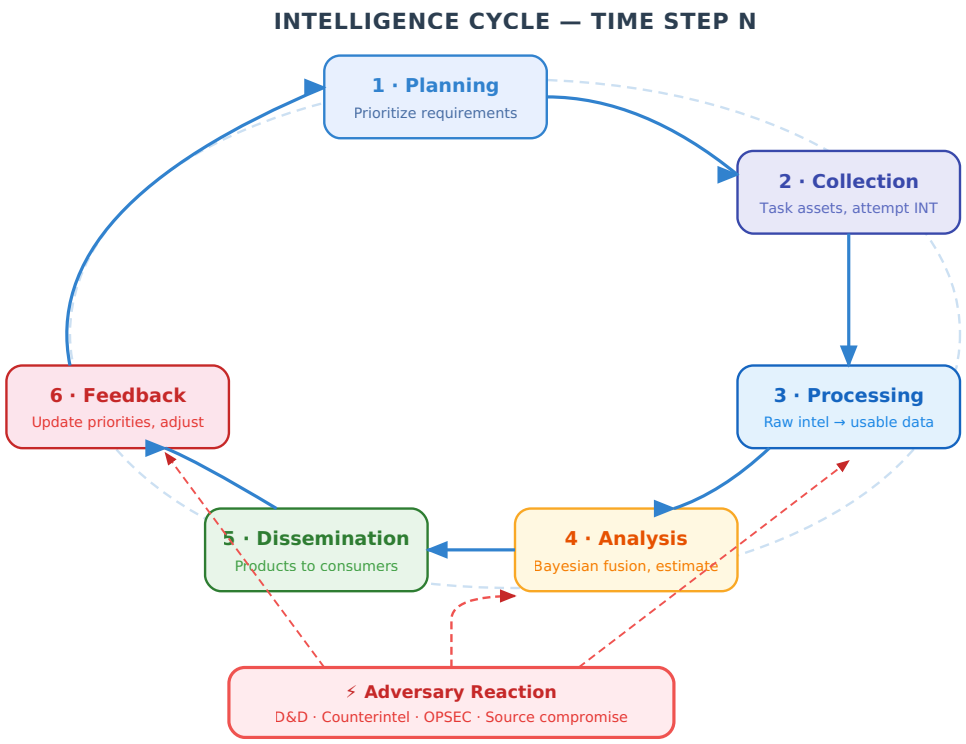
Package	Discipline/Role	Key Contents
`sigint`	SIGINT	RF propagation, radar, geolocation, frequency hopper tracking
`humint`	HUMINT	MICE recruitment, source reliability, network analysis
`imint`	IMINT	EO/IR/SAR sensors, orbital revisit, ATR, change detection
`masint`	MASINT	Nuclear seismic, hydroacoustic, ACINT, RADINT, CBINT
`osint`	OSINT	Social media modeling, NLP extraction, credibility scoring
`finint`	FININT	Layering detection, crypto tracing, hawala, sanctions evasion
`cycle`	Cycle Engine	Time-stepped orchestration, adversary reaction, feedback
`fusion`	Bayesian Fusion	Evidence integration, corroboration tracking, confidence
`collection`	Collection Mgmt	SEF/ON/SIR/RFI hierarchy, game-theoretic tasking
`counterintel`	Counterintelligence	Mole detection, double-agent games, compromise cascades
`covert`	Covert Action	Political warfare, propaganda, paramilitary, front companies
`deception`	Denial & Deception	

		OPSEC, maskirovka, military deception, counter-collection
`scenarios`	Scenario Engine	6 built-in scenarios, dynamic adversary reaction hooks

2.3 Intelligence Cycle Engine

The cycle engine drives the simulation through the six phases of the intelligence cycle at configurable time steps. Each time step may trigger:

1. **Planning:** Collection requirements are prioritized based on existing intelligence gaps, national intelligence priorities, and feedback from prior cycles.
2. **Collection:** Assets are tasked via the collection management hierarchy; discipline-specific collection events fire according to asset availability and physics constraints.
3. **Processing:** Raw collection data is processed through discipline-specific pipelines (signal demodulation, image exploitation, financial transaction analysis, etc.).
4. **Analysis:** Processed data enters the Bayesian fusion engine; analysts update estimates; corroboration is checked across INT disciplines.
5. **Dissemination:** Intelligence products are generated and distributed according to classification and need-to-know constraints.
6. **Feedback:** Consumer feedback updates collection priorities; source reliability is adjusted; adversary reactions are computed for the next cycle.



3. SIGINT: Signals Intelligence

The SIGINT package models the electromagnetic collection domain, implementing RF signal propagation physics, radar systems, emitter geolocation, and communications intelligence. All propagation models conform to ITU-R recommendations, ensuring physical accuracy for collection probability estimation.

3.1 RF Propagation Physics

Free-Space Path Loss (ITU-R P.525)

The fundamental propagation model computes free-space path loss (FSPL) per ITU-R P. 525-3:

$$ \text{FSPL}(\text{dB}) = 20 \log_{10}(d) + 20 \log_{10}(f) + 20 \log_{10}\!\left(\frac{4\pi}{c} \right) $$

where d is the link distance in meters, f is frequency in Hz, and c is the speed of light. This baseline is then augmented with atmospheric and precipitation effects.

Atmospheric Absorption (ITU-R P.676)

Above 10 GHz, atmospheric attenuation becomes significant. The model implements ITU-R P.676-13 specific attenuation, accounting for both oxygen and water vapor absorption lines:

$$ A_{\text{atm}} = \gamma_o(f) \cdot r_o + \gamma_w(f) \cdot r_w \quad (\text{dB}) $$

where γ_o and γ_w are the specific attenuations due to dry air and water vapor (dB/km), and r are the equivalent path lengths through each medium. The 22.235 GHz water vapor line and 60 GHz oxygen complex are modeled with line-by-line computation.

Rain Fade (ITU-R P.838)

Precipitation attenuation follows ITU-R P.838-4, with rain rate R (mm/h) mapped to specific attenuation:

$$ \gamma_R = k \cdot R^{\alpha} \quad (\text{dB/km}) $$

The coefficients k and α are frequency- and polarization-dependent, given by the regression fits in Recommendation P.838. The effective rain path length accounts for the 0°C isotherm height and rain height per ITU-R P.839.

Received Signal Model

The complete link budget for a SIGINT collection platform at range R from an emitter of power P_t at frequency f:

$$ P_r = P_t + G_t + G_r - \text{FSPL}(f, R) - A_{\text{atm}}(f, R) - A_{\text{rain}}(f, R, R_{\text{rate}}) - L_{\text{misc}} \quad (\text{dB}) $$

Collection occurs when P_r exceeds the receiver sensitivity threshold. The probability of intercept is further modulated by the emitter's duty cycle, antenna scan pattern, and any applied emission control (EMCON) posture.

3.2 Radar Systems

Radar Range Equation

The radar detection model implements the standard radar range equation with Swerling target fluctuation:

$$ R_{\max} = \left[\frac{P_t \cdot G_t^2 \cdot \lambda^2 \cdot \sigma}{(4\pi)^3 \cdot k \cdot T_0 \cdot B \cdot F \cdot (\text{SNR})_{\min}} \right]^{1/4} $$

where σ is the target radar cross-section, B is the receiver bandwidth, F is the noise figure, and $(\text{SNR})_{\min}$ is the minimum detectable signal-to-noise ratio for the given detection probability and false alarm rate.

Swerling Target Models

Five Swerling cases model target RCS fluctuation statistics:

Case	PDF	Correlation	Target Type
0 (Non-fluctuating)	Constant σ	N/A	Calibration sphere
1	Exponential	Scan-to-scan	Many small scatterers
2	Exponential	Pulse-to-pulse	Case 1 at high PRF
3	4th-order chi-squared	Scan-to-scan	Dominant + small scatterers
4	4th-order chi-squared	Pulse-to-pulse	Case 3 at high PRF

Each case modifies the detection probability computation via the appropriate cumulative distribution, affecting the achievable collection range for radar-target pairs.

3.3 Geolocation

The geolocation subsystem implements three primary emitter location techniques:

Time Difference of Arrival (TDOA)

Measures the differential time of arrival of an emitter's signal at multiple receivers. For N receivers, the time difference between receivers i and j defines a hyperboloid:

$$ \Delta t_{ij} = \frac{|\mathbf{r}_i - \mathbf{r}_e| - |\mathbf{r}_j - \mathbf{r}_e|}{c} $$

The intersection of $N-1$ hyperboloids yields the emitter position. The Cramér-Rao lower bound on TDOA localization accuracy is:

$$ \sigma_{\text{pos}} \geq c \cdot \sigma_t \cdot \text{GDOP}^{1/2} $$

where GDOP (geometric dilution of precision) depends on the receiver-emitter geometry.

Frequency Difference of Arrival (FDOA)

Exploits the differential Doppler shift observed by moving receivers. For a receiver moving with velocity $\mathbf{v}_i$:

$$ f_{D,i} = \frac{f_c}{c} \cdot (\mathbf{v}_i \cdot \hat{\mathbf{u}}_i) $$

FDOA is typically combined with TDOA for improved localization, particularly for moving emitters or when receiver motion provides Doppler diversity.

Angle of Arrival (AOA)

Direction-finding receivers measure the bearing to the emitter. Multiple AOA measurements intersect at the emitter location. The bearing accuracy depends on the antenna baseline and SNR:

$$ \sigma_\theta \approx \frac{\lambda}{B \cdot \sqrt{2 \cdot \text{SNR}}} $$

where B is the interferometer baseline length.

3.4 Frequency Hopper Tracking

Frequency-hopping spread spectrum (FHSS) emitters present a particular challenge to SIGINT collection. The tracker models:

- **Hop rate:** Number of frequency transitions per second (slow: <100 hops/s; fast: ≥100 hops/s)
- **Hop set:** The set of N frequencies available to the hopper, typically a subset of a larger band
- **Dwell time:** Time spent on each frequency before hopping
- **Hop sequence:** Pseudorandom or deterministic pattern governing frequency selection

The intercept probability for a scanning receiver with bandwidth B_r, scan rate R_s, and hopper dwell time T_d is:

$$ P_{\text{intercept}} = \frac{B_r}{B_{\text{total}}} \cdot \frac{T_d}{T_{\text{scan}}} \cdot P_{\text{detect}|\text{tune}} $$

Wideband receivers and digital channelized approaches significantly increase this probability by monitoring multiple hop channels simultaneously.

4. HUMINT: Human Intelligence

The HUMINT package models the human dimension of intelligence collection: source recruitment, handling, reliability assessment, and network analysis. The models are grounded in CIA doctrinal frameworks and reflect the inherently probabilistic nature of human-source intelligence.

4.1 MICE Recruitment Model

Source recruitment follows the MICE framework, the standard CIA motivational taxonomy for understanding why individuals provide intelligence:

Motivation	Description	Recruitment Strategy
Money	Financial need or greed	Direct payment, expense coverage, lifestyle improvement

Ideology	Belief in the cause or resentment of own government	Appeal to principles, shared values, moral framing
Compromise	Vulnerability to coercion (blackmail, legal exposure)	Leverage compromising information, legal jeopardy
Ego	Desire for recognition, importance, or control	Flattery, access, sense of significance

Each potential source has a vector of susceptibilities across the four motivations, which evolve over time based on life events, handling quality, and adversary counterintelligence pressure. The recruitment probability is:

$$ P_{\text{recruit}} = 1 - \prod_{i \in \text{MICE}} (1 - s_i \cdot a_i) $$

where s_i is the source's susceptibility to motivation i and a_i is the case officer's approach effectiveness for motivation i.

4.2 Source Reliability and Aging

ABCDEF Reliability Decay Model

Source reliability is tracked along two axes using the standard intelligence community grading scale:

- **Source Reliability (A–F):** From confirmed (A) to unreliable (F)
- **Information Credibility (1–6):** From confirmed (1) to cannot be judged (6)

Reliability decays over time according to a model that accounts for source aging, handling stress, and exposure risk:

$$ R(t) = R_0 \cdot e^{-\lambda t} \cdot \bigl(1 - P_{\text{compromise}}(t)\bigr) \cdot \bigl(1 - P_{D\&D}(t)\bigr) $$

where λ is the base degradation rate, $P_{\text{compromise}}$ is the cumulative probability of source compromise, and $P_{D\&D}$ is the probability the source has been turned (knowingly providing disinformation).

Compromise Probability

The compromise model accounts for multiple risk factors:

$$ P_{\text{compromise}}(t) = 1 - \exp\!\left(-\int_0^t \bigl[\lambda_{\text{opsec}} + \lambda_{\text{surv}} + \lambda_{\text{counter}} + \lambda_{\text{assoc}}\bigr] dt\right) $$

where the hazard rates represent: OPSEC failures by the source (λ_{opsec}), adversary surveillance detection (λ_{surv}), active counterintelligence investigation (λ_{counter}), and guilt-by-association exposure (λ_{assoc}).

4.3 Network Analysis

The HUMINT network analysis subsystem models the social graph of sources and their relationships, enabling:

- **Betweenness centrality:** Identifying sources that serve as critical information conduits
- **Cluster detection:** Identifying closely-connected groups that may share vulnerabilities
- **Compromise cascade modeling:** When one source is compromised, graph proximity determines the probability that linked sources are also identified
- **Access path analysis:** Finding the minimum-risk path from case officer to target information via intermediate sources

The compromise cascade probability for source j given compromise of source i at graph distance d_{ij}:

$$ P_{\text{cascade}}(j|i) = P_{\text{base}} \cdot e^{-\alpha \cdot d_{ij}} $$

where α controls how rapidly cascade risk decays with graph distance. Close associates (distance 1) face the highest risk; the cascade attenuates with each degree of separation.

5. IMINT: Imagery Intelligence

The IMINT package models space-based and airborne imagery collection, implementing sensor physics, orbital mechanics for revisit modeling, and automated image exploitation algorithms.

5.1 Sensor Physics

Electro-Optical (EO) and Infrared (IR) Sensors

The ground sample distance (GSD) for a pushbroom imager at orbital altitude h with focal length f and detector pitch p:

$$ \text{GSD} = \frac{p \cdot h}{f} $$

National Imagery Interpretability Rating Scale (NIIRS) is estimated from GSD and modulation transfer function (MTF) using the General Image Quality Equation (GIQE):

$$ \text{NIIRS} = C_0 + C_1 \cdot \log_{10}(\text{GSD}_G) + C_2 \cdot (1 - \text{SNR}_{\text{norm}})^{1/2} + \cdots $$

where the coefficients depend on the sensor type (EO panchromatic, IR, or multispectral). NIIRS levels range from 0 (uninterpretable) to 9 (the highest resolution), with tactically significant thresholds at NIIRS 4 (detect vehicles), 6 (identify vehicle type), and 7 (identify vehicle model).

Synthetic Aperture Radar (SAR)

SAR resolution is determined by bandwidth (range) and synthetic aperture length (azimuth), independent of range:

$$ \delta_r = \frac{c}{2B} \qquad \delta_a = \frac{\lambda \cdot R}{2 L_{\text{sa}}} $$

SAR operates in multiple modes: stripmap (moderate resolution, wide swath), spotlight (high resolution, narrow swath), and ScanSAR (coarse resolution, ultra-wide swath), with collection trade-offs modeled accordingly.

5.2 Orbital Mechanics and Revisit

Walker Constellation Model

Satellite constellations are modeled as Walker delta patterns, defined by the triple $(N/P/F)$ where N is the total number of satellites, P is the number of orbital planes, and F is the phasing parameter:

$$ \Delta\Omega = \frac{360°}{P} \qquad \Delta\nu = F \cdot \frac{360°}{N} $$

The revisit time for a point target is computed from the combined coverage of all satellites in the constellation. For a single sun-synchronous orbit at altitude h and inclination i, the ground track spacing between successive passes at the equator is:

$$ \Delta L = \omega_E \cdot T_{\text{orbit}} = \omega_E \cdot 2\pi \cdot \sqrt{\frac{a^3}{\mu}} $$

where ω_E is Earth's rotation rate and a is the semi-major axis. Cloud cover probability further modulates the effective revisit for EO sensors.

5.3 Automated Target Recognition and Change Detection

The IMINT exploitation pipeline includes:

- **Automated Target Recognition (ATR):** Probability of correct classification (P_{cc}) modeled as a function of NIIRS, training data coverage, and target distinctiveness
- **Change detection:** Co-registered image pairs are compared using difference metrics (pixel differencing, ratio maps, or more sophisticated methods); detection probability depends on the change magnitude relative to the noise floor
- **Photogrammetry:** 3D position estimation from stereo image pairs, with accuracy determined by the intersection angle and GSD

6. MASINT: Measurement and Signatures Intelligence

MASINT encompasses technically-derived intelligence from phenomena not covered by other disciplines. The simulator implements nuclear seismic, hydroacoustic, ACINT, RADINT, CBINT, and IR signature models.

6.1 Nuclear Seismic Discrimination

Mb-Ms Discriminant

The primary discriminant between nuclear explosions and earthquakes uses the body-wave magnitude (M_b) versus surface-wave magnitude (M_s) relationship, as established by the CTBT International Monitoring System:

$$ M_b - M_s \text{ discriminant:} \quad \text{Nuclear: } M_b - M_s > \theta \quad \text{Earthquake: } M_b - M_s < \theta $$

For earthquakes, the empirical relationship is approximately $M_s \approx 1.5 M_b - 3.2$, while nuclear explosions have disproportionately low surface waves relative to body waves, yielding higher $M_b - M_s$ values. The discriminant threshold is set at the 95% confidence level per CTBT verification standards.

CTBT IMS Detection

The CTBT International Monitoring System network is modeled with its four technologies:

Technology	Stations	Primary Detection
Seismic	50 primary + 120 auxiliary	Seismic waves (body + surface)
Hydroacoustic	11	Acoustic waves in ocean
Infrasound	60	Low-frequency atmospheric waves
Radiation	80	Particulate and noble gas

Detection probability at each station depends on event magnitude, source-to-station distance, and station noise conditions. The network detection threshold is computed as the minimum magnitude at which three or more stations detect the event (CTBT verification criterion).

6.2 Hydroacoustic Processing

The hydroacoustic model implements the Mackenzie sound speed profile equation for ocean acoustic propagation:

$$ c(D,T,S) = 1448.96 + 4.591T - 0.05304T^2 + 2.374 \times 10^{-4}T^3 + 1.340(S-35) + 1.630 \times 10^{-2}D \\ + 1.675 \times 10^{-7}D^2 - 1.025 \times 10^{-2}T(S-35) - 7.139 \times 10^{-13}TD^3 $$

where T is temperature (°C), S is salinity (PSU), and D is depth (m). The resulting sound speed profile determines the SOFAR channel depth and transmission loss, which govern hydroacoustic detection ranges for CTBT monitoring and submarine tracking.

6.3 ACINT and RADINT

Acoustic Intelligence (ACINT)

Submarine detection via passive acoustic intelligence models broadband and narrowband radiated noise signatures. The sonar detection range equation:

$$ \text{TL}(R) = \text{SL} - \text{NL} - \text{DI} + \text{DT} + \text{RL} $$

where SL is the source level of the submarine's radiated noise, NL is the ambient noise level, DI is the hydrophone directivity index, DT is the detection threshold, and RL represents reverberation losses. Source levels are modeled for different submarine classes and operating conditions (speed, depth, machinery state).

Radar Intelligence (RADINT)

RADINT models the radar cross-section (RCS) of targets for non-cooperative target identification. The RCS varies with aspect angle, frequency, and polarization. Statistical RCS models include:

- Empirical RCS tables for aircraft, ships, and ground vehicles by class
- Frequency-dependent RCS scaling (Rayleigh, resonance, and optical regions)
- Aspect-dependent RCS variation with probability density for fluctuation statistics

6.4 CBINT and IR Signatures

Chemical/Biological Intelligence (CBINT)

Chemical and biological agent detection models atmospheric dispersion (Gaussian plume/puff models) and sensor response characteristics:

$$ C(x,y,z) = \frac{Q}{2\pi \sigma_y \sigma_z u} \cdot \exp\!\left(-\frac{y^2}{2\sigma_y^2}\right) \cdot \left[\exp\!\left(-\frac{(z-H)^2}{2\sigma_z^2}\right) + \exp\!\left(-\frac{(z+H)^2}{2\sigma_z^2}\right)\right] $$

where Q is the source emission rate, H is the effective plume height, u is mean wind speed, and σ_y, σ_z are dispersion coefficients (Pasquill–Gifford stability classes).

Infrared Signatures

IR signature modeling computes apparent temperature contrast for target detection in thermal infrared bands (3–5 µm MWIR, 8–12 µm LWIR). The target contrast radiance:

$$ \Delta L = \varepsilon_t \cdot L(T_t) + \rho_t \cdot L_{\text{sky}} - L(T_{\text{bg}}) $$

where ε_t is target emissivity, ρ_t is reflectivity, and $L(T)$ is the Planck radiance at temperature T.

7. OSINT: Open Source Intelligence

The OSINT package models intelligence derived from publicly available sources, focusing on social media volume dynamics, natural language processing for entity extraction, and source credibility assessment.

7.1 Social Media Volume Modeling

Information flow through social media is modeled as a stochastic process with several components:

- **Baseline volume:** Steady-state posting rate for each platform and topic
- **Event-driven spikes:** Poisson-triggered bursts with exponential decay
- **Amplification dynamics:** Retweet/share cascades modeled as Galton-Watson branching processes
- **Bot/inorganic activity:** Coordinated inauthentic behavior detected via temporal pattern analysis

The volume model for a topic τ at time t:

$$ V(\tau, t) = V_{\text{base}}(\tau) + \sum_k A_k \cdot e^{-(t - t_k)/\tau_{\text{decay}}} + \varepsilon(t) $$

where A_k is the amplitude of event k at time t_k, τ_{decay} is the characteristic decay time, and $\varepsilon(t)$ is the noise floor.

7.2 NLP Entity Extraction

The NLP pipeline processes raw text from OSINT sources to extract structured intelligence:

- **Named entity recognition (NER):** Persons, organizations, locations, dates, events
- **Relationship extraction:** Associative links between entities (affiliation, location, communication)
- **Sentiment and stance analysis:** Position and tone assessment for source credibility weighting
- **Temporal tagging:** Event chronology reconstruction from multiple reports

Extraction confidence is modeled as a function of source quality, text clarity, and corroboration from independent sources.

7.3 Source Credibility

OSINT source credibility is assessed on multiple dimensions:

Dimension	High Credibility	Low Credibility
Proximity	First-hand witness, official source	Third-hand, anonymous
Track record	Consistent accurate reporting	History of errors or retraction
Corroboration	Independent confirmation	Sole source, no corroboration
Plausibility	Consistent with known facts	Contradicts established information

8. FININT: Financial Intelligence

The FININT package models financial system exploitation for intelligence purposes, implementing detection algorithms for money laundering, sanctions evasion, and illicit financial networks.

8.1 Layering Detection

The placement-layering-integration money laundering model tracks funds through multiple financial transformations. The layering detection algorithm identifies suspicious fund flows through:

- **Rapid sequential transfers:** Funds moving through multiple accounts/jurisdictions in short time periods
- **Structuring:** Transactions just below reporting thresholds
- **Circular flows:** Funds returning to origin through circuitous paths
- **Round-tripping:** Funds crossing borders via trade misinvoicing

The layering detection score for a transaction chain of length n across j jurisdictions with average velocity v:

$$ S_{\text{layer}} = w_1 \cdot f(n) + w_2 \cdot g(j) + w_3 \cdot h(v) + w_4 \cdot k(\text{threshold}_{\text{proximity}}) $$

where each component function maps the respective indicator to a normalized risk score and the weights are calibrated against known laundering typologies.

8.2 Cryptocurrency Tracing

Crypto transaction tracing models the traceability of funds through blockchain-based financial systems:

- **UTXO chain analysis:** Following unspent transaction outputs through mixing services and exchanges
- **Cluster identification:** Grouping addresses likely controlled by the same entity via common-input heuristic and change address detection
- **Mixer/tumbler modeling:** Probabilistic tracing through CoinJoin, centralized mixers, and privacy coins with varying obfuscation effectiveness

The traceability coefficient after m mixing rounds with anonymity set A:

$$ T_m = T_0 \cdot \left(1 - \frac{1}{A}\right)^m $$

8.3 Shell Company Analysis

Shell company detection uses corporate registry data patterns to identify likely front entities:

- **Beneficial ownership opacity:** Multi-layered ownership chains through secrecy jurisdictions
- **Registration patterns:** Same registered agent, virtual office addresses, minimal financial activity
- **Network position:** Centrality in trade-based money laundering networks

8.4 Hawala Detection (FATF)

The hawala/informal value transfer system (IVTS) detection model implements Financial Action Task Force (FATF) red flags:

FATF Red Flag	Detection Method
Geographic discrepancies	Sender/receiver in different regions with no apparent business connection
Volume anomalies	Transaction volumes inconsistent with declared business activity
Structuring patterns	Multiple small transfers from different sources to same beneficiary
Lack of formal channels	Value transfer without corresponding formal financial system activity
Round-number patterns	Repeated transfers in round amounts typical of hawala settlements

8.5 Sanctions Evasion

Sanctions evasion detection models the techniques used to circumvent trade and financial restrictions:

- **Transshipment routing:** Goods routed through non-sanctioned intermediaries
- **Flag state manipulation:** Vessel reflagging to obscure ownership
- **Front company layering:** Multi-jurisdictional corporate structures to obscure beneficial ownership
- **Crypto-based evasion:** Cryptocurrency for cross-border value transfer outside traditional banking

9. Multi-INT Fusion Methodology

The Bayesian fusion engine integrates evidence across all six INT disciplines to produce unified intelligence assessments with quantified confidence levels.

9.1 Bayesian Evidence Integration

Each collection event produces an evidence vector $\mathbf{E} = (e_1, \ldots, e_k)$ representing observations relevant to a hypothesis H. The posterior probability of the hypothesis given all evidence is:

$$ P(H \mid \mathbf{E}) = \frac{P(H) \cdot \prod_{i=1}^{k} \frac{P(e_i \mid H)}{P(e_i)}}{Z} $$

where $P(H)$ is the prior, $P(e_i \mid H)$ is the likelihood of evidence i given hypothesis H, and Z is the normalization constant. This factorization assumes conditional independence of evidence given the hypothesis; when dependencies exist (e.g., two SIGINT reports derived from the same intercept), a dependency correction factor is applied.

9.2 Cross-Discipline Corroboration

Corroboration occurs when independent collection disciplines produce consistent evidence for the same hypothesis. The corroboration bonus in the fusion model:

$$ \text{LR}_{\text{corrob}} = \text{LR}_{\text{SIGINT}} \cdot \text{LR}_{\text{HUMINT}} \cdot \text{LR}_{\text{IMINT}} \cdot \text{LR}_{\text{MASINT}} \cdot \text{LR}_{\text{OSINT}} \cdot \text{LR}_{\text{FININT}} \cdot \beta_{\text{ind}} $$

where each LR is the discipline-specific likelihood ratio and β_{ind} is the independence bonus that rewards cross-discipline confirmation. If two disciplines share a common source of error (e.g., SIGINT and OSINT both relying on the same intercepted communications), β_{ind} is reduced accordingly.

9.3 Confidence Quantification

The fusion engine produces confidence assessments at three levels:

- **Discipline-level confidence:** Based on source reliability, collection conditions, and processing quality within each INT
- **Cross-INT confidence:** Based on degree of corroboration, independence of sources, and consistency of evidence
- **Assessment-level confidence:** The final confidence in the intelligence product, incorporating all discipline contributions, remaining information gaps, and known adversary deception potential

Confidence Level	Cross-INT Support	Typical Scenario
High (>0.9)	3+ independent disciplines corroborating	SIGINT + IMINT + HUMINT confirming weapons facility
Medium (0.5–0.9)	2 disciplines, or 1 with strong corroboration	SIGINT intercept confirmed by OSINT social media posts
Low (<0.5)	Single discipline, or conflicting evidence	Unverified HUMINT source, no SIGINT/IMINT corroboration

10. Collection Management

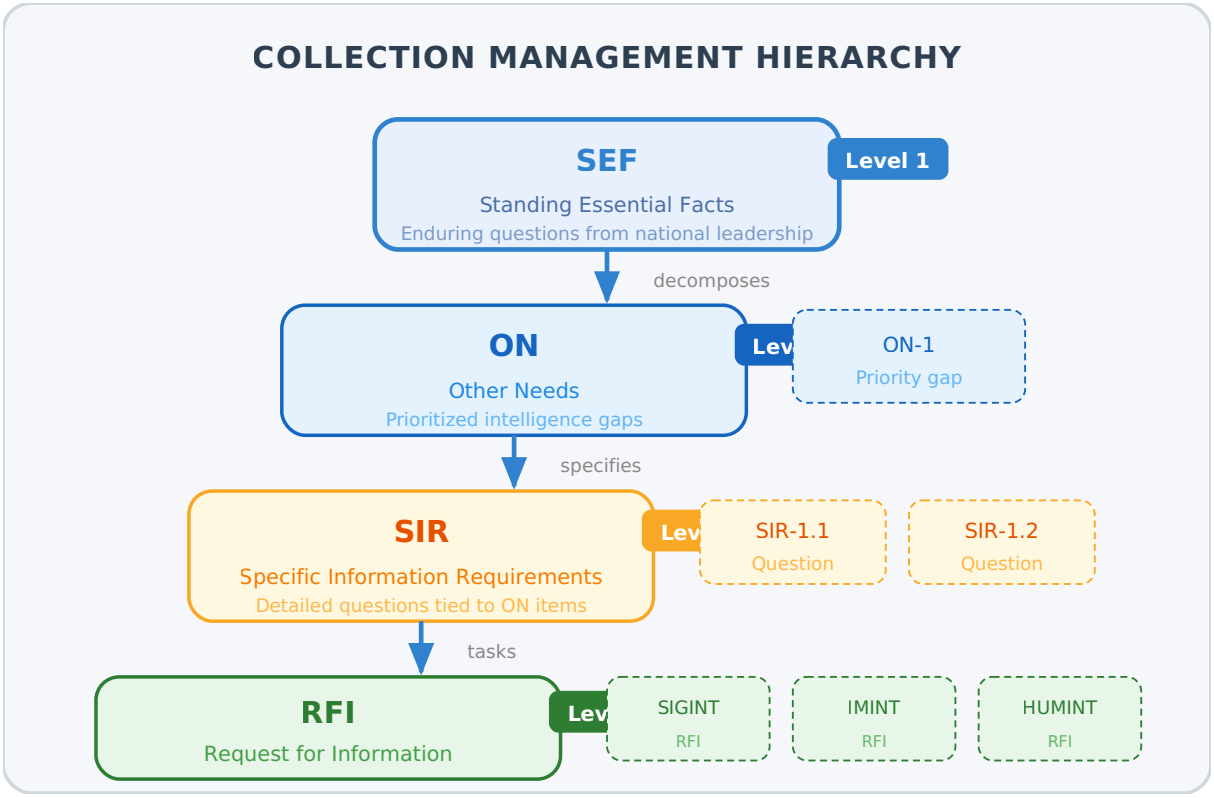
The collection management system implements the hierarchical prioritization and tasking of intelligence assets, with game-theoretic optimization for adversarial environments.

10.1 Collection Requirement Hierarchy

Requirements flow through a four-tier hierarchy:

Level	Abbreviation	Description	Scope
1	**SEF**	Standing Essential Facts	Enduring questions from national leadership
2	**ON**	Other Needs	Prioritized intelligence gaps
3	**SIR**	Specific Information Requirements	Detailed questions tied to ON items
4	**RFI**	Request for Information	Specific collection tasking for assets

Each SIR is decomposed into multiple RFIs, and each RFI specifies the required INT discipline(s), collection parameters, timeliness requirements, and acceptable confidence levels.



10.2 Game-Theoretic Asset Tasking

In an adversarial environment, collection tasking must account for the fact that the adversary adapts their behavior in response to observed collection. This is modeled as a two-player game:

- **Collector's strategy:** Allocation of collection assets across targets and INT disciplines
- **Adversary's strategy:** Allocation of OPSEC resources, deception operations, and emission control

The collector seeks to maximize expected information gain; the adversary seeks to minimize it. The Nash equilibrium is approximated using iterative best-response dynamics, where each side alternately optimizes its strategy given the other's current posture:

$$ \pi_C^* = \arg\max_{\pi_C} I\!\left(\pi_C,\, \pi_A^{(n)}\right) \qquad \pi_A^* = \arg\max_{\pi_A} -I\!\left(\pi_C^{(n)},\, \pi_A\right) $$

where I is the mutual information between the collection outcomes and the intelligence parameter of interest. The iterative process converges when neither side can improve its payoff by unilaterally changing strategy.

10.3 Collection Prioritization

RFIs are prioritized using a weighted scoring model:

$$ \text{Priority}(\text{RFI}_i) = w_{\text{gap}} \cdot G_i + w_{\text{urg}} \cdot U_i + w_{\text{value}} \cdot V_i - w_{\text{cost}} \cdot C_i - w_{\text{risk}} \cdot R_i $$

where G is the intelligence gap severity, U is urgency, V is expected intelligence value, C is collection cost (asset time, opportunity cost), and R is operational risk (source exposure, asset compromise).

11. Counterintelligence and Adversary Modeling

The counterintelligence and adversary modeling subsystem creates the dynamic adversarial environment that distinguishes intel-collection-sim from passive simulation frameworks. Adversaries react, adapt, deceive, and counter-collect.

11.1 Denial and Deception (D&D)

The adversary D&D model implements the full spectrum of denial and deception operations:

Operational Security (OPSEC)

Adversary OPSEC measures reduce the collection effectiveness of friendly assets:

OPSEC Measure	Discipline Affected	Effectiveness Model
Emission control (EMCON)	SIGINT	Reduces emitter duty cycle; probability of intercept drops proportionally
Camouflage and concealment	IMINT	Reduces target contrast and NIIRS interpretability
Communications security (COMSEC)	SIGINT	Encryption increases processing difficulty; content exploitation probability drops
Counter-surveillance	HUMINT	Increases λ_{surv} hazard rate for source compromise
Financial layering	FININT	Increases layering depth; reduces traceability coefficient

Military Deception and Maskirovka

The Russian concept of maskirovka (military deception) is modeled as a multi-layered deception strategy:

- **Strategic deception:** False force postures, simulated headquarters activity, deceptive communications
- **Operational deception:** Feints, demonstrations, false assembly areas
- **Tactical deception:** Camouflage, decoys, thermal shielding, radar reflectors

Deception effectiveness is modeled as the probability that the friendly intelligence assessment is misled:

$$ P_{\text{deceived}} = P_{\text{accept false}} \cdot \bigl(1 - P_{\text{detect deception}} \bigr) $$

where $P_{\text{accept false}}$ is the probability the deception narrative is accepted and $P_{\text{detect deception}}$ is the probability the friendly analyst detects the deception, which increases with multi-INT corroboration (a key advantage of fusion).

Counter-Collection

Adversary counter-collection operations directly target friendly intelligence assets:

- **Technical counter-measures:** Jamming (SIGINT), radar spoofing, IR decoys
- **Human counter-intelligence:** Surveillance of known case officers, double-agent operations
- **Cyber collection:** Targeting collection systems and communication channels

11.2 Mole Detection and Double-Agent Games

Mole Detection

The mole detection model identifies anomalies in information flow that may indicate an insider threat:

- **Statistical anomaly detection:** Deviations from baseline information access patterns
- **Honeypot canaries:** Planted information whose unauthorized disclosure indicates compromise
- **Behavioral analysis:** Changes in work patterns, financial indicators, foreign travel

The detection probability over time for a mole with access level L and the system's detection rate λ_d:

$$ P_{\text{detect}}(t) = 1 - e^{-\lambda_d \cdot L \cdot t} $$

Double-Agent Games

When a source is identified as potentially compromised, the handler faces a decision: terminate the relationship, continue with awareness of potential disinformation, or

attempt to "double" the double agent. This is modeled as a sequential game of imperfect information:

- **State:** Source is genuine, compromised (feeding disinformation), or doubled (genuinely recruited but under adversary control
- **Handler's actions:** Terminate, continue, feed counter-deception
- **Adversary's actions:** Maintain cover, escalate disinformation, expose the operation

The expected value of each action depends on the handler's belief about the source's true state, which is updated via Bayesian inference as new observations arrive.

Damage Assessment and Compromise Cascades

When a source compromise is detected, the damage assessment model evaluates:

- **Direct damage:** Information the compromised source had access to
- **Cascade damage:** Information from other sources that could be inferred from the compromised source's knowledge (network analysis)
- **Operational damage:** Compromised methods, dead drops, communication channels
- **Counterintelligence exposure:** Case officer identities, handling procedures, technical capabilities revealed

11.3 Covert Action Operations

The covert action module models deniable operations that influence conditions in the target environment:

Operation Type	Modeling Approach	Key Metrics
Political warfare	Influence propagation through elite networks	Regime stability index, elite defection probability
Propaganda	Information diffusion model with source attribution	Penetration rate, credibility score, counter-narrative effectiveness
Paramilitary	Force capability model with logistic constraints	

		Operational readiness, sustainment days, area control percentage
Economic operations	Market impact model with sanction/regime coupling	GDP impact, regime revenue reduction, black market growth
Front companies	Corporate network with beneficial ownership obfuscation	Cover depth, detection probability, operational utility

12. Built-in Scenarios

The six built-in scenarios demonstrate the system's ability to simulate complex, multi-discipline intelligence operations with dynamic adversary responses.

Scenario	Primary INTs	Adversary Reaction	Complexity
Nuclear Test Monitoring	MASINT, SIGINT	Decoupling, cavity masking, evasion of IMS	High
SIGINT Sweep Operation	SIGINT, OSINT	EMCON, frequency migration, COMSEC upgrades	Medium
Financial Crime Investigation	FININT, OSINT	Shell restructuring, crypto mixing, jurisdiction shopping	Medium
HUMINT Network Penetration	HUMINT, SIGINT	Counter-intel sweep, double-agent feeding, surveillance	High
Imagery Intelligence Campaign	IMINT, MASINT	Camouflage, decoys, facility concealment, timing deception	Medium
	All 6 INTs		Very High

Full-Spectrum Intelligence Operation		Coordinated D&D, counterintel, OPSEC, counter-collection	

12.1 Nuclear Test Monitoring Scenario

This scenario simulates the detection and identification of a clandestine nuclear test. The adversary attempts to evade detection through decoupling (reducing seismic yield by detonating in a large underground cavity), evading the IMS network, and masking the test as a natural earthquake.

The friendly collection strategy employs MASINT (seismic, hydroacoustic, radionuclide), SIGINT (intercepting test preparation communications), and OSINT (monitoring social media for test-related announcements). The Bayesian fusion engine integrates seismic $M_b–M_s$ discriminants with radionuclide detections and SIGINT-derived indicators to assess the nuclear test hypothesis.

12.2 Full-Spectrum Intelligence Operation Scenario

The most complex scenario exercises all six INT disciplines simultaneously. A regional adversary is developing a prohibited weapons program while conducting denial and deception operations, active counterintelligence, and covert influence activities. The friendly intelligence community must plan collection across all disciplines, manage collection assets, detect and counter adversary deception, and produce fused intelligence assessments.

This scenario exercises the full intelligence cycle with feedback: early collection failures (due to adversary OPSEC) drive revised collection strategies, while adversary counterintelligence successes (detected through the mole detection model) force operational security reviews of friendly HUMINT networks.

13. Validation and Testing

The simulator maintains 551 tests, including over 90 physics validation tests that verify the physical accuracy of the collection models.

13.1 Physics Validation Approach

Each physics model is validated against published standards and empirical data:

Model	Validation Standard	Validation Method
FSPL	ITU-R P.525-3	Comparison with analytical free-space path loss at reference distances and frequencies
Atmospheric absorption	ITU-R P.676-13	Line-by-line computation benchmark against ITU reference values at 1–1000 GHz
Rain fade	ITU-R P.838-4	Specific attenuation at standard rain rates compared to ITU regression coefficients
Mb-Ms discriminant	CTBT IMS	Historical nuclear test vs. earthquake populations at known magnitudes
Hydroacoustic SSP	Mackenzie (1981)	Sound speed at standard ocean temperature/salinity/depth profiles
Hawala detection	FATF 40 Recommendations	Red flag patterns against known case study typologies
Radar range	Skolnik reference	Maximum detection range vs. Skolnik's radar handbook values for standard targets
GSD/NIIRS	GIQE 5.0	NIIRS predictions at known GSD/MTF/SNR compared to GIQE estimates
TDOA geolocation	Analytical CRLB	Localization error vs. Cramér-Rao lower bound for known geometries
Swerling detection	Marcum/Q-function	

		Detection probability vs. Marcum function reference for each Swerling case

13.2 Integration Testing

Beyond physics validation, integration tests verify:

- **Cross-INT fusion consistency:** That corroboration from independent disciplines increases confidence as expected
- **Adversary reaction dynamics:** That adversary OPSEC adaptations reduce collection effectiveness and that the game-theoretic tasking equilibrium is reached
- **Intelligence cycle completeness:** That feedback from dissemination alters planning priorities in subsequent cycles
- **Compromise cascade accuracy:** That HUMINT network compromise propagates consistent with the graph distance model
- **Scenario reproducibility:** That fixed random seeds produce identical simulation runs

13.3 Test Coverage Summary

Category	Count	Focus
Physics validation	90+	Physical accuracy against standards
Unit tests	~300	Individual model component correctness
Integration tests	~100	Cross-package interaction and fusion
Scenario tests	~60	End-to-end scenario execution
Total	**551**	

14. Cross-Simulation Integration

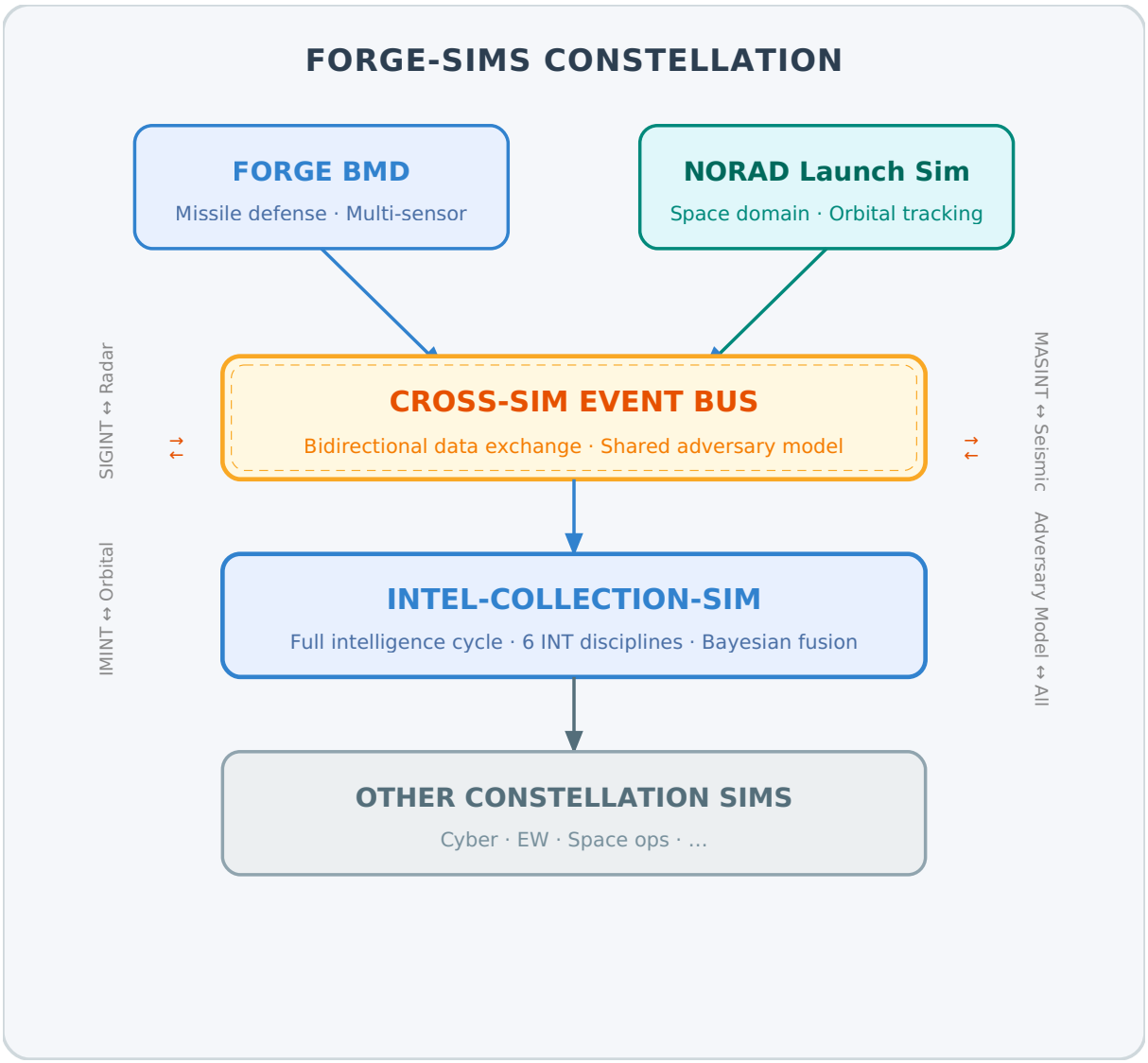
Intel-collection-sim provides integration hooks for the FORGE-SIMS constellation, enabling multi-domain operations research that combines intelligence collection simulation with complementary simulation systems.

14.1 FORGE-SIMS Constellation

The FORGE-SIMS constellation includes:

- **FORGE:** Missile defense simulation with multi-sensor fusion
- **NORAD Launch Simulation:** Space domain awareness and orbital tracking
- **Intel-collection-sim:** Intelligence cycle simulation (this system)
- **Other constellation members:** Additional simulation platforms for cyber, electronic warfare, and space operations

14.2 Integration Architecture



14.3 Integration Points

Integration Point	Direction	Data Exchange
SIGINT ↔ FORGE radar	Bidirectional	Radar parameters, target tracks, collection opportunities
MASINT seismic ↔ NORAD	Bidirectional	Launch detection, seismic events, tracking data
IMINT ↔ NORAD orbital	Bidirectional	Satellite tasking, orbital parameters, revisit windows

FININT ↔ Market analysis	Outbound	Financial anomaly indicators, sanctions compliance
Adversary model ↔ All	Bidirectional	Adversary posture, OPSEC state, deception indicators

15. Conclusion

Intel-collection-sim provides a comprehensive, physics-grounded simulation platform for the full intelligence cycle across six disciplines. The system's key contributions are:

- **Physics fidelity across all INT disciplines:** 90+ validation tests ensure that collection outcomes emerge from authentic physical processes, from ITU-R-compliant RF propagation to CTBT-standard seismic discrimination.
- **Adversary-aware simulation:** The dynamic adversary reaction system—including denial and deception, counterintelligence, and adaptive OPSEC—ensures that collection strategies must account for an intelligent opponent, reflecting the fundamental nature of intelligence operations.
- **Bayesian multi-INT fusion:** The evidence integration engine with cross-discipline corroboration provides a principled framework for combining disparate intelligence sources into unified assessments with quantified confidence.
- **Complete intelligence cycle modeling:** The time-stepped cycle engine with feedback ensures that collection planning, processing, analysis, and dissemination are not isolated events but an iterative process that adapts to adversary reactions and consumer needs.
- **Game-theoretic collection management:** The asset tasking system recognizes that intelligence collection is a strategic interaction between collector and adversary, producing tasking strategies that are robust against adversary adaptation.
- **Constellation integration:** Cross-simulation hooks enable multi-domain operations research by connecting intelligence collection to missile defense, space domain awareness, and other simulation domains.

The six built-in scenarios demonstrate the system's capability across a range of intelligence problems, from focused nuclear monitoring to full-spectrum multi-discipline operations. The 551-test suite, including over 90 physics validations, provides confidence that the simulation's outputs reflect authentic physical and behavioral dynamics rather than artifacts of the modeling framework.

Future development directions include expanded counterintelligence modeling, integration of cyber as a seventh INT discipline, machine learning-based collection strategy optimization, and real-time human-in-the-loop simulation interfaces for training applications.

References

1. International Telecommunication Union, Recommendation ITU-R P.525-3: Calculation of Free-Space Attenuation, Geneva, 2019.
2. International Telecommunication Union, Recommendation ITU-R P.676-13: Attenuation by Atmospheric Gases and Related Effects, Geneva, 2023.
3. International Telecommunication Union, Recommendation ITU-R P.838-4: Specific Attenuation Model for Rain for Use in Prediction Methods, Geneva, 2005.
4. International Telecommunication Union, Recommendation ITU-R P.839-4: Rain Height Model for Prediction Methods, Geneva, 2013.
5. Comprehensive Nuclear-Test-Ban Treaty Organization, CTBT International Monitoring System: Seismic, Hydroacoustic, Infrasound, and Radionuclide Technologies, Vienna, 2020.
6. Financial Action Task Force, FATF 40 Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, Paris, 2023.
7. Financial Action Task Force, FATF Report on Money Laundering through Hawala and Other IVTS, Paris, 2013.
8. Mackenzie, K.V., "Nine-Term Equation for Sound Speed in the Oceans," Journal of the Acoustical Society of America, vol. 70, no. 3, pp. 807–812, 1981.
9. Skolnik, M.I., Radar Handbook, 3rd ed., McGraw-Hill, New York, 2008.
10. Swerling, P., "Probability of Detection for Fluctuating Targets," IRE Transactions on Information Theory, vol. 6, no. 2, pp. 269–308, 1960.
11. Marcum, J.I., "A Statistical Theory of Target Detection by Pulsed Radar," IRE Transactions on Information Theory, vol. 6, no. 2, pp. 145–267, 1960.

12. Leachtenauer, J.C. and Driggers, R.G., Surveillance and Reconnaissance Imaging Systems: Modeling and Performance Prediction, Artech House, 2001.

13. General Image Quality Equation (GIQE) 5.0, National Geospatial-Intelligence Agency, 2015.

14. Walker, J.G., Satellite Constellations, IEE Publication, 1977.

15. U.S. Central Intelligence Agency, A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis, Center for the Study of Intelligence, 2009.

16. Dulles, A.W., The Craft of Intelligence, Greenwood Press, 1963.

17. Godson, R. and Wirtz, J.J., Strategic Denial and Deception: The Twenty-First Century Challenge, Transaction Publishers, 2002.

18. Whaley, B., Stratagem: Deception and Surprise in War, Artech House, 1969.

19. Bayes, T., "An Essay towards Solving a Problem in the Doctrine of Chances," Philosophical Transactions of the Royal Society, vol. 53, pp. 370–418, 1763.

20. Nash, J.F., "Non-Cooperative Games," Annals of Mathematics, vol. 54, no. 2, pp. 286–295, 1951.

21. Pasquill, F., Atmospheric Diffusion: The Dispersion of Windborne Material from Industrial and Other Sources, 2nd ed., Ellis Horwood, 1974.

22. Joint Publication 2-0, Joint Intelligence, U.S. Department of Defense, 2013.

23. Joint Publication 2-01, Joint and National Intelligence Support to Military Operations, U.S. Department of Defense, 2017.

24. International Civil Aviation Organization, Convention on International Civil Aviation (Chicago Convention), Annex 6, 1944.