Cybersecurity, Artificial Intelligence, and the Protection of Space Assets



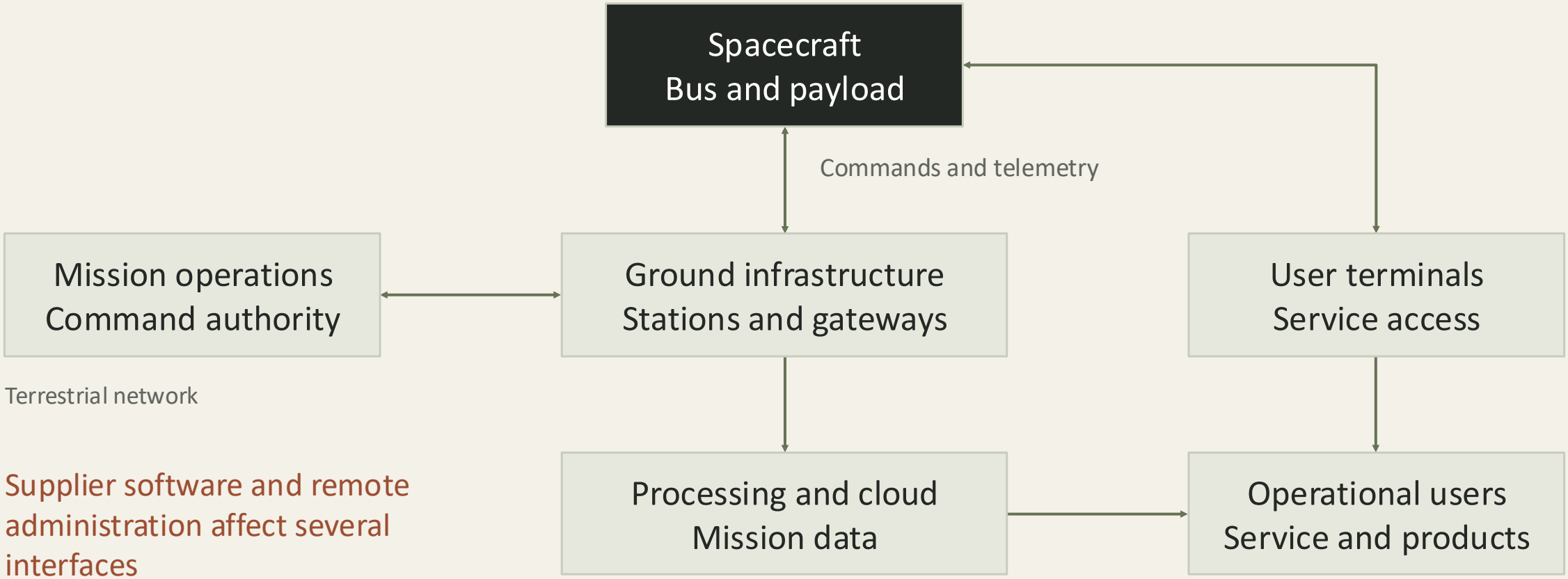
Heriberto Acosta-Maestre, PhD

Mission planning, procurement, and operational oversight

Satellite-data composite, Suomi NPP VIIRS. NASA/JPL

The architecture of a space service

Conceptual architecture. Functions and ownership vary by mission.



(Lightman et al., 2022; McCarthy, Mamula, et al., 2023; NASA, 2023)

Cyber exposure across the mission lifecycle

Design	Command authority and trust boundaries
Integration	Supplier software and partner access
Operations	Credentials, updates, and recovery
Retirement	Access withdrawal and retained data



Ground infrastructure at Goldstone, August 2026

JPL intrusion discovered in 2018

Stolen mission data and weaknesses in partner segmentation

Photo credit NASA/JPL-Caltech

(NASA, 2023; NASA OIG, 2019; Lightman et al., 2022)

Operational consequences depend on the access obtained

Analytical pathways. Consequences depend on privileges and architecture.

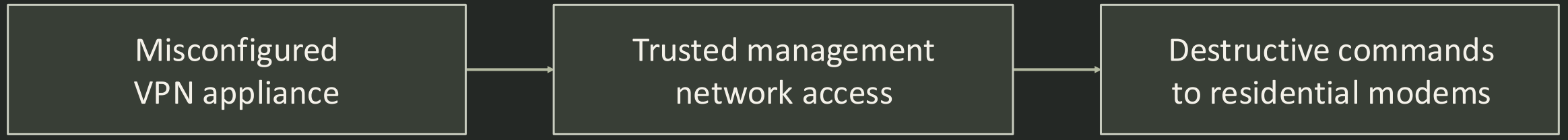
Access or disruption	Mission function	Planning consequence
Command-system access	Spacecraft and payload control	Loss of trusted command authority
Data or metadata alteration	Intelligence, surveillance, and reconnaissance	Unreliable or stale operational picture
Terminal management abuse	Satellite communications	Interrupted coordination and service
PNT signal or data manipulation	Positioning, navigation, and timing	Navigation or synchronization errors

Radio jamming, signal spoofing, and network intrusion have different mechanisms

(Lightman et al., 2022; McCarthy, Li-Baboud, et al., 2023; U.S. Space Force, 2024)

KA-SAT in February 2022

Documented incident. February 24, 2022



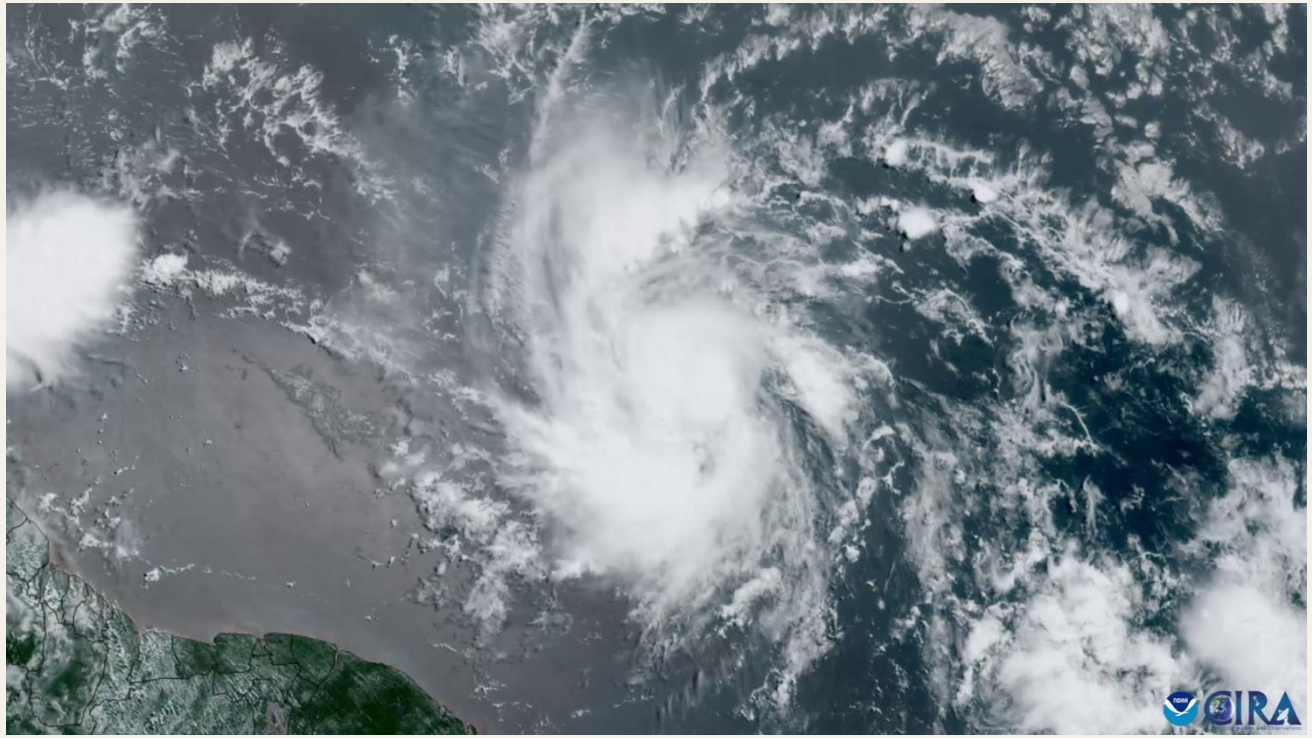
Consumer service disruption

Viasat reported no evidence of satellite compromise

Operator account	Technical sequence and affected partition
U.S. government assessment	Russian attribution and command-and-control objective

(Viasat, 2022; CISA, 2022; CISA & FBI, 2022)

Western Hemisphere dependencies



Beryl, GOES-16 GeoColor imagery, 2024

NOAA/CIRA. Still from an official NOAA animation.

(NOAA NESDIS, 2024; Telebras, n.d.; McCarthy, Li-Baboud, et al., 2023)

Caribbean weather awareness

Timely observations and usable delivery networks

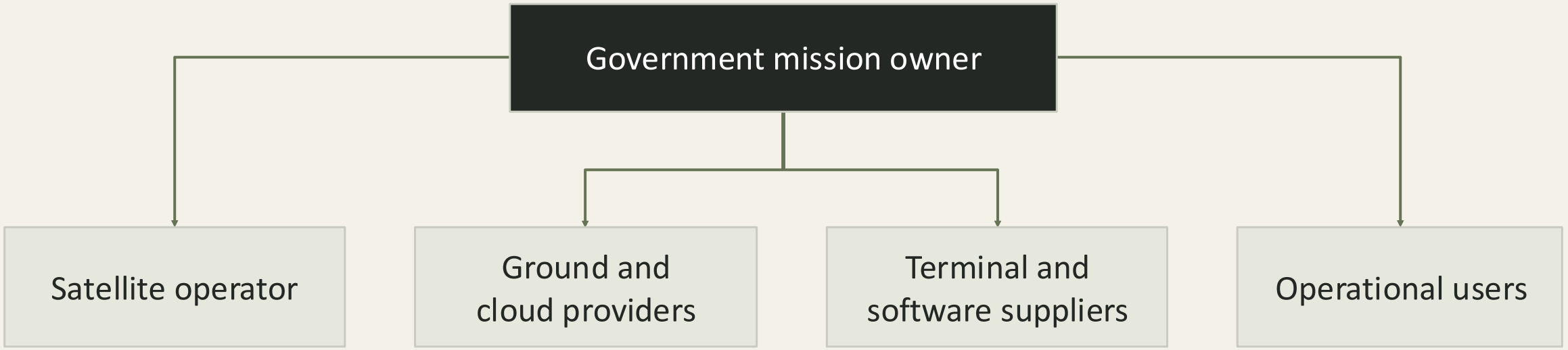
Brazil's SGDC

Civil Ka-band broadband
Military X-band communications

Regional dependencies, with no cyber incident asserted

Commercial integration changes the responsibility chain

2024 U.S. policy directs integration before crisis and conflict



Monitoring, incident authority, and restoration duties cross organizational boundaries

Conceptual responsibility map

(Garamone, 2024; U.S. Space Force, 2024; GAO, 2025; McCarthy, Mamula, et al., 2023)

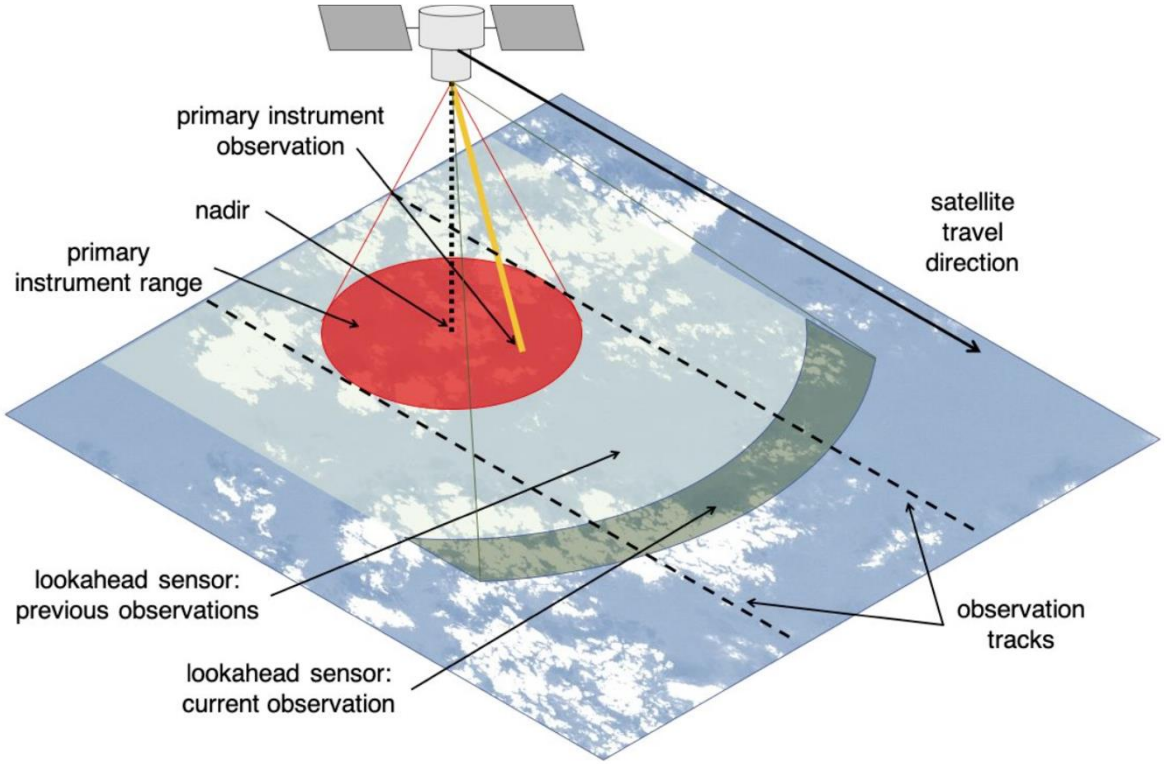
AI across the mission

Mission task	Verified example	Evidence status
Telemetry anomaly detection	Cuéllar et al. NASA mission datasets, 2024	Peer-reviewed research evaluation
Satellite-data analysis	Expanded Prithvi Geospatial model, 2024	Released model and reported applications
Observation planning	Dynamic Targeting CogniSAT-6, July 2025	Flight test of cloud avoidance
Onboard image processing	Φsat-2 Science phase in 2025	Demonstrator mission

Algorithm performance and operational authority require separate evidence

(Cuéllar et al., 2024; Leese, 2024; NASA JPL, 2025; ESA, 2025)

Bounded autonomy in observation planning



General look-ahead concept. CogniSAT-6 tilted its imaging sensor.

(NASA JPL, 2025; ESA, 2025)

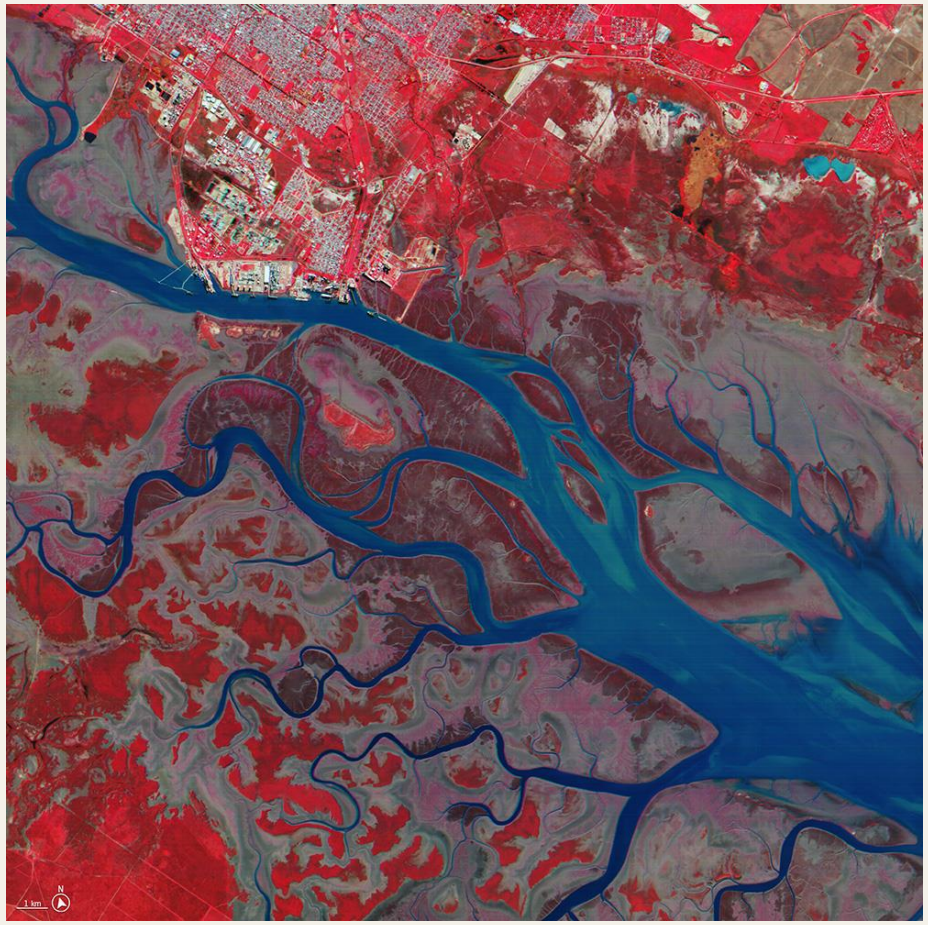
CogniSAT-6 flight test

Cloud analysis informed sensor pointing

Reported cycle under 90 seconds

NASA/JPL-Caltech

Evidence before operational reliance



Bahía Blanca, Argentina
Φsat-2 false-color infrared composite

Source evidence	Retain observations and acquisition context
Validation	Test the intended sensor, conditions, and task
Anomaly alerts	Engineering review establishes significance

Image ©ESA, published July 15, 2025

(Cuéllar et al., 2024; Leese, 2024; ESA, 2025; Autio et al., 2024)

Attacks on AI-supported workflows

Illustrative attack pathways. No satellite incident is asserted.

Attacker access	Manipulation	Potential operational effect
Training or development chain	Data poisoning or altered model	Biased or unreliable analysis
Operational input pipeline	Evasion through manipulated inputs	Missed detection or false classification
Retrieved records or documents	Prompt injection into an assistant	Misleading guidance or tool misuse

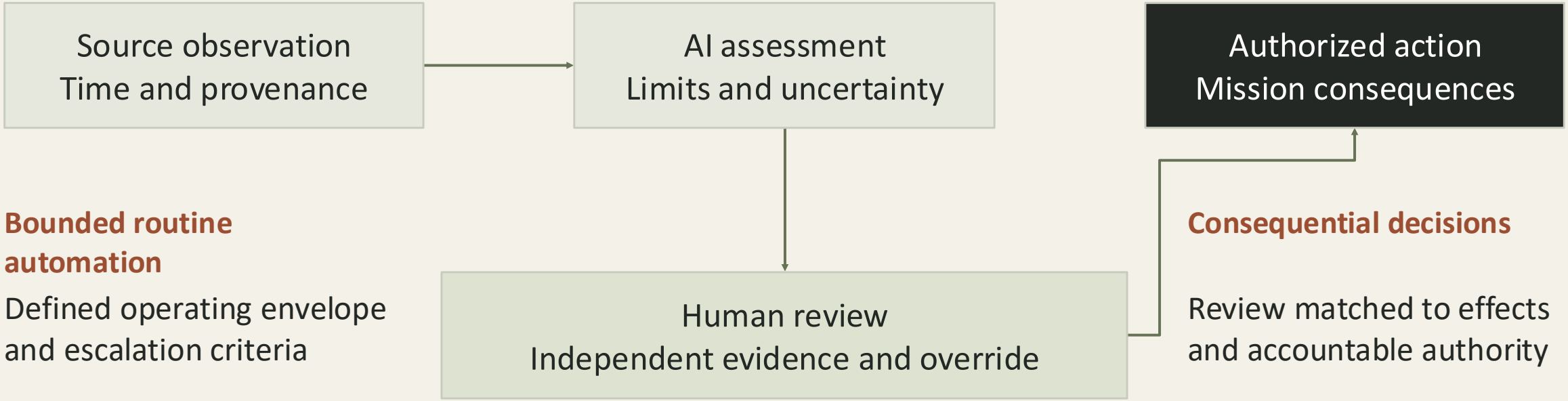
The cyber defense boundary includes models and data pipelines

Confident errors and automation bias can occur without an attacker

(Vassilev et al., 2025; Autio et al., 2024)

Human oversight at consequential decisions

Recommended review and authority model



Oversight requires evidence, time, training, and an effective ability to intervene

(Autio et al., 2024; U.S. DoD, 2021)

Procurement and continuity requirements

Recommended commitments for institutions purchasing space services

Commitment	Responsible party	Acceptance evidence
Essential service and tolerable outage	Government mission owner	Minimum service demonstrated under disruption
Incident and restoration duties	Owner and delivery-chain providers	Joint reporting and recovery exercise
Cyber and AI requirements	Acquisition office and suppliers	Access, integrity, update, and use-case testing
Usable alternatives	Operators and service providers	Fallback with working equipment and trained staff

2026 GAO oversight continues to highlight NASA cyber risk management

(CISA & FBI, 2022; Pascoe et al., 2024; GAO, 2024; GAO, 2026; McCarthy, Mamula, et al., 2023)

Priorities for mission owners

Protection follows the mission’s dependencies

Essential functions	Map terrestrial and commercial dependencies
Continuity	Exercise alternatives and trusted recovery
Accountability	Assign duties and require procurement evidence
Human judgment	Match AI authority to operational consequence

(NASA, 2023; Garamone, 2024; CISA & FBI, 2022; Autio et al., 2024; Pascoe et al., 2024)