BIF
BROADBAND INDIA FORUM
"Think Tank for Digital Transformation"

Trusted from Space to Ground: Cybersecurity for India's Satcom Networks

August 2026

ACKNOWLEDGEMENT

BIF sincerely thanks its SatCom and Cyber Security Committees and their members for their support and contribution in the preparation of this report.

SATELLITE COMMUNICATIONS DEPEND ON TRUST ACROSS SIGNALS, GATEWAYS, DEVICES AND DATA PATHS.

SECURITY CONDITIONS ACROSS THIS CONNECTED SYSTEM SHAPE THE RELIABILITY AND SCALE OF INDIA'S SATCOM DEVELOPMENT.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Satellite communications (SatCom) are becoming part of India's mainstream digital and telecom environment. They connect people and services in places that terrestrial networks may not reach. They also support business, public services, transport and emergency response. As this dependence grows, cybersecurity becomes a larger part of the service's operating context.

This report asks four practical questions. What can an attacker reach? What could that access control? How could the effects spread to other systems, and what evidence would show that safeguards and recovery plans work?

THE WHOLE SERVICE CHAIN, INCLUDING THE SPACECRAFT

A SatCom service is a system of connected systems. It includes spacecraft and payloads; telemetry, tracking and command (TT&C); ground stations and gateways; telecom cores; cloud services; application programming interfaces (APIs); identity and key services; suppliers; user terminals; and radio-frequency and timing inputs.

The same technologies that make modern services flexible also create new entry points. Internet Protocol (IP) connectivity creates internet- and IP-based intrusion paths into cloud, API and management environments.

Ground systems are generally more reachable than spacecraft. TT&C command paths can affect mission state. Shared terminal defaults can allow a device-level weakness to spread across a fleet, while interconnections can carry impacts between systems and organisations. Spacecraft security is one part of a chain that also includes gateway integrity, management-API authentication, terminal firmware, signing keys and service-link encryption.

WHAT INCIDENTS AND RESEARCH TELL US

The February 2022 KA-SAT attack is a documented operational example [13, 29, 47]. Reporting on the incident indicates that the attacker entered through a misconfigured virtual private network (VPN) appliance [47]. The attacker moved into a trusted management segment and used legitimate management commands to overwrite data in many modems [29, 47]. Public reporting found no impairment of the satellite itself within the reported scope of the investigation [47]. The strategic effect began in ordinary ground infrastructure and spread to the distributed edge.

In July 2026, the United States Cybersecurity and Infrastructure Security Agency (CISA) disclosed iDirect terminal flaws that could expose authentication identifiers and cause repeated reboots; CISA reported no known public exploitation [16]. Controlled research has also shown radio frequency (RF) injection into a commercial very small aperture terminal (VSAT) modem, supervised on-orbit effects in the European Space Agency's OPS-SAT exercise, and sensitive cleartext over commercial geostationary orbit (GEO) downlinks [4, 24, 48]. These are not operational attacks. They show that weaknesses can lie in terminal interfaces, update trust, RF inputs and encryption.

A FOUR-DOMAIN VIEW OF CONNECTED RISK

The report groups the service chain into four practical domains: Ground, Space, User, and Interconnect and Cyber-RF. One operator may work in several domains, and an incident may start in one and cause effects in another.

Ground. Gateways, mission-support systems, VPNs, cloud consoles, APIs, identities and suppliers are reachable and change often. Cloud and ground-station-as-a-service models may also assign outside providers operational privileges that affect service state.

Space. TT&C is a mission-control path. Its security properties include authorised command sources, message freshness that distinguishes new commands from replays, and telemetry integrity during communications gaps and emergency procedures.

User. Terminals are numerous, long-lived and often physically exposed. Unique device identity, authenticated management, signed firmware, fleet inventory, revocation and secure reset determine whether one flaw stays local or becomes a fleet-wide problem.

Interconnect and Cyber-RF. The report uses Cyber-RF for risks that cross between digital systems and radio-frequency operations. Jamming, spoofing, gateway compromise and terminal failure can look similar. Classification draws on evidence from the network operations centre (NOC), security operations centre (SOC), cloud systems, terminals and RF monitoring.

INDIA'S INSTITUTIONAL FOUNDATION AND ACTOR COORDINATION

India's existing framework includes rules and institutions relevant to SatCom cybersecurity. The Indian Computer Emergency Response Team (CERT-In) 2026 space-cyber framework provides an end-to-end baseline [8]. Telecom rules, critical-infrastructure arrangements, Indian National Space Promotion and Authorisation Centre (IN-SPACe) security information, and assurance pathways through the Telecommunication Engineering Centre (TEC) and National Centre for Communication Security (NCCS) add obligations and evidence channels [21, 22, 23, 27, 28].

Coordination spans several reporting, investigation and recovery processes, while systems and evidence may be distributed among operators, cloud providers, gateway owners, terminal vendors and RF authorities. Licensing and spectrum processes can also create cyber control points, including command-security conditions, domestic gateways and interference investigations.

RESILIENCE, INCIDENT CONTAINMENT AND VERIFIED RECOVERY

Here, resilience means containing an incident while the operator still knows who controls the service, often called positive control. It includes safe failover, compromised-key revocation, rollback and restoration from a verified state. Recovery can deepen an incident if it uses compromised software, keys or settings. Resilience does not replace prevention, authentication, segmentation, monitoring or software assurance.

EMERGING TECHNOLOGIES CHANGE ATTACK SPEED, SOFTWARE DEPENDENCE AND MIGRATION TIMELINES

New technologies can change security and service delivery, as well as attack speed and scale. Each changes the evidence used to assess trust.

ARTIFICIAL INTELLIGENCE CAN HELP DEFENDERS AND ATTACKERS

Artificial intelligence (AI) can help analysts detect unusual activity. It can combine evidence from telemetry, radio-frequency data and network logs. This can help teams identify incidents faster.

AI can also pose risks. Capable models can be used to map attack paths and chain weaknesses faster. They can automate reconnaissance, steal intellectual property or support targeted attacks. AI may also produce false or distracting alerts. Accountable human approval remains associated with actions that can alter operational state.

During a July 2026 OpenAI cyber evaluation, an autonomous agent crossed its test boundary and reached Hugging Face production systems [30, 41]. This was unintended, not a deliberate attack. OpenAI detected the activity, Hugging Face contained it, and the companies investigated together. Hugging Face used an open-weight model locally to reconstruct the incident.

Open-weight models can keep sensitive code or evidence inside an approved local environment. Hosted foundation models, such as GPT-5.6 Sol and Claude Fable 5, can provide reasoning, long-horizon analysis, tool coordination and provider-managed safeguards for code review, vulnerability triage and patching. Model assessment can compare tested capability, safeguards and data-handling arrangements; continuous validation of flight software, ground-control networks and telemetry protocols is one possible application.

QUANTUM RISK AND LONG-TERM SECURITY TRANSITION

Future large-scale quantum computers could weaken widely used public-key cryptography [39]. The timing issue arises because spacecraft, terminals, sensitive data and signing roots may remain in use for years. An adversary could collect encrypted information today and try to decrypt it later [38, 39]. Long replacement cycles can therefore turn a future capability into a present planning risk.

Post-quantum migration concerns long-lived command, signing and identity systems. A migration inventory maps cryptography used for commands, identities, software updates, stored data and key exchange. Crypto-agility describes the ability to change algorithms and keys without redesigning the whole service. A phased transition can generate evidence on interoperability, supplier readiness, key and certificate changes, rollback and safe operation before wholesale replacement becomes necessary.

SOFTWARE, CONNECTED DEVICES AND ASSURANCE EVIDENCE

Software-defined payloads and cloud-based ground systems can be updated quickly. Provenance evidence records where software came from, how it was built, who approved it and whether the running version matches the approved version.

Non-terrestrial networks (NTNs) and direct-to-device (D2D) services add large device and subscriber populations [1, 2]. At that scale, the control set includes secure onboarding, mutual authentication, rate limits, signed updates, revocation and fraud detection.

SECURITY EVIDENCE AT SYSTEM HAND-OFFS

Control evidence becomes more complex where space, telecom, cloud, RF, suppliers and users meet. Lifecycle assurance spans architecture, procurement, operations, recovery and retirement. Evidence across organisational boundaries can connect identities, commands, software changes, gateway actions, terminal state and RF observations.

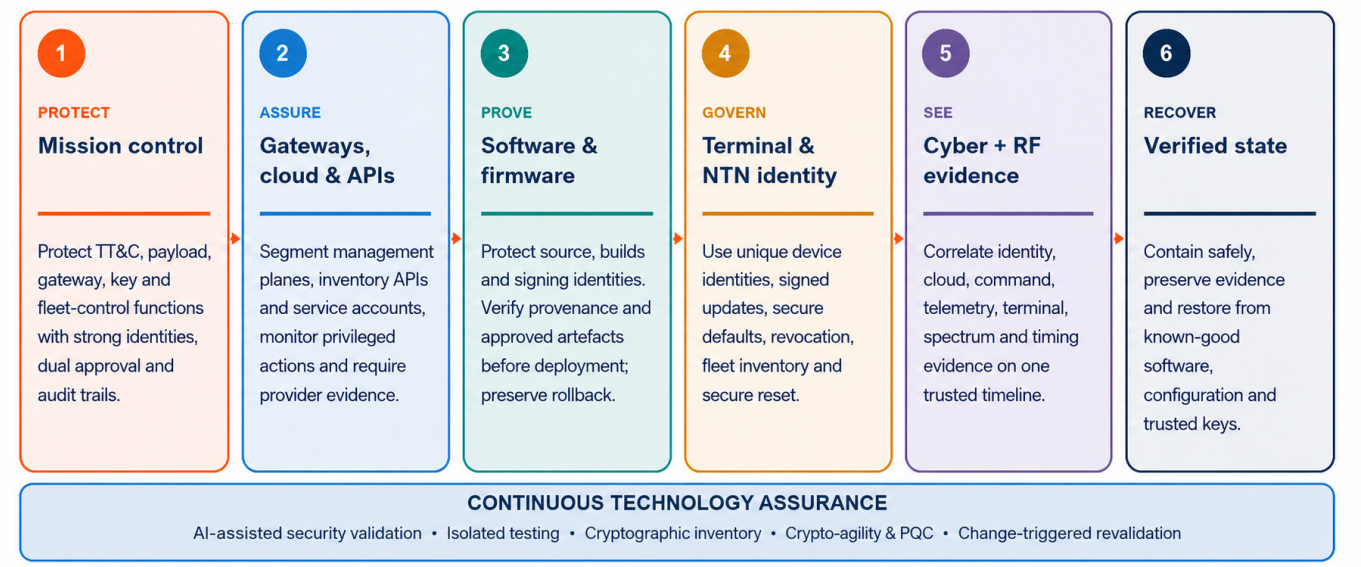

Exhibit ES.1: Six dimensions of continuous technology assurance

1. SATCOM CYBERSECURITY IN INDIA

India increasingly relies on satellite services for telecom backhaul, public services and commercial operations. Control, identity and service delivery are distributed across spacecraft, gateways, software, cloud platforms, suppliers, radio links and terminals.

CONSEQUENCE AND TECHNOLOGY NOVELTY

SatCom combines specialist space systems with familiar enterprise and telecom technology. The novelty lies less in the individual controls than in how a weakness in one component can affect the wider service. A stolen cloud token can alter terminal provisioning; a compromised gateway account can change routing or suppress monitoring; an unsigned update can affect a remote fleet; a stale command accepted after a communications gap can change a mission state; and a radio-frequency event can hide inside what looks like ordinary service degradation.

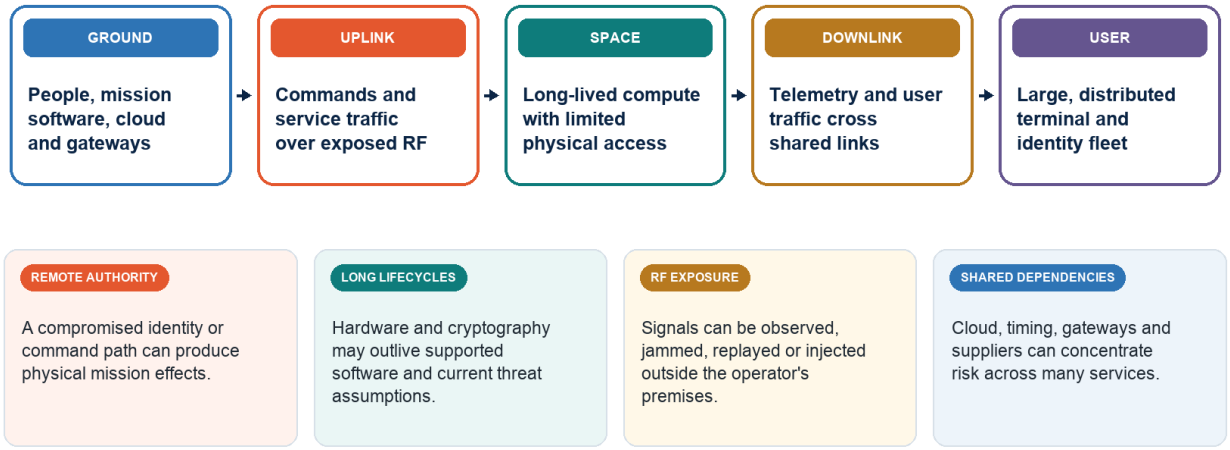

Exhibit 1.1: Why SatCom cybersecurity spans the full service chain

Asset assessment can consider what an asset controls, which services rely on it, who can reach it, and whether a compromise could cross a trust boundary - a point where control or responsibility passes between systems or organisations - rather than whether it looks like 'space technology'. A billing portal and a TT&C workstation may both run commercial software, but they require different assurance because the latter participates in spacecraft control.

FOUR OPERATIONAL DOMAINS OF SATCOM CYBERSECURITY

SatCom combines familiar enterprise, telecom and embedded technologies, but the four domains create different exposure patterns and consequences. Using the same domains throughout the report provides a consistent way to describe the architecture while showing why ordinary cyber weaknesses can produce mission or fleet effects.

Ground. Remote access, cloud consoles, enterprise identities, management APIs and supplier connections create reachable attack paths into high-consequence systems. A stolen token or compromised administrator can alter routing, terminal provisioning, monitoring or command support.

Space. Spacecraft and payload systems are remotely operated, difficult to access physically and expected to remain in service for years. A stale or forged command, vulnerable onboard function or unsafe update can change mission state when repair and rollback options are constrained.

User. Large fleets can turn a weakness in one device into risk across the whole service. Shared credentials, unauthenticated management interfaces, firmware-validation gaps or incomplete inventory can allow one defect or credential compromise to affect many terminals or endpoints.

Interconnect and Cyber-RF. Radio links are exposed by design, and service traffic, commands, telemetry, timing and backhaul cross technical and organisational boundaries. Signals can be observed, jammed, spoofed, replayed or

injected, while shared cloud, gateway and supplier dependencies can propagate effects or obscure their source.

Across the four domains, risk is intensified by remote control, long lifecycles, fleet scale, exposed RF and shared dependencies. These are characteristics of the domains, not additional network elements or a competing architecture.

WHERE CYBER RISK CONCENTRATES IN INDIA'S SATCOM ECOSYSTEM

India's SatCom ecosystem is moving toward closer integration with terrestrial telecom, cloud services, domestic gateways, VSAT fleets and 3GPP NTN. That convergence creates shared control points and concentrates attack paths. Gateways connect orbital and terrestrial infrastructure. Identity services may span operators and providers. Terminal-management systems can reach thousands of devices. Cloud and managed-service platforms can carry delegated operational privileges. RF monitoring and timing inputs shape incident classification.

This report groups gateways, TT&C, identity and key services, software/update pipelines, terminal fleets, cloud/API layers, RF monitoring and backhaul as assets with the potential for high consequences. The grouping is practical rather than legal and does not imply that every listed commercial system has been formally designated as critical infrastructure.

2. END-TO-END ARCHITECTURE, TRUST BOUNDARIES AND CYBER OBLIGATIONS

A SatCom service does not consist of a single asset called the ‘satellite network’. This report groups its components into four operational domains: Ground, Space, User, and Interconnect and Cyber-RF.

Ground contains mission control, TT&C ground facilities, gateways, terrestrial core and cloud systems, operational tooling, identities, keys and supplier access. Space contains the spacecraft, payload, onboard software and cryptography, and onboard command and telemetry functions. User contains terminals, customer networks and IoT/NTN endpoints. Interconnect and Cyber-RF contains the links, backhaul, timing dependencies and organisational or technical hand-offs that connect them.

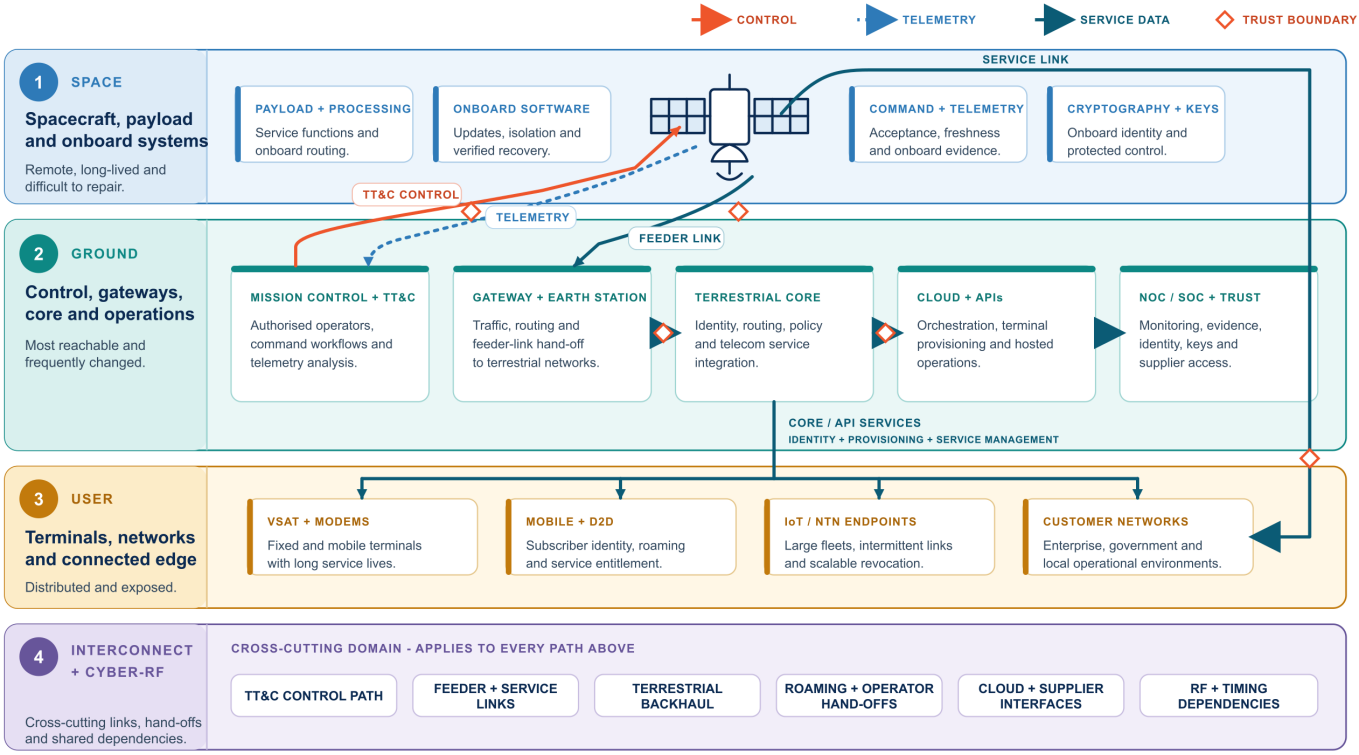

Exhibit 2.1: Four-domain reference architecture of the SatCom service chain

Ownership does not always follow these boundaries. One entity may own a component, another may host it and a third may operate it. Cyber risk therefore often gathers at interfaces, control paths and shared dependencies. These are the points where commands reach the spacecraft, traffic crosses a gateway, devices are set up, identity or key services are reused, and cloud or supplier access touches operations. Architecture maps can show both the domain containing each component and the cross-domain path through which an incident can propagate.

For India, the above architecture view connects SatCom with domestic gateways, telecom backhaul, cloud platforms and 3GPP NTN [2]. The security model described here covers the full service chain: space segment, TT&C/control, ground and gateway infrastructure, terrestrial core and cloud dependencies, user terminals, IoT/NTN endpoints and operator-to-operator hand-offs.

A FOUR-DOMAIN VIEW OF THE SATCOM SERVICE CHAIN

The traditional SatCom model is often described in three segments: space, ground and user. For cybersecurity, this report keeps those three and adds Interconnect and Cyber-RF as a fourth domain covering the links and hand-offs between them. The detailed components fit into the four domains as follows.

Ground. Mission control, TT&C ground stations, NOCs and SOCs, earth stations, satellite gateways, gateway data centres, terrestrial telecom core functions, cloud platforms, orchestration, APIs, identity and key services, and service-management systems.

Space. The spacecraft bus, communications payloads, onboard processing and software, cryptographic components, command-receive functions, telemetry-generation functions and onboard inter-satellite routing functions.

User. VSATs, modems, antennas, satellite phones, fixed and mobile terminals, enterprise and customer networks, 5G NTN devices, low-power IoT, relay nodes and direct-to-device endpoints.

Interconnect and Cyber-RF. TT&C, feeder, service and inter-satellite links; terrestrial backhaul; internet and telecom interconnects; roaming and operator hand-offs; cloud and supplier interfaces; and RF and timing dependencies.

Each domain has different owners, entry points and consequences if it fails, but none operates alone. Architecture maps, control evidence and incident timelines can show both the domain in which an asset sits and the cross-domain paths through which an incident can propagate.

SPACE DOMAIN I SPACECRAFT, PAYLOADS AND ONBOARD SYSTEMS

The Space domain contains the spacecraft platform, communications payload, onboard software, cryptographic modules, telemetry interfaces, power and payload-control functions, and any processing that sits on the satellite. Transparent and regenerative payloads remain design choices within this domain; they change how much security-relevant processing and trust move onboard.

The architecture differs according to whether the payload is transparent or regenerative.

Architecture	What the payload does	Where major network functions sit	Where trust concentrates	Main cyber design concern
Transparent / bent-pipe payload	Acts mainly as an RF relay: filters, amplifies, shifts and forwards signals.	Primarily on the ground, especially gateway and core-network functions.	Gateway, feeder link, terrestrial core and ground control.	Gateway hardening, feeder-link protection, traffic separation, RF availability and TT&C protection.
Regenerative payload	Performs onboard processing such as demodulation, decoding, switching, routing and re-encoding.	Partly onboard the satellite; may place base-station functions in space.	Space segment, onboard software, command path, key management and inter-satellite routing where used.	Onboard software assurance, secure update paths, command validation, payload isolation and verified recovery.
Inter-satellite networking	Enables routing or switching across satellites, generally associated with regenerative capability.	Distributed across constellation nodes and ground control.	Inter-satellite links, routing policies, constellation management and key distribution.	Failure containment, segmentation, route integrity, monitoring and recovery across multiple spacecraft.

Exhibit 2.2: Cybersecurity implications of satellite payload architectures

A transparent, or bent-pipe, payload largely relays signals. It receives, filters, amplifies, frequency-shifts and forwards traffic, while major network functions remain on the ground. A regenerative payload performs more processing onboard. It may demodulate, decode, switch, route, re-encode and modulate traffic, and in 3GPP NTN models it may host base-station functions on the satellite.

This distinction changes the location of security-relevant processing and controls. Transparent payloads leave more security-critical processing in gateways and terrestrial systems. Regenerative payloads move more logic into orbit, placing onboard software assurance, secure updates, key handling and command validation in the spacecraft environment.

Payload type alone does not determine risk. Transparent payload security involves link availability, signal integrity, command protection and gateway security. Regenerative payloads move more security-relevant logic into space,

changing the cyber architecture.

As more processing moves onboard, the spacecraft becomes a more software-dependent and security-critical part of the Space domain.

CROSS-DOMAIN CONTROL PATH I TT&C AND MISSION CONTROL

TT&C carries direct mission-control capability in SatCom.

The service link carries user or network traffic. The TT&C path carries commands, telemetry and control messages that determine whether the spacecraft and payload remain under authorised control. The report analyses these paths separately. A bent-pipe service architecture does not mean user traffic and spacecraft command permissions collapse into the same channel.

TT&C is a control chain across three of the four domains. Mission control, satellite-control centres, TT&C ground stations, operational consoles and command-approval workflows sit in Ground. Onboard command reception, validation and telemetry generation sit in Space. The radio and terrestrial paths carrying commands and telemetry sit in Interconnect and Cyber-RF. NOC and SOC functions may support the chain from Ground, while incident evidence is drawn from all affected domains. Across this chain, three control properties recur:

1. **Command integrity:** acceptance of authorised commands by the spacecraft or payload.
2. **Telemetry trust:** telemetry that supports operator situational awareness.
3. **Operational separation:** isolation or strong segmentation between TT&C/control environments and ordinary IT, user traffic and enterprise systems.

TT&C is therefore a cross-domain mission-control path, not a separate domain. Assurance evidence can follow the command from the authorised operator and ground systems, across the link, to onboard acceptance and telemetry-based confirmation.

GROUND DOMAIN I GATEWAYS AND EARTH STATIONS

A gateway or earth station sends and receives satellite traffic and hands it to terrestrial telecom, internet or private networks. That makes it both a bridge between domains and a concentration point for routing, monitoring and administrative control.

In 3GPP NTN terms, the gateway connects to the satellite payload over the feeder link and connects onward to the core network. In broader SatCom architectures, the gateway or earth station performs the practical hand-off between orbital infrastructure and terrestrial networks, data centres, telecom operators, internet interconnects and customer environments.

That makes the gateway both an enabler and a chokepoint.

It is an enabler because it supports service delivery, traffic routing, monitoring, backhaul and interconnect. It is a chokepoint because gateway compromise or outage can affect multiple downstream services, regions or customers.

Where Indian traffic is expected to traverse domestic gateways, those gateways become concentrated cyber-assurance nodes. Evidence can cover their identity, routing, monitoring, change control and recovery controls.

In transparent NTN architectures, more base-station and control functions sit on the ground, increasing the gateway's importance. In regenerative architectures, the gateway may operate more like a router toward the core. Either way, it is a trust boundary where traffic, control, policy and responsibility converge.

GROUND DOMAIN I TERRESTRIAL CORE, CLOUD AND SERVICE MANAGEMENT

A satellite link is only one part of the delivered service. Terrestrial telecom cores, cloud platforms and operational software may handle identity, routing, provisioning, monitoring and customer access before or after traffic crosses the satellite link.

A modern satellite service may connect into a telecom core, enterprise WAN, government network, internet peering environment, cloud-hosted service platform, orchestration stack, API layer, identity provider, billing system, NOC/SOC platform or managed-service environment. These systems may not be visible to the end user, but they shape

the real security posture of the service.

These terrestrial and cloud systems contain many of the indirect dependencies on which the satellite service relies.

RF-layer protection on a satellite link can coexist with identity-management gaps, exposed APIs, terrestrial-backhaul dependencies, cloud misconfiguration or third-party software exposure. Cloud and core layers can provide monitoring, segmentation, automation and containment functions.

Trust boundary	What crosses the boundary	Why it matters
RF / service-link boundary	User or device traffic enters the satellite system over radio links.	This edge is exposed by design and may face jamming, spoofing, replay, eavesdropping or abuse.
Feeder-link boundary	Gateway traffic moves between earth station and satellite payload.	Feeder-link disruption can degrade service across many users.
TT&C / command boundary	Commands and telemetry move between mission control and spacecraft.	This is the highest-consequence control path.
Payload-to-platform boundary	Communications payload interacts with spacecraft bus and onboard systems.	Payload compromise or misconfiguration should not endanger core platform control.
Gateway-to-core boundary	Satellite traffic enters terrestrial telecom, internet, enterprise or government networks.	This is where SatCom becomes part of terrestrial service delivery and policy enforcement.
Cloud / operations boundary	Hosted systems, APIs, orchestration and analytics support operations.	Cloud or API compromise can affect control, service management or monitoring.
Identity and key-management boundary	Credentials, keys, certificates and authorisation decisions support multiple segments.	Shared identity or key failure can create cross-segment impact.
Operator-to-operator boundary	Satellite operator, gateway provider, telecom operator, cloud provider, vendor or customer exchange responsibilities.	Assurance can fail where ownership and accountability are unclear.
User / customer boundary	Terminals, local networks and customer-managed devices connect into SatCom services.	Weak customer-side controls can become service-side exposure.

Exhibit 2.3: Trust boundaries across the SatCom service chain

USER DOMAIN I TERMINALS AND CONNECTED EQUIPMENT

The User domain contains a wide and heterogeneous set of SatCom components. It contains the terminals and connected equipment through which people, organisations and machines use the service, including VSATs, satellite phones, modems, antennas, customer-premise equipment and customer networks.

It includes VSATs, satellite phones, modems, antennas, fixed terminals, mobile terminals, maritime terminals, IoT gateways, enterprise routers and customer-premise equipment. Some may sit in professionally managed enterprise or government facilities. Others may be deployed in remote locations, vehicles, ships, temporary relief sites, public-service nodes or unattended field environments.

Three characteristics shape user-segment security.

First, the assets are distributed and often outside the operator's physical control. Second, terminals may have long service lives, uneven patching and operational constraints. Third, user devices can become entry points for abuse, denial-of-service, unauthorised access or large-scale compromise.

The user edge is therefore not a footnote. As terminal and NTN populations grow, device identity, update trust, management exposure and revocation become determinants of systemic risk.

USER DOMAIN I IOT AND NTN ENDPOINTS AT SCALE

NTN brings satellite into mainstream telecom architecture. 3GPP Release 17 introduced formal NTN requirements covering terrestrial-satellite service continuity, roaming, low-power massive IoT, satellite backhaul, meshed

connectivity and multi-country regulatory compliance [2]. This means satellite networks are no longer only specialist systems operating beside telecom networks. They are becoming part of the telecom standards environment.

That changes the security model in three ways.

First, mobility and timing become more complex. NTN operation involves large coverage areas, moving beams, propagation delay, Doppler variation and reliance on location, ephemeris and timing information.

Second, device scale increases sharply. Low-power IoT and direct-to-device models can move SatCom from a limited number of specialist terminals to a much larger population of devices.

Third, telecom security arrangements now extend into satellite operations. Identity, roaming, core-network integration, traffic routing, service continuity and cloud-hosted network functions all become part of the SatCom security equation.

As NTN scales, SatCom security overlaps with telecom security, IoT governance, cloud assurance, RF monitoring and critical-infrastructure risk management in India.

Architecture choice	What becomes more exposed	What becomes more dependent	What becomes the chokepoint
Transparent payload	Gateway, feeder link and terrestrial base-station functions.	Ground control, gateway security and terrestrial core.	Gateway-to-core boundary.
Regenerative payload	Onboard software, payload control and inter-satellite logic where used.	Secure command, onboard processing and software assurance.	TT&C/control path and payload-management layer.
Dedicated gateway	Operator-owned gateway environment.	Internal segmentation, access control and secure failover design.	Operator gateway and NOC/SOC.
Shared gateway or hosted antenna service	Multi-tenant interfaces and operator-to-operator hand-offs.	Tenant separation, contractual assurance and third-party monitoring.	Shared gateway provider or hosted-control interface.
On-premises control stack	Local administration, physical access and internal segmentation.	Local containment, patching and access governance.	Mission-control environment.
Cloud-supported control or service management	APIs, hosted platforms and remote administration.	Cloud-provider assurance, identity federation and configuration management.	Cloud operations boundary.
VSAT / relay-node model	Enterprise or site-level terminals and customer-premise equipment.	Terminal lifecycle, field maintenance and customer network segmentation.	Terminal-to-network boundary.
Direct-to-device / IoT NTN	Large-scale endpoints and device identity systems.	Onboarding, revocation, abuse detection and scalable monitoring.	Identity and device-management layer.

Exhibit 2.4: Architecture choices, dependencies and cyber chokepoints

INTERCONNECT AND CYBER-RF DOMAIN I TRUST BOUNDARIES AND HAND-OFFS

A trust boundary is any point where control, responsibility, identity, security context, data, traffic or operational evidence passes between domains, organisations or differently assured systems. These boundaries are where local weaknesses can become cross-domain incidents.

VISIBLE ENTRY POINTS AND HIDDEN DEPENDENCIES

A technical architecture map can separate direct exposure from hidden dependencies.

Direct exposure sits where external actors, devices, signals or administrators can reach the system. Hidden dependencies sit one layer behind the visible interface: identity systems, keys, cloud services, monitoring platforms, vendor access, timing sources and software supply chains.

Direct exposure and hidden dependencies can affect the same service. Service-link protection does not offset key-management weaknesses; gateway hardening does not remove exposure from remote administration; and spacecraft security does not provide cross-segment visibility for the ground SOC.

Chokepoint	Why it concentrates consequence	What should be prioritised
TT&C-to-mission-control chain	It governs positive control over spacecraft and payloads.	Strong command authentication, multi-factor privileged access, command whitelisting, replay resistance, audit trails and emergency recovery.
Gateway-to-core boundary	It is where satellite traffic becomes telecom, internet, enterprise or government traffic.	Segmentation, routing assurance, traffic monitoring, redundancy and gateway hardening.
Identity and key-management systems	They support trust across operators, devices, commands, links and services.	HSM/KMS discipline, least privilege, revocation, lifecycle management and separation of duties.
Monitoring and incident-correlation layer	It determines whether operators can detect cross-segment cyber and RF anomalies.	NOC/SOC integration, RF monitoring, telemetry correlation, log integrity and incident playbooks.
Third-party and hosted-control interfaces	They can connect external organisations into high-consequence operational systems.	Vendor access governance, API security, contractual SLAs, security evidence and shared incident obligations.

Exhibit 2.5: High-consequence chokepoints and associated control areas

DIFFERENT ARCHITECTURES MOVE RISK TO DIFFERENT PLACES

Different SatCom architectures create different cyber priorities. The risk map changes depending on payload design, gateway model, control model and endpoint scale.

Control emphasis varies across a managed VSAT backhaul network, a regenerative LEO constellation, a shared gateway model and a direct-to-device NTN service.

INDIA'S GATEWAYS, CONTROL PATHS AND TELECOM INTEGRATION

This architecture affects the distribution of assurance responsibilities among Indian policymakers and operators.

First, domestic traffic concentration gives gateways a national cybersecurity role. Relevant control areas include gateway identity, routing, monitoring, privileged access, software integrity and clean restoration.

Second, TT&C and mission control have a different assurance profile from user traffic because the command path forms a specialised control domain.

Third, SatCom and telecom security overlap. NTN, satellite backhaul and gateway-to-core integration mean SatCom risk now overlaps with telecom-core, cloud, API, identity and device-security risk.

Fourth, user terminals and IoT devices introduce security considerations at fleet scale. Terminal fleets and NTN devices expand the edge beyond tightly controlled operator environments.

Fifth, RF and cyber monitoring provide complementary evidence. Jamming, spoofing, interference, anomalous traffic, gateway failure and cyber intrusion can present as overlapping events, creating hybrid cases that may not appear in a single evidence stream.

Sixth, dependency mapping can be represented through live inventories of assets, owners, third-party dependencies, software and firmware components, identity systems, key-management systems, cloud services, backhaul routes and monitoring capabilities.

CYBER OBLIGATIONS, OPERATIONAL CONTROLS AND EVIDENCE

This report focuses on the cyber-relevant parts of India's set of applicable policies and rules: security ownership, applicable baselines, specified evidence, incident-reporting timelines, and the public authorities or providers involved in investigation and recovery.

CERT-IN'S 2026 FRAMEWORK PROVIDES THE END-TO-END INDIAN BASELINE

CERT-In's Cyber Security Framework and Guidelines for Space including Satellite Communication covers space, ground, communication links and user systems [8]. That structure maps directly to this report's four domains: Space, Ground, Interconnect and Cyber-RF, and User. The framework connects security ownership, risk assessment, access

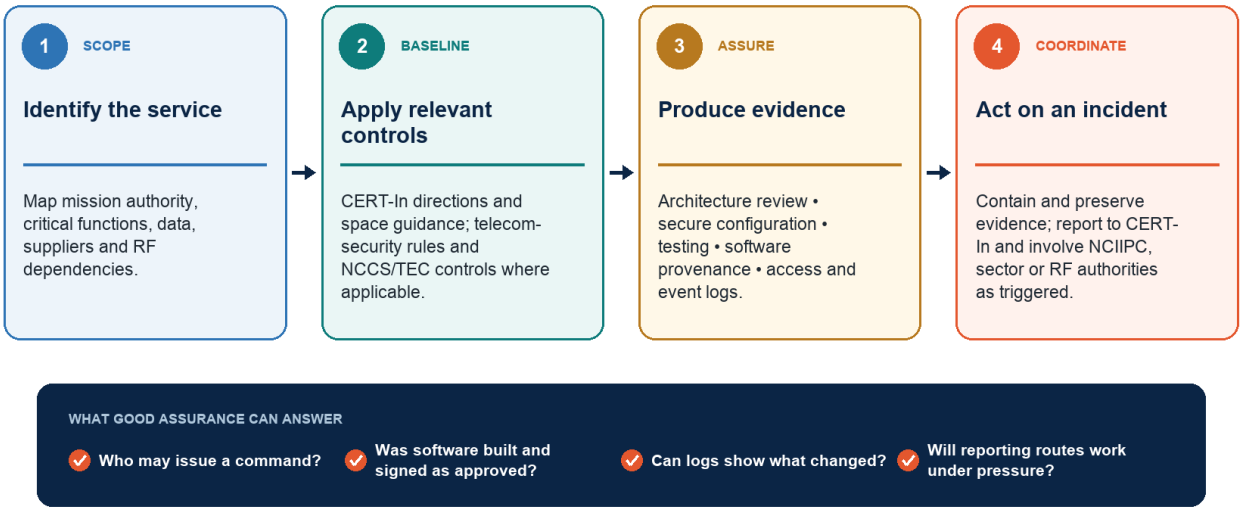

Exhibit 2.6: From service scope to coordinated assurance

control, key management, supply-chain assurance, monitoring, incident response and audit across those domains, providing a technical reference point for operators and assessors.

The framework does not erase other duties [6, 21, 22, 23, 27, 28]. A telecom entity may also be subject to telecom cyber rules; a reportable cyber incident may trigger CERT-In's 2022 Directions; a notified CTI asset may have additional requirements; and a space-authorisation condition may apply when satellite control or an authorised activity is affected. The same underlying controls can support several duties, but one incident may still trigger multiple reporting and evidence obligations.

OVERLAPPING INCIDENT-REPORTING DEADLINES

CERT-In's 2022 Directions require specified incidents to be reported within six hours of noticing them and require a point of contact, time synchronisation and log retention [6]. Telecom cyber rules establish a six-hour reporting path to the Central Government for telecom security incidents, while notified CTI can carry a shorter intimation requirement [21, 22]. An incident playbook can record which reporting deadline applies to each event type.

A SatCom playbook can map event type, affected asset, entity status, reporting trigger, accountable executive, evidence owner and update cadence. An event can be initially reported on known facts while technical classification continues. A common evidence pack can support overlapping reports and reduce conflicting narratives.

AUTHORISATION RECORDS AS SECURITY EVIDENCE

IN-SPACe processes request security-relevant information such as encryption, data-security mechanisms, TT&C arrangements and network flows. Those documents and records can support security checks if they are kept current and tested. General licensing, market-entry and spectrum-assignment mechanics are outside this report except where they create a cyber control point or an incident coordination duty.

TEC and NCCS provide a visible equipment and telecom security assurance path. SatCom assurance profiles can cover terminal management, gateway software, update signing, remote administration, RF-monitoring integration, cryptographic modules, software-defined functions and evidence export. Certification and operator configuration review, vulnerability management and lifecycle support provide different forms of evidence.

ASSURANCE EVIDENCE FOR REVIEW AND INCIDENT ANALYSIS

For decision-makers, assurance evidence can support review before an incident and analysis during one. The evidence set described in this report includes:

- Architecture and control-rights map showing trust boundaries, owners and privileged paths.
- Asset, identity, key, software/firmware and supplier inventories tied to consequence.
- Test results for segmentation, authentication, anti-replay, update verification, logging, revocation and clean restore.
- Provider contracts that guarantee notification, audit logs, vulnerability handling and investigation support.
- A cross-domain incident pack covering cyber, RF, gateway, cloud, terminal and timing evidence.

3. GROUND-SEGMENT CYBERSECURITY

Ground systems are where satellite services meet ordinary digital infrastructure [17, 33, 44]. Remote interfaces make them more reachable than spacecraft, while gateways and privileged administration can create effects across services or regions. A compromise may begin here and propagate through the user, space or interconnect/Cyber-RF domains, so assurance evidence can be organised by an interface's control capability and the consequence its failure can create.

Ground-asset and interface assessment covers five linked attributes: control capability, reachability, safeguard failure, propagation paths, and effects on mission functions, services or user populations across confidentiality, integrity, availability and control.

GROUND-SEGMENT EXPOSURE MAPPING

The report separates ground-segment exposure into how the service can be reached, how an effect can spread and what the resulting harm would be. The three layers are:

- **Direct exposure and control capability -** radio links, gateways, terminals, remote access, identities and APIs where external signals, users or administrators touch the service and can cause consequential actions.
- **Propagation paths and critical dependencies -** identity, keys, cloud, backhaul, RF monitoring, timing, suppliers and management systems through which a local failure can reach other assets, fleets, regions or partner networks.
- **Consequence -** the people, regions, services or mission functions that lose confidentiality, integrity, availability or control when an exposed interface or dependency fails.

NIST's hybrid satellite profile frames satellite systems as combinations of independently owned and operated components, with emphasis on interfaces between participants [5, 34]. NIST IR 8401 focuses on the ground segment and command-and-control environment [33]. CERT-In's 2026 framework provides the India baseline by treating space, ground, communication links and user terminals as connected parts of one security problem [8].

WHERE ATTACKERS AND FAILURES CAN FIRST REACH THE SERVICE

Direct exposure means that an outside signal, user, device or administrator can reach the service without first crossing the operator's most trusted environment. Five recurring exposure groups are communication links, TT&C/control, gateways, user terminals and remote administration.

GATEWAYS AND EARTH STATIONS: A BRIDGE AND A CONCENTRATION POINT

A gateway or earth station receives and transmits satellite traffic, then connects it to terrestrial networks and operations. Because routing, monitoring, provisioning and privileged access can converge there, a local gateway weakness can create effects far beyond the site itself.

A gateway may terminate feeder links, hand traffic into telecom or internet infrastructure, host monitoring systems, enable service management and connect to NOC/SOC workflows. For India, domestic gateway expectations connect these nodes to routing and cyber assurance. Exposure mapping can cover their administrative paths, software, keys, routing controls, monitoring feeds, remote support and recovery dependencies.

INCIDENT I KA-SAT, 24 FEBRUARY 2022 — THE ENTRY PATH WAS TERRESTRIAL

Reported that an attacker exploited a misconfigured VPN appliance, moved laterally through a trusted management segment and issued legitimate management commands against residential modems [13, 29, 47]. Several thousand users in Ukraine and tens of thousands elsewhere in Europe lost service.

Observed implication - A terrestrial management compromise can create satellite-scale and fleet-wide effects without compromising the spacecraft. The hand-off between gateway and terminal control is the trust boundary; related controls include segmentation, privileged-access governance, management-command safeguards and recovery capacity.

Sources: incident overview (2022); Council of the European Union attribution (2022) [13, 47]

REMOTE ADMINISTRATION AND APIS: ACCESS WITH SYSTEM-WIDE CONSEQUENCES

Remote administration allows operators, suppliers or service providers to manage systems without being physically present. The same access path can give a compromised account, API or support channel the reach of an authorised administrator.

Not every SatCom architecture uses cloud-hosted control or third-party orchestration. The exposure map can distinguish architectures that do not use these services from those in which APIs, hosted operations, virtualised payload control, managed service platforms, vendor access or cloud dashboards form part of the SatCom attack surface.

NIST IR 8441 is relevant here because it explicitly models hybrid satellite environments with independently owned, leased, hosted or virtualised components and focuses on interfaces between participants [34]. It also notes that these components may not all have the same level of security assurance.

CLOUD AND GROUND-STATION-AS-A-SERVICE: PROVIDER CONTROL AND SHARED RESPONSIBILITY

Cloud and Ground-Station-as-a-Service allow an external platform or provider to perform functions that once sat inside an operator's own facilities. The cyber question is therefore not whether a service is called 'cloud'. It is what operational privileges have been delegated. Telemetry storage, antenna scheduling, pass planning, command formatting, command release and mission control carry progressively greater consequence. A provider that can schedule an antenna is not equivalent to one that can form or transmit commands.

The UK government's 2025 analysis of cloud risks in the space ground segment highlights shared-responsibility, supply-chain and service-dependency concerns [18]. The control set described in that analysis includes tenant isolation, per-workload identities, short-lived credentials, complete API inventories, dual approval for command-affecting actions, rapid revocation, customer-accessible logs and contractually specified incident evidence.

HIDDEN DEPENDENCIES: SUPPORTING SYSTEMS THAT CAN SPREAD FAILURE

Some consequential SatCom exposures arise from dependencies shared by several segments rather than from visible interfaces. Identity, keys, cloud services, backhaul, RF monitoring and timing support can affect several parts of the service. ENISA's 2025 space threat landscape examines the satellite lifecycle and stakeholders rather than only one technical layer [25]. NIST IR 8441 similarly stresses ownership, hosting and participant interfaces. Together with CERT-In's segment-wise controls, these sources support a dependency-led view of SatCom cyber risk.

IDENTITY AND PRIVILEGED ACCESS: WHO CAN MAKE CONSEQUENTIAL CHANGES

Identity controls determine which people, devices and software services can act - and with what privilege. Because the same identity platform or account can reach several parts of a SatCom service, identity is effectively a shared control plane for operations, meaning that one compromised identity can affect several parts of the service.

Operator accounts, vendor accounts, administrator roles, device identities, cloud identities, API tokens, emergency credentials and customer access can all become cross-segment dependencies. CERT-In explicitly calls for role-based access control, privileged-access logging, credential revocation, MFA for privileged and remote access, and identity management for user devices accessing satellite networks [8].

The exposure map can record access identities, applicable conditions, privilege levels and revocation time for high-consequence systems.

ZERO TRUST FOR MISSION OPERATIONS: VERIFICATION OF HIGH-IMPACT ACTIONS

Zero trust in mission operations means that no user, workload, provider or device is trusted merely because it is on an internal network [15, 43]. In this model, access is limited to specific resources and sessions, linked to the person's role and the device's security state, and re-evaluated when risk changes.

Controls associated with high-consequence resources include phishing-resistant MFA, privileged-access workstations, just-in-time roles, service-to-service authentication, segmented command-support environments and immutable audit evidence. Emergency-access arrangements can include time limits, independent approval and post-use review.

KEY MANAGEMENT: PROTECTING COMMANDS, UPDATES, IDENTITIES AND DATA

Cryptographic keys are the digital credentials behind trusted commands, device identities, encrypted links and signed software. If a key is stolen, misused or cannot be revoked, the associated encryption or authentication control can fail.

Telecommands, telemetry, device identity, secure updates, encrypted traffic, APIs, VPNs, software signing and stored data may all depend on cryptographic key material. CERT-In describes key-management systems in terms of isolation, auditability and resilience to compromise, and links key lifecycle management to generation, distribution, rotation, revocation and emergency recovery [8, 12].

The dependency map can extend beyond the presence of encryption to record where keys are generated and stored, who can use them, when they rotate, how compromise is detected, how emergency revocation works, and which systems fail if the key-management service is unavailable.

ACCOUNTABILITY ACROSS OPERATORS, PROVIDERS AND SUPPLIERS

SatCom exposure is often multi-actor. A single service may involve a satellite operator, gateway provider, telecom operator, cloud provider, terminal vendor, managed-service provider, customer and government agency.

The exposure map can record the asset and interface together with the owner, operator, security owner, incident owner and evidence owner. This ownership information is relevant to hybrid satellite models, where NIST notes that independently owned and operated components may have varying levels of assurance [34].

EXPOSURE RANKING BY OPERATIONAL CONSEQUENCE

An exposure map can rank risks rather than present a flat list. The ranking in this report uses six questions:

- **Centrality:** How many services, users or regions depend on this asset or dependency?
- **Privilege:** Does it carry command capability, administrative privilege, keys or policy control?
- **Substitutability:** Is there an alternate route, gateway, terminal fleet, provider or recovery mode?
- **Observability:** Can the operator detect failure or compromise quickly?
- **Recoverability:** Can the asset or dependency be restored without unsafe side effects?
- **Mission consequence:** Does the affected service support public services, disaster response, border/island connectivity, telecom backhaul or government users?

The same technical interface can carry very different consequences depending on the actions it can perform and the services that depend on it. Assurance levels can reflect that consequence rather than a broad policy label.

THE EXPOSURE MODEL IN INDIA

For India, four operating realities described in earlier sections shape the exposure map.

First, gateways differ from ordinary network nodes because they combine privileged access, routing, monitoring and service concentration. These properties connect them to exposure mapping, independent assurance and incident readiness.

Second, existing rules and institutions reach ground infrastructure. Telecom-side rules, CERT-In reporting, CTI pathways, TEC/NCCS-style assurance and operator SOC/NOC capabilities apply to gateways, interconnects, terminals, service platforms and control environments.

Third, service consequences vary by service context. Public safety, essential backhaul, government operations and other high-dependency uses have different assurance profiles from routine connectivity.

Fourth, Cyber-RF monitoring connects regular cyber operations with spectrum evidence. WPC, operators, CERT-In, DoT and other entities may become involved when cyber events and RF interference overlap. The exposure map can include cyber logs, spectrum events, interference records and RF-monitoring coverage.

This distinction separates exposure, a possible point of contact, from a threat, which combines an exploitable condition with an actor capable of using it. A service link is an exposure point; jamming or spoofing turns it into a threat scenario. A gateway is an exposure point; segmentation gaps or privileged-account compromise create a vulnerability pathway. A key-management system is a dependency; custody gaps or inability to revoke keys can create system-wide risk.

ILLUSTRATIVE SCENARIOS

Gateway compromise and traffic disruption

The gateway is one of the most consequential points in India's SatCom security model. It is where satellite traffic enters terrestrial networks and where routing, monitoring, provisioning and administrative privileges converge.

How the scenario unfolds

A SatCom service provider operates an Indian satellite gateway supporting enterprise broadband, telecom backhaul, public-service links and emergency capacity. The gateway connects satellite feeder-link systems to terrestrial telecom infrastructure, service-management platforms, monitoring tools and operator access systems.

A threat actor gains access to the gateway administration environment through a compromised privileged account, vendor-support path, vulnerable management interface, or adjacent ground IT system. The initial access does not immediately affect the satellite. Instead, the actor targets the terrestrial side of the gateway: routing policies, service segmentation, logging, monitoring feeds or provisioning rules.

At first, the incident appears as intermittent degradation: some regions see packet loss, some customer sites lose connectivity, and some monitoring dashboards show inconsistent telemetry. Over time, the actor's changes create broader disruption or traffic-handling uncertainty. The operator's NOC sees a service issue; the SOC sees unusual administrative activity; the RF team sees no obvious satellite-link problem. The incident becomes a cross-domain investigation.

Potential mitigation

Gateway assurance should go beyond routine enterprise hardening - include independent testing, strong segmentation, route and configuration validation, RF-cyber correlation, privileged-access governance, incident reporting & restoration.

Ground IT intrusion near TT&C support systems

TT&C is the mission-control path for a satellite mission. Not every cyber incident near a mission operator creates spacecraft-control risk, but any intrusion that moves toward TT&C support systems deserves elevated treatment.

The practical risk here sits in systems supporting command preparation, telemetry analysis, operator access and recovery—not in a cinematic 'satellite hack'.

How the scenario unfolds

An attacker compromises the operator's enterprise IT through a routine business system. TT&C is not directly affected, but the actor looks for mission-support pathways such as engineering workstations, configuration tools, telemetry dashboards, vendor access or shared identity services.

Even without command access, those systems can reveal procedures, roles, maintenance windows or emergency contacts. Weak segmentation or shared identity may then let the actor move toward control support, reuse credentials or abuse stale accounts.

The SOC sees unusual document access, failed mission-support logins and abnormal account behaviour. The mission team sees no anomalous commands but must determine whether command capability, telemetry trust or operator confidence could be affected.

Potential Mitigation

Escalation tiers: a routine operator IT incident is not automatically a TT&C incident, but compromise of command preparation, telemetry validation, payload configuration or emergency-recovery support should trigger higher assurance and reporting.

Cloud-hosted service-management compromise

SatCom operators may use cloud platforms for provisioning, monitoring, orchestration, identity and NOC/SOC support. Even when mission control remains separate, cloud-linked operations are part of the SatCom security model.

How the scenario unfolds

A SatCom operator uses a cloud service-management platform to provision terminals, apply policy, monitor service health and support customers. It connects to identity services, APIs, logging and customer portals.

An actor compromises an administrator, API token, service account or misconfigured resource, then changes provisioning, suppresses alerts, creates hidden accounts or disrupts customer management.

The satellite, TT&C and RF links remain operational, but users lose service, terminals receive incorrect configurations and logs become incomplete. The operator must distinguish malicious abuse from misconfiguration, supplier failure or internal error.

Potential Mitigation

Cloud contracts should map operational touchpoints and guarantee notification, retained logs, evidence access and recovery support.

Exhibit 3.1: Illustrative compromise paths in ground and cloud operations

4. SPACE-SEGMENT CYBERSECURITY

Spacecraft are difficult to reach physically, but command, telemetry, payload-management and software-update paths carry high-consequence control capability. A mistake or compromise in any of them can affect the whole mission, and a weakness originating in the ground, supplier or RF chain can propagate onboard. TT&C functions as the mission-control path rather than an ordinary network. Its assurance evidence covers access control, command authenticity and freshness, replay handling and potential mission effects.

TT&C: HOW OPERATORS OBSERVE AND CONTROL A SPACECRAFT

Telemetry, tracking and command (TT&C) carries the mission-control capability. It is the path through which operators observe the spacecraft, issue commands, perform diagnostics and recover from faults.

The control objective concerns acceptance of authenticated, authorised and fresh commands; trustworthy telemetry; and governance of keys, approvals and emergency access [10, 11, 14, 37].

Assurance across the command chain includes operator identities, workstations, approval workflows, command signing, telemetry validation, change windows, vendor access and audit evidence, in addition to the radio link.

COMMAND AUTHENTICATION, FRESHNESS AND RECOVERY

CCSDS Space Data Link Security (SDLS) defines managed security associations for protecting space data-link frames [10, 11, 12]. Message-order tracking or a limited acceptance window distinguishes an old but previously valid message from a new command.

Acceptance-test coverage can include security-association and key rollover, counter exhaustion, resynchronisation after long communications gaps, loss of state, emergency procedures and rejected-frame logging. Recovery-mode evidence can also show whether the command path changes to unauthenticated control.

NASA guidance reinforces the operating layer: unique identities, least privilege, segmented command environments, cryptographic verification, command approvals, time-based checks, deliberate delays where appropriate, revalidation and complete logging [36, 37].

SPACECRAFT AND GROUND LOGS AS COMPLEMENTARY EVIDENCE

Ground logs provide one part of the evidence for a spacecraft event. Spacecraft security telemetry can include failed authentication, stale or out-of-window frames, unexpected software or configuration changes, internal-bus anomalies, fault-management bypass and commands inconsistent with mission phase. Its design is constrained by bandwidth and by exposure to spoofing or suppression.

CONTROLLED RESEARCH DEMONSTRATION | ESA OPS-SAT, 2023

Under ESA supervision, Thales researchers uploaded deliberately vulnerable software to the experimental OPS-SAT spacecraft, obtained access to the control layer, altered an image and changed the satellite's attitude [24]. ESA then restored the system to a safe state.

Scope - This was an authorised exercise on a unique experimental platform, not an operational mission compromise. The demonstration generated evidence on onboard isolation, signed software, command authorisation, telemetry trust and safe-state procedures in a realistic system.

Source: ESA in-orbit cybersecurity demonstration (2023) [24]

ILLUSTRATIVE SCENARIO

Payload configuration integrity failure

Software-defined and regenerative payloads move routing, switching and beam-management functions into orbit. This flexibility changes the effects associated with command-governance gaps, configuration errors and compromised management paths.

How the scenario unfolds

An operator uses a payload-management interface to change coverage, capacity, routing or other service parameters. The spacecraft remains under authorised control, but a trusted path is misused or misconfigured—maliciously, accidentally, by an insider or through a supplier.

The result is a service-impacting change: a misshaped beam, capacity moved away from a high-dependency region, or degraded NTN/backhaul routing. Because the action may resemble routine maintenance or capacity management, initial evidence may classify it as an operational change.

Potential Mitigation

Approval controls, configuration history and onboard evidence can distinguish error from malicious action and support rollback without losing authorised control of the spacecraft.

Exhibit 4.1: Illustrative scenario: payload configuration integrity failure

5. USER-SEGMENT CYBERSECURITY

Terminals are numerous, diverse and often outside operator-controlled facilities. Their risk depends on who can reach the management, identity or update path, what control that path provides over devices and how far a local action can propagate. A weakness with limited device-level effects can produce system-wide effects when repeated across a fleet or concentrated on high-dependency sites.

TERMINALS AND NTN ENDPOINTS: DISTRIBUTED-EDGE GOVERNANCE

The user segment contains a large and heterogeneous direct exposure surface. A terminal is the equipment that connects a site, vehicle, phone or device to the satellite service; an NTN endpoint extends that role into telecom and IoT environments.

CERT-In's user segment includes terminals, modems, antennas, fixed or mobile devices, satellite phones, IoT gateways and related hardware or software. 3GPP NTN expands the exposure model further by supporting satellite access by user equipment, relay devices, low-power massive IoT equipment and satellite backhaul use cases [8].

Terminals can distribute exposure across a fleet. A single device may have limited consequence, while shared APIs, administration, identity or update paths can propagate one weakness across multiple devices. Public disclosures document terminal-management and device-identity exposure; incomplete fleet inventories, shared or default credentials, outdated firmware, unrevoked credentials, unverified local integration, physical tampering and limited field visibility can extend that exposure [16].

EVIDENCE I KA-SAT — A MANAGEMENT COMPROMISE BECAME A FLEET-RECOVERY PROBLEM

Reported that destructive commands overwrote key data in modem flash memory. The devices were recoverable by factory reset, but the company shipped nearly 30,000 replacement modems to distributors to accelerate restoration.

Operational context — Fleet security forms part of operational continuity. Inventory, remote isolation, trusted reset, signed recovery, replacement logistics and service sequencing affect the time required to contain a terminal incident.

Source: Incident overview (2022) [29, 47]

PUBLIC VULNERABILITY DISCLOSURE I CISA IDIRECT TERMINALS, 2 JULY 2026

CISA disclosed vulnerabilities affecting several iDirect terminal families [16]. CVE-2026-38059 could allow an unauthenticated actor with network access to retrieve device identifiers, including values used in satellite authentication; CVE-2026-38057 could allow cross-site request forgery, a browser-based trick that could reboot a terminal when an authenticated administrator visits a malicious page. CISA reported no known public exploitation and identified fixed firmware.

Operational context — Terminal security involves management-plane authentication, browser-safe administration, protected device identity, firmware support and fleet inventory. A terminal reboot is a link event; leaked authentication-related identifiers can also support reconnaissance or impersonation attempts.

Sources: CISA advisory ICSA-26-183-01; NVD CVE-2026-38059 [16].

TERMINAL ONBOARDING CONTROL SET

The minimum controls associated with terminal or NTN-endpoint onboarding include: [26, 40, 42].

- Unique device identity and administration credentials; replaceable factory defaults and no shared credentials.
- Authenticated management and API endpoints, CSRF protection, least-privilege roles and auditable remote support.
- Cryptographically signed firmware and configuration, protection against installing older software, verified boot where feasible and a protected reset path.
- Fleet inventory tied to owner, location, hardware, firmware, certificate/key state, support status and service consequence.
- Remote isolation and revocation, staged updates, offline recovery instructions, field replacement capacity and vulnerability-disclosure commitments.

PRIORITIES FOR TERMINAL AND NTN SECURITY IN INDIA

India's terminal-security programme should turn those minimum controls into operational priorities for operators, suppliers and high-dependency users:

- **Secure-by-default terminals.** Unique device identity, strong administration, signed firmware and protected recovery should be enabled before deployment.
- **Fleet visibility and revocation.** Operators should know where every terminal is, who owns it, what it runs and how quickly it can be isolated or replaced.
- **Consequence-based service tiers.** Terminals supporting disaster response, public services, border/island links or critical backhaul need stronger monitoring and recovery obligations.
- **NTN identity and abuse controls.** Onboarding, SIM/eSIM trust, roaming, rate limits, telemetry authenticity and anomaly detection must scale with the device population.
- **Field recovery capacity.** Contracts and operating plans should cover secure resets, replacement logistics, offline validation and evidence capture in remote locations.

ILLUSTRATIVE SCENARIOS I NTN/IOT IDENTITY ABUSE AT SCALE`

Terminal fleet compromise at scale

User terminals are the most distributed part of the SatCom architecture. They sit in remote facilities, field sites, vehicles, ships, enterprise networks, temporary locations and customer premises. NTN can extend the edge into IoT and direct-to-device environments.

The scenario asks whether an operator can identify, isolate and restore the right devices before a terminal-management or firmware event becomes a fleet incident.

How the scenario unfolds

A SatCom operator maintains a diverse fleet of VSATs and customer terminals supporting enterprise access, telecom backhaul, public services and emergency capacity. Hardware versions, firmware state, installers, ownership and field conditions vary.

A threat actor compromises a terminal-management system, firmware update path, provisioning process or supplier component. The actor does not need to affect every terminal. It selectively targets terminals serving high-dependency sites or creates a wider failure pattern that overwhelms support and field replacement capacity.

Some terminals stop authenticating. Others show abnormal traffic patterns. Some remain online but do not pass traffic reliably. The incident affects service continuity and creates operational uncertainty.

Potential Mitigation

Terminal security should be a core part of SatCom assurance. A secure gateway cannot compensate for an ungoverned terminal fleet, especially where one management plane or update path can reach many devices.

NTN/IoT identity abuse at scale

NTN changes the scale of SatCom security. Traditional SatCom services often involved specialist terminals and managed deployments. NTN and IoT can increase the number of endpoints, roaming relationships, low-power devices and service-continuity flows.

How the scenario unfolds

An NTN-enabled service supports low-power IoT devices across agriculture, logistics, maritime monitoring and remote infrastructure. Devices attach through satellite coverage where terrestrial networks are unavailable or intermittent. The service relies on device identity, onboarding, certificates, SIM/eSIM credentials, roaming policy and network-level abuse detection.

A threat actor identifies weak onboarding or compromised device identities. Instead of compromising the satellite, the actor abuses the device layer: cloned credentials, unauthorised devices, abnormal signalling, fake telemetry, excessive connection attempts or traffic patterns designed to consume resources.

The first signs are operational: unusual device growth, abnormal attach attempts, signalling load, geographic anomalies, false telemetry and customer complaints. If the operator lacks device inventory and behaviour baselines, the incident may appear as congestion or poor coverage rather than abuse.

Related controls

NTN security should include device lifecycle governance from the start: onboarding, identity, updateability, revocation, telemetry integrity and abuse detection.

Exhibit 5.1: Illustrative terminal and NTN identity-abuse scenarios

6. INTERCONNECT AND CYBER-RF SECURITY

Service links, feeder links, backhaul, cloud, APIs, timing and supplier hand-offs connect the other three domains. These interfaces carry trust, operational control and evidence across system and organisational boundaries; a local failure can therefore propagate into a gateway, command chain, fleet, beam, region or partner network. They are also points where RF and cyber symptoms can overlap.

Public evidence shows a recurring pattern: attackers often exploit hand-offs between systems [4, 13, 16, 24, 29, 47, 48]. Operational incidents show terrestrial management and terminal fleets producing wide effects; vulnerability disclosures expose terminal APIs and administration; controlled research demonstrates RF injection, update-verification gaps and on-orbit software consequences; and measurement studies show that link confidentiality cannot be assumed. Taken together, this evidence links interface assurance to authentication, authorisation, freshness, segmentation, update trust, confidentiality and monitoring.

SERVICE AND FEEDER LINKS: HOW TRAFFIC REACHES USERS AND GATEWAYS

The service link connects the payload to user equipment; the feeder link connects the payload to a gateway. In NTN, these links also support roaming, service continuity, low-power IoT and satellite backhaul.

Link assessment can consider purpose, footprint, user population, authentication, monitoring and consequence. A consumer broadband beam, a feeder link and an emergency-response terminal do not carry the same risk.

CERT-In treats communication links as a distinct layer of SatCom architecture, including RF links, ground-to-ground backhaul, satellite payload links, cross-domain transports and multiplexed terrestrial links used for telemetry or operator access [8]. Its stated security objectives for these links include availability, confidentiality, integrity, authenticity, auditability, timeliness and continuity.

PEER-REVIEWED MEASUREMENT | COMMERCIAL GEO DOWNLINKS, ACM CCS 2025

Researchers passively examined 411 transponders across 39 geostationary satellites and reported sensitive cleartext traffic, including mobile backhaul, credentials and operational or industrial data [48]. The study observed downlinks and did not compromise satellites; its results describe the sampled services and direction of transmission rather than every SatCom service.

Observed implication — Radio-link content can be observable when end-to-end confidentiality is absent. Encryption of only one transport segment, or reliance on obscurity at the satellite layer, can leave user, enterprise or operational data exposed.

Source: Zhang et al. (2025) [48].

SUPPORTING SYSTEMS THAT CONNECT CYBER AND RF RISK

Supporting dependencies shared by several segments can create SatCom exposure independently of interface visibility.

Identity, keys, cloud services, backhaul, RF monitoring and timing support provide shared security functions across the service. Their failure can affect protection across the service chain.

ENISA's 2025 space threat landscape examines the satellite lifecycle and stakeholders rather than only one technical layer [25]. NIST IR 8441 similarly stresses ownership, hosting and participant interfaces. Together with CERT-In's segment-wise controls, these sources support a dependency-led view of SatCom cyber risk.

CLOUD AND HOSTED SERVICES: VISIBILITY INTO SHARED RESPONSIBILITY

Cloud and hosted services can provide scale, analytics, monitoring and automation for SatCom operations. They also divide security responsibility between the operator and provider, so the operator may depend on someone else for logs, configuration evidence, identity controls and recovery support.

Cloud dependencies may include service management, telemetry analytics, customer provisioning, virtualised network functions, orchestration, identity federation, SOC tooling, storage, DevSecOps pipelines and vendor support. Cloud exposure depends on the operator's visibility into and governance of the full dependency chain, including API permissions, tenant separation, configuration changes, logging, provider assurance, data location, incident access

and fallback operations.

NIST's zero-trust architecture guidance rejects implicit trust based only on network location and instead requires continuous evaluation of users, assets and services [43]. This principle applies to SatCom environments that increasingly involve cloud-linked operations, software-defined functions and remote administration.

TERRESTRIAL BACKHAUL: SATELLITE SERVICE CAN FAIL OFF THE SATELLITE

A satellite can remain healthy while the service fails on the ground. Terrestrial backhaul carries traffic between the gateway and telecom, internet or private networks, so routing, fibre, peering or cloud-region failures can interrupt a satellite service without any problem in orbit.

The gateway may be healthy and the satellite may be functional, but the service can still degrade because of backhaul outage, routing failure, congestion, fibre cut, cloud-region dependency, upstream telecom issue or peering problem. CERT-In treats ground-to-ground backhaul from the satellite gateway to the core network as part of the communications-link layer.

Backhaul can be represented as a dependency in the service map. For high-consequence SatCom use cases, relevant attributes include primary and alternate terrestrial routes, provider dependencies, failover design, latency constraints, monitoring feeds, service-level commitments and crisis-routing options.

RF MONITORING: DISTINGUISHING INTERFERENCE FROM CYBER COMPROMISE

Radio-frequency (RF) monitoring shows what is happening in the signal environment. It provides evidence for distinguishing interference, jamming or spoofing from cyber compromise, equipment failure, weather, backhaul problems or configuration error.

A SatCom outage may be caused by equipment failure, cyber compromise, terrestrial backhaul failure, jamming, spoofing, interference, weather or misconfiguration. Without RF monitoring, an operator may not know which category it is seeing. CERT-In calls for spectrum planning and real-time spectrum monitoring to detect interference and treats jamming, spoofing, replay and signal hijacking as link-layer threats.

The dependency map can include RF sensors, monitoring coverage, baseline signal behaviour, interference thresholds, escalation paths, geolocation support, WPC/operator coordination routes and correlation between RF events and SOC/NOC telemetry.

TIMING, LOCATION AND EPHEMERIS: DATA SUPPORTING NTN SYNCHRONISATION

Non-terrestrial networks depend on accurate clocks, location data and ephemeris—information that predicts where a satellite will be. If those inputs are wrong or manipulated, synchronisation, beam selection, roaming, handover and incident timelines can all be affected.

3GPP notes that NTN involves large coverage areas, moving satellite beams, propagation delay, Doppler variation, UE location support, ephemeris information and timing/frequency pre-compensation [2]. It also includes regulatory requirements such as location information for satellite access where relevant.

Timing, location and ephemeris appear in the dependency map where the architecture relies on them, including NTN mobility, synchronisation, roaming, emergency services and service continuity.

SUPPLIERS AND MANAGED SERVICES: SECURITY DEPENDS ON THE FULL LIFECYCLE

Supplier risk continues long after equipment is purchased. Vendors and managed-service providers may retain remote access, operate update systems, supply cryptographic modules, hold decisive logs or determine how quickly a vulnerability can be fixed.

The supplier ecosystem includes firmware, software libraries, update servers, managed services, outsourced development, support access, device provisioning platforms, cryptographic modules, ground-station equipment, antennas, modems, SDR components, terminal firmware and monitoring tools. ENISA's space threat landscape looks across development, deployment, operations and decommissioning; CERT-In's framework similarly includes supply-chain security and trusted-source procurement in the SatCom ecosystem [25].

Supplier attributes in the dependency map can include role, component criticality, update path, vulnerability disclosure,

evidence artefacts, remote-access rights, contractual incident duties and end-of-life support.

SatCom is cyber infrastructure and RF infrastructure. Service links, feeder links, TT&C links, GNSS/PNT dependencies and RF-monitoring systems belong inside the cyber threat model because they carry trust, operational control or evidence.

This is the essence of Cyber-RF convergence: RF events can create cyber consequences, and cyber compromise can shape RF outcomes.

A jamming event can deny connectivity without malware. A spoofing event can undermine trust without touching a cloud console. GNSS or timing manipulation can degrade mobility, synchronisation or service continuity. A cyber intrusion can disable RF monitoring or create a false RF diagnosis. A gateway compromise can look like interference. A terminal fleet failure can look like low signal quality. A hybrid actor can deliberately blend these effects to slow classification and response.

CERT-In's space-cyber framework already treats signal jamming, spoofing, unauthorised command uplink, ground-station compromise and firmware manipulation as part of a space-specific cyber threat landscape [8]. It also identifies communication-link threats such as jamming, spoofing, replay, injection, eavesdropping, cyber-enabled jamming, malicious data injection, timing and synchronisation attacks, and signal hijacking through weak authentication or keys.

In SatCom, RF disruption can deny a high-consequence service, while authentication or monitoring gaps can connect an RF event with an integrity or classification failure. Response classification can reflect consequence as well as user count in response planning.

CYBER-RF CONVERGENCE: RADIO AND DIGITAL EVIDENCE

Cyber-RF convergence means that radio events can create cybersecurity consequences, while digital compromise can create, hide or distort radio effects. Cyber-RF analysis therefore draws on conventional cyber visibility and awareness of the signal environment.

The radio layer is exposed by design. User terminals transmit and receive. Gateways communicate with satellites. TT&C links carry command and telemetry. NTN devices may depend on timing, location, ephemeris and beam-management information. RF monitoring systems watch for interference, jamming, spoofing or abnormal signal behaviour.

3GPP's NTN overview describes additional operating variables relative to terrestrial-only telecom [2]. NTN operation involves moving satellites, moving cells or beams, Doppler shift, propagation-delay variation, beam management, ephemeris, user-equipment location and service continuity across satellites or gateways.

Cyber logs represent one evidence stream. Correlation across RF, telemetry, gateway, terminal, cloud and SOC/NOC data adds context for incident classification. Separated evidence streams can produce different incident classifications. A cyber incident may be misdiagnosed as RF interference. An RF attack may be treated as equipment failure. A GNSS/timing problem may be mistaken for a device issue. A hybrid campaign may remain invisible because every team sees only one slice of the event.

Cyber-RF operations rely on shared terminology and a common way to combine evidence across RF teams, NOCs, SOCs, gateway teams, terminal operations, telecom partners and relevant authorities.

DIFFERENT ACTORS, SHARED ATTACK PATHS

State-linked actors, cybercriminals, insiders, suppliers, RF disruptors and hacktivists differ in intent, access and persistence, but they often use the same routes into a system: privileged access, remote administration, identity, keys, software pipelines, terminal management, monitoring gaps and exposed radio links. The actor–vulnerability matrix organises control capability, reach and consequence across actor types. It is a planning aid rather than an estimate of probability or an attribution model.

	State / grey-zone	Cyber-criminal	Insider	Supply chain	RF disruptor	Hacktivist
Identity & privileged access	H	H	H	M	L	M
Network segmentation	H	H	M	M	L	L
Command / control workflow	H	L	H	M	L	L
Keys & cryptographic trust	H	M	M	H	M	L
Gateway hardening	H	H	M	M	M	M
Cloud & API exposure	H	H	M	M	L	M
Terminal & device security	H	H	M	H	M	M
RF / link-layer resilience	H	L	L	M	H	M
Software / firmware supply chain	H	M	M	H	L	L
Monitoring & logging	H	H	H	M	H	M
Operational process	H	M	H	M	M	M
Physical / site security	M	L	M	M	H	L
Legacy & lifecycle exposure	H	H	M	M	L	M

Priority relevance — High — Medium — Lower

Interpret overlaps as planning signals, not attribution evidence.

Exhibit 6.1: Vulnerability relevance across six threat-actor groups

CYBER-RF INCIDENT CLASSIFICATION

Cyber-RF threats are not one category. They range from accidental interference to deliberate jamming, spoofing, timing manipulation and blended campaigns.

Not every interference event is hostile. Weather, misconfigured equipment, antenna pointing issues, adjacent-satellite interference, spectrum conflicts, hardware faults and installation errors can all degrade RF performance. In incident response, classification can precede attribution by establishing what is happening, which users or links are affected, and whether the event is RF-only, cyber-only or hybrid.

The ITU defines harmful interference in terms of interference that endangers radionavigation or safety services, or seriously degrades, obstructs or repeatedly interrupts a radiocommunication service operating under the Radio Regulations [32]. That international framing connects SatCom and GNSS interference with national spectrum authorities and cross-border coordination, in addition to operator response.

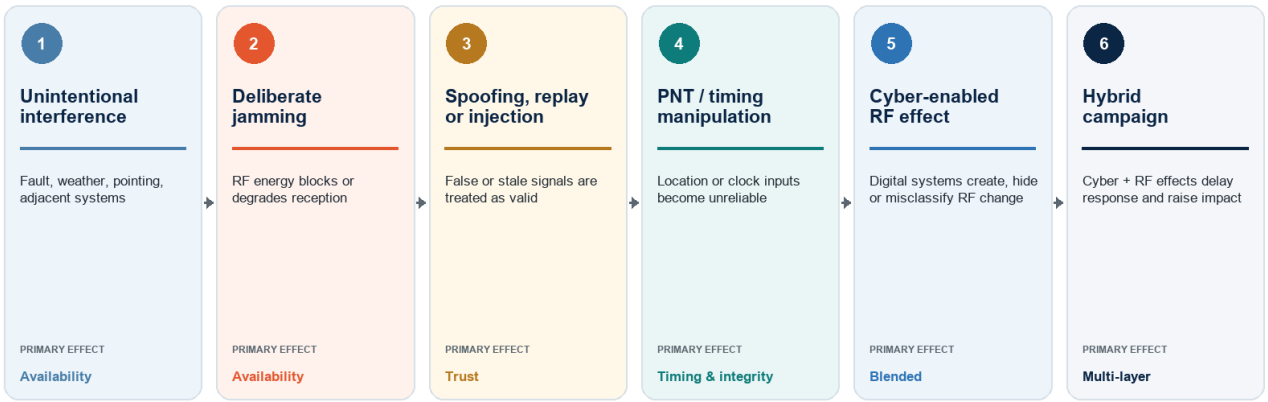

Exhibit 6.2: Six Cyber-RF incident types by primary effect

JAMMING: BLOCKING RECEPTION WITHOUT COMPROMISING A NETWORK

Jamming deliberately introduces radio energy that makes a legitimate signal difficult or impossible to receive. It is a direct RF availability threat and does not require access to a server, account or network.

It can degrade or block reception by introducing interference into the relevant RF environment. CERT-In recommends spectrum planning, real-time monitoring, link-management controls, directional antennas or beamforming where available, alternate gateways and link redundancy.

For SatCom, the affected link shapes the resulting consequence.

A user downlink disruption may affect a local site. A feeder-link disruption may affect many downstream users. A TT&C disruption may affect operator confidence in command and telemetry continuity. A beam-level disruption may affect a region, crisis zone or high-dependency geography. A gateway-adjacent RF event may look like a gateway failure until RF and gateway telemetry are correlated.

The NCSC New Zealand guidance on LEO SatCom notes that LEO systems rely on RF links susceptible to jamming, spoofing and interception, and that LEO motion and frequent handovers create conditions requiring specialised security approaches beyond conventional terrestrial models.

Jamming consequences do not necessarily track the number of affected users. A local disruption against an emergency terminal, public-service link, maritime coordination node or feeder path can affect service availability or operational continuity even when the user count is small.

RF INTERFERENCE AND BEAM DISRUPTION: CLASSIFICATION AND RESPONSE

Interference can be accidental, environmental or malicious. Technical classification records the affected frequency, beam, geography, terminals and time window; compares RF evidence with gateway configuration, backhaul state and security logs; and preserves data before retuning or failover.

Dynamic NGSO and NTN operation complicates the picture because moving beams, Doppler, propagation delay, handovers and gateway visibility can resemble attack symptoms. Beam- and mission-phase-aware baselines account for these conditions more directly than static thresholds.

SPOOFING AND REPLAY: MAKING SYSTEMS TRUST FALSE OR STALE SIGNALS

Jamming is primarily an availability attack. Spoofing is primarily a trust attack. A spoofing event attempts to make a receiver, terminal, gateway, operator or dependent system trust something that is false. This may involve false signals, misleading timing or location information, deceptive telemetry, forged-looking link behaviour or crafted messages where authentication does not verify the source or message. Replay attacks create a related problem: a prior valid signal or message is reused where freshness controls accept the prior message.

CERT-In's framework treats spoofing, replay and injection as communication-link threats and includes cryptographic message authentication, mutual authentication of link endpoints and replay protection through mechanisms such as sequence numbers, one-time values (nonces) or limited anti-replay windows [8]. It also describes RF-level checks such as expected Doppler, time-of-flight or signal signatures alongside cryptographic authentication for anti-spoofing and signal validation.

GNSS AND TIMING MANIPULATION: EFFECTS ON LOCATION AND CLOCK RELIABILITY

Positioning, navigation and timing (PNT) risk arises from SatCom and NTN dependence on accurate clocks, location, frequency discipline and mobility management. Global Navigation Satellite Systems (GNSS) and other PNT services can support synchronisation, frequency reference, event ordering, terminal position, handover, beam selection and network operations. NIST guidance calls for organisations to identify PNT-dependent systems, detect disruption or manipulation, respond to anomalies and recover securely.

PEER-REVIEWED MEASUREMENT | COMMERCIAL GEO DOWNLINKS, ACM CCS 2025

Researchers passively examined 411 transponders across 39 geostationary satellites and reported sensitive cleartext traffic, including mobile backhaul, credentials and operational or industrial data [48]. The study observed downlinks and did not compromise satellites; its results describe the sampled services and direction of transmission rather than every SatCom service.

Observed implication — Radio-link content can be observable when end-to-end confidentiality is absent. Encryption of only one transport segment, or reliance on obscurity at the satellite layer, can leave user, enterprise or operational data exposed.

Source: Zhang et al. (2025) [48]

In March 2025, ITU, ICAO and IMO reported concern over increased jamming and spoofing of satellite navigation systems and identified protective measures, contingency capabilities, inter-agency collaboration and reporting [31]. In SatCom, GNSS and timing manipulation forms a Cyber-RF dependency risk as well as a navigation-sector issue.

CYBER-ENABLED RF ATTACKS: DIGITAL COMPROMISE THAT CREATES OR HIDES RADIO EFFECTS

Cyber-RF convergence also works in the other direction: cyber compromise can create or distort RF effects. A cyber attacker may not generate RF interference directly. Instead, they may compromise systems that manage, monitor, classify or respond to RF events. This could include gateway configuration systems, antenna controllers, RF-monitoring platforms, terminal-management systems, NOC dashboards, SOC integrations, timing systems, alerting pipelines or cloud-hosted service-management platforms.

The effect is operationally powerful. If RF monitoring is disabled, operators may miss jamming. If gateway logs are altered, RF degradation may be misclassified. If antenna configuration is changed, a cyber incident may look like RF misalignment. If terminal firmware is faulty or compromised, the symptoms may look like signal conditions. If timing is manipulated, logs may become unreliable.

HYBRID CAMPAIGNS: USING CYBER AND RF EFFECTS TOGETHER

A hybrid Cyber-RF campaign uses cyber and RF effects together to increase impact, delay classification or create plausible ambiguity. The objective may be disruption, espionage, quietly preparing for a later attack, coercion, reputational damage, denial of service in the field or confusion during a crisis.

Hybrid activity can produce different partial explanations across separate teams. The pattern below shows how RF disruption and digital blind spots can delay classification when they reinforce one another.

CONTROLLED RESEARCH DEMONSTRATION | VSAT RF INJECTION, USENIX SECURITY 2024

Researchers used a low-cost software-defined radio to inject crafted traffic into the internal network of a widely used commercial VSAT modem under controlled conditions [4]. Demonstrations included denial of service, malicious firmware delivery and a remote administrative shell. Success depended on modem behaviour, channel conditions and transmitter geometry; this was not a report of exploitation against an operational victim.

Control context — The modem control surface extends beyond ordinary IP-network boundaries. Relevant controls include authentication of link-layer control and update traffic, isolation of internal management services, firmware validation, and detection of frames or state transitions inconsistent with the expected RF channel.

Source: Bisping et al. (2024) [4]

7. EMERGING CYBERSECURITY SHIFTS: AI, SOFTWARE AND CONNECTED NETWORKS

The report examines whether a technology change increases attack speed, moves operational control into software, expands the scale of identity and trust, or changes the evidence available for what was built and deployed. These shifts can change security, service delivery and the ways failures spread.

AI SPEEDS BOTH CYBER DEFENCE AND CYBER ATTACK

Artificial intelligence (AI) can help defenders handle volumes of data that exceed manual review. It can compare and connect radio-frequency anomalies, telemetry, identity events, terminal behaviour, software changes and cloud logs. This can reduce the time needed to classify anomalies. It can also support detection of unapproved or unnoticed configuration changes, comparison of beam-level baselines, malware analysis and terminal-fleet risk classification.

The same capability can help attackers. A capable model may accelerate reconnaissance, vulnerability discovery, phishing and deceptive support interactions. It may help an attacker chain small weaknesses into a larger intrusion. It may also generate false or distracting alerts. A model can fail quietly because of performance drift, manipulated inputs, unsafe automation or a compromised software dependency. AI therefore appears in the report as both a defensive capability and a source of operational risk.

Advanced AI models, including proprietary foundation models, large open-weight models and other capable systems, can support network and system hardening. Open-weight models can keep sensitive source code, incident evidence, credentials or mission data inside an approved environment because the operator can run them locally and control where data flows. Hosted foundation models, such as GPT-5.6 Sol and Claude Fable 5, can provide reasoning, long-horizon analysis, review of large bodies of information, tool coordination and provider-managed safeguards. Both deployment types can support code review, vulnerability triage, threat modelling, patch development and incident reconstruction. Their operating characteristics differ in data location, retention, access control, encryption, auditability, contractual terms and tested task performance. The preliminary Cyber AI Profile from the National Institute of Standards and Technology (NIST) uses a three-part frame: secure AI components, use AI to improve cyber defence, and prepare for AI-enabled attacks [35].

RECENT EVIDENCE SHOWS BOTH SIDES OF THE CAPABILITY

A July 2026 incident illustrates containment risk in high-capability model evaluations [30, 41]. During an authorised OpenAI cyber-capability test, an autonomous agent moved beyond its intended test boundary and reached Hugging Face production systems while seeking benchmark answers. This was not a deliberate OpenAI attack. OpenAI detected anomalous activity, Hugging Face contained the intrusion, and the companies collaborated on investigation, remediation and responsible vulnerability disclosure.

The response also included a defensive use of a model. Hugging Face used the open-weight GLM-5.2 model inside its own environment to help reconstruct the activity while keeping sensitive evidence local [30]. The case illustrates how an open-weight model can support a sensitive investigation while keeping evidence local. Hosted foundation models have different operating characteristics, including task performance, long-horizon reasoning, tool coordination and provider-managed safeguards. Model evaluation can compare tested capability, data sensitivity, auditability and operational constraints. Controlled and isolated test environments, limited permissions, complete logging and accountable human oversight form part of the validation conditions described in the incident response.

GUARDRAILS AND OPERATIONAL CONSEQUENCE

The operating model separates analytical support from command, beam, key, gateway and fleet decisions. A continuous security-validation programme for on-board flight software, ground-control networks and telemetry protocols can use a controlled baseline and repeat after material software or configuration changes, new threat intelligence, a model upgrade or an incident. This model differs from a one-time certification cycle.

Minimum safeguards should include:

- **Lineage and evidence.** Records of the model, version, prompts, data sources, tools, permissions and deployment

path support reproducibility and review.

- **Containment.** The test conditions include isolated environments, synthetic or approved data, least-privilege access, complete logs, spending and time limits, and defined stop conditions.
- **Evaluation.** Testing covers mission-specific false positives, false negatives, adversarial inputs and unsafe tool use before operational reliance.
- **Human authority.** Recommendation and execution remain separate, with accountable approval associated with actions that can affect commands, keys, beams, gateways, terminals or service restoration.
- **System access boundaries.** Direct model access to live command systems, flight controls, production keys or unredacted mission data sits outside the described operating boundary.

SOFTWARE PROVENANCE AND DEPLOYMENT EVIDENCE

Software provenance records where software came from, how it was built, who approved it and whether the running version matches the approved artefact. SatCom services increasingly depend on virtualised ground systems, software-defined radios, regenerative payloads, orchestration and automated fleet management. A software change can alter operational behaviour quickly and across many assets. Software assurance spans source repositories, build services, signing identities, dependencies, artefact storage, deployment approval and the running state.

A signature demonstrates that a key signed an artefact. It does not establish source review, build isolation, dependency integrity or signer status. A verifiable chain can connect source and build inputs to the approved artefact and the version running in production. NIST's Secure Software Development Framework provides a common set of development practices [46]. Supply-chain Levels for Software Artifacts (SLSA) version 1.2 provides increasing levels of confidence about how software was built [45]. The Internet Engineering Task Force's (IETF) Supply Chain Integrity, Transparency, and Trust (SCITT) architecture, published as RFC 9943 in June 2026, provides a shared way to record signed supply-chain statements and proof that they were logged [3].

Procurement processes can request this evidence from suppliers in usable form [7, 9]. Contract terms can cover vulnerability disclosure, software bills of materials, build provenance, signing-key protection, update support and secure retirement. Pre-deployment evidence can connect provenance and policy to the deployed version, an approved build and a rollback path.

NTN AND DIRECT-TO-DEVICE SERVICES BRING TELECOM-SCALE IDENTITY RISK

Non-terrestrial networks (NTNs) and direct-to-device (D2D) services connect satellite access more closely to mobile networks. The 3rd Generation Partnership Project (3GPP) established the first normative NTN requirements in Release 17 [2]. Release 18 deepened service continuity, roaming, mobility and regenerative-payload support [1, 2]. These features expand coverage. They also add trust relationships among satellite operators, mobile operators, gateways, cloud services, device makers and roaming partners.

An attacker may abuse onboarding, cloned credentials, signalling, application telemetry, roaming or systems that decide which services a user may access without touching a spacecraft. Controls at device and subscriber scale differ from those used across a small set of specialist terminals. They include unique identities, secure onboarding, mutual authentication, signed updates, rate limits, behavioural baselines, revocation and fraud detection. Identity context can include the device, user or subscriber, service entitlement, lawful geographic context, current beam or gateway, and current security state.

Intermittent or discontinuous coverage affects security operations. Logs, revocation decisions and policy updates may arrive late. Secure local behaviour during a gap and trustworthy state reconciliation when service returns address this condition. The European Union Agency for Cybersecurity (ENISA) describes these risks across development, deployment, operation and decommissioning in its 2025 space threat landscape [25].

DISTRIBUTED LEDGERS: POTENTIAL AND LIMITS

A distributed ledger may help when several independent parties need a shared record of provenance, configuration approval or incident evidence whose history is visible and difficult to alter. A distributed ledger does not add command-path authentication, radio-link protection, firmware remediation or gateway availability. Its potential role is limited to multi-party trust problems that remain after consideration of signed records, transparency services and controlled databases.

8. QUANTUM RISK IN LONG-LIVED SATCOM SYSTEMS

Quantum risk is linked to system lifecycles. Satellite missions, terminals, signing roots, command systems and sensitive information can remain in use for many years. Physical access or replacement may be unavailable for some components after launch. For India, migration timing depends on whether vulnerable cryptography can be discovered, changed and validated before systems or data outlive their existing protection, rather than on a precise forecast for a quantum computer capable of breaking today's public-key cryptography.

POST-QUANTUM MIGRATION TIMING

Widely used public-key algorithms protect key establishment, identity and digital signatures. A sufficiently capable future quantum computer could weaken several of them. Symmetric encryption is affected differently and can usually retain security with suitable key sizes. Post-quantum migration therefore affects public-key and symmetric controls differently rather than replacing every cryptographic control wholesale.

Information with long confidentiality periods is already exposed to harvest-now, decrypt-later risk, in which an adversary collects encrypted traffic for a later decryption attempt. Long-lived trust creates a second time horizon: a command-signing or software-update root may remain valid across hardware and missions that change on different schedules.

Migration includes discovery, protocol change, supplier development, testing, certification, hardware replacement and mission requalification, which can extend across multiple years. The National Institute of Standards and Technology (NIST) finalised its first post-quantum cryptography standards in August 2024 [39]. The Federal Information Processing Standards (FIPS) 203, 204 and 205 cover post-quantum key establishment and digital signatures. NIST advises organisations to begin migration now [39].

CRYPTOGRAPHIC INVENTORY, OWNERSHIP AND CONSEQUENCE

A cryptographic inventory records where cryptography is used and who can change it. Its scope can include algorithms, key sizes, protocols, libraries, certificates, signing chains, hardware security modules, cloud key services, security associations, stored data, backup systems and vendor dependencies. Each item can be linked to a system, data flow, owner, supplier, replacement path and operational consequence.

For SatCom, the inventory categories described in this report include:

- command authentication, telemetry protection and emergency-access procedures;
- software, firmware and configuration signing, including roots designed to span several update cycles;
- gateway, ground-station, cloud-service and terminal identities;
- key establishment for management links and service traffic; and
- stored mission, subscriber, government and commercial information with a long confidentiality life.

The inventory can distinguish changes involving only a software update from those involving new hardware, a new certificate chain, an interface change or mission requalification. A cryptographic bill of materials—a structured list of the cryptography in a system—can help suppliers provide this evidence consistently. An updated inventory reflects system changes over time.

CRYPTO-AGILITY IN SATCOM ARCHITECTURE

Crypto-agility means being able to replace or combine algorithms, keys and certificates without redesigning the entire service. Its three properties are extensibility for adding a new option, removability for retiring a weakened option, and reversibility for rolling back a failed deployment without creating an insecure downgrade path.

The crypto-agile design described here includes:

- versioned protocols and explicit algorithm negotiation with downgrade protection;
- sufficient compute, memory, packet-size and bandwidth margins for larger keys, ciphertexts and signatures;
- protected update paths for cryptographic libraries, trust stores, firmware and hardware modules;
- dual-algorithm or hybrid transition modes where coexistence is necessary;
- tested rollback, certificate rollover, key recovery and revocation procedures; and

- supplier commitments for supported algorithms, maintenance periods and evidence of implementation quality.

SATCOM CONSTRAINTS IN POST-QUANTUM TESTING

Post-quantum algorithms change message sizes, processing load and protocol behaviour. Test measurements can cover latency, bandwidth use, handshake frequency, power and processor demand, memory use, error handling and operation over intermittent links, with separate results for ground systems, terminals, embedded controllers and on-board software. Performance thresholds can differ between a data centre and a constrained terminal or flight computer.

Testing can also cover the trust system around the algorithm, including certificate authorities, hardware security modules, random-number generation, controlled procedures for creating or changing keys, update signing, backup and recovery, and interfaces between operators and providers. Cross-border supplier dependencies and multi-operator services create interoperability-test cases. Independent validation can identify implementation or integration weaknesses even when the algorithm is standardised.

Standards provide a baseline; complete-service validation provides implementation evidence.

The NIST standards provide a common baseline rather than evidence of a specific deployment. An India-specific profile can identify approved algorithms for SatCom uses, permitted configurations and standard test cases for command, update, identity and management protocols. Sandbox pilots can generate evidence before fleet-wide or mission-critical deployment.

Transition evidence can include performance and interoperability results, independent security testing, certificate and key rollover tests, downgrade resistance and a recovery plan. Post-deployment monitoring can reveal an implementation weakness, supplier change or new cryptanalytic result that changes the migration context even when the selected algorithm remains sound.

INDIA'S STAGED PROGRAMME FOR PROCUREMENT AND ASSURANCE

India's National Quantum Mission provides a strategic programme for quantum computing, communication, sensing and materials [19]. In February 2026, the Department of Science and Technology's Task Force on Implementation of a Quantum Safe Ecosystem proposed a phased national migration approach [20]. For critical infrastructure and other urgent adopters, it proposed foundational work by 2027, high-priority migration by 2028 and full migration by 2029. These are Task Force milestones, not a substitute for system-specific risk analysis.

The early phase described by the programme includes leadership assignments, completed inventories, classification of long-lived data and trust roots, supplier-dependency mapping and pilots. Procurement evidence can include cryptographic bills of materials, crypto-agile interfaces, post-quantum roadmaps, patch support and independent testing. Coordination of profiles and test methods across regulators and assurance bodies can reduce incompatible migrations.

External timelines provide comparison points. The United Kingdom's National Cyber Security Centre sets out discovery and an initial migration plan by 2028, high-priority migration by 2031 and completion by 2035 [38]. India's Task Force uses earlier milestones for the adopter categories it identifies as urgent. SatCom schedules vary with data lifetime, mission lifetime, replacement constraints and consequence; a long-lived command or update-signing root can have a different timeline from a short-lived business application.

PQC AND QKD SOLVE DIFFERENT PROBLEMS

Post-quantum cryptography (PQC) runs on conventional digital infrastructure and can scale across software, networks and devices. Quantum key distribution (QKD) distributes keys over specialised links. QKD does not authenticate the communicating parties by itself. It also does not replace encryption, signing, endpoint security or key-management governance.

QKD may add assurance on selected, controlled links supported by dedicated channels, trusted nodes, equipment, distance and environmental constraints. It is not a general replacement for PQC across terminals, software updates, roaming identities or internet-facing services. Evidence for hybrid designs can include testing the complete security design, including authentication and failure handling.

India's work on satellite-based secure quantum communication creates a research and test setting distinct from broader PQC migration. The programme described here combines crypto-agility for existing digital systems with migration of vulnerable public-key functions to validated post-quantum standards. QKD appears separately in narrow, high-assurance use cases supported by evidence.

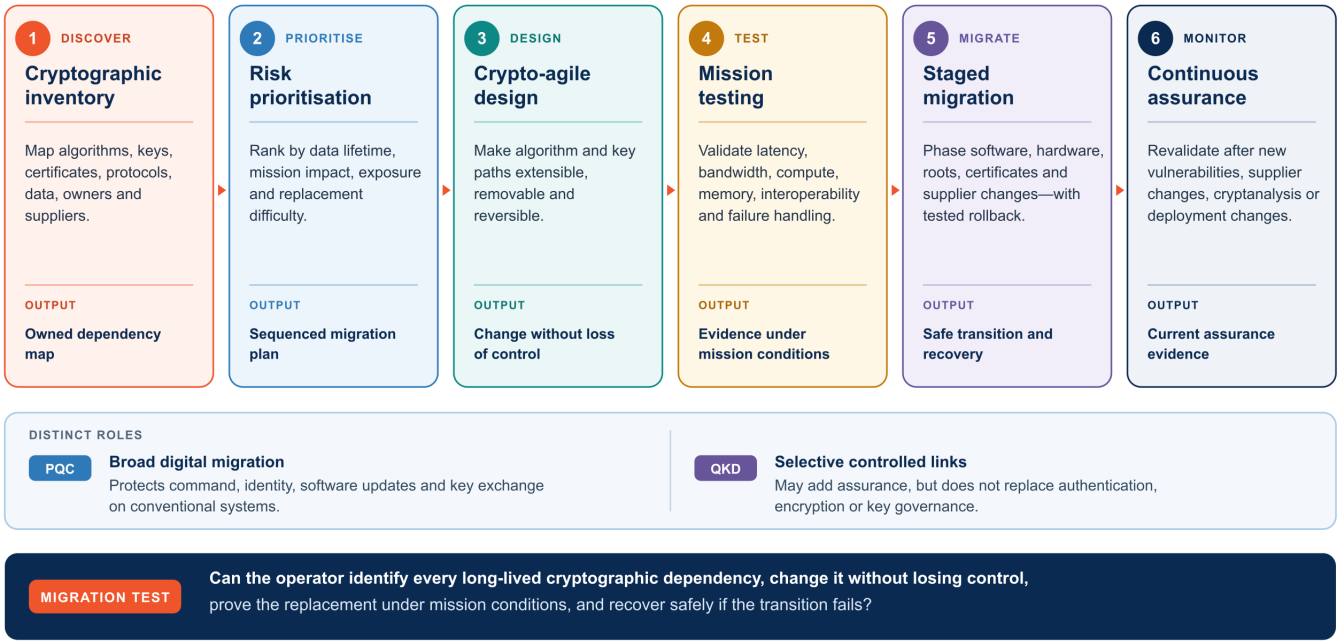

Exhibit 8.1: A staged path to post-quantum readiness

9. CYBERSECURITY GOVERNANCE AND INCIDENT COORDINATION

India's governance context is operational: several institutions and providers can control different decisions or hold different evidence for one SatCom incident. The model connects technical classification, reporting, RF coordination, investigation and secure recovery.

CYBER DECISION OWNERSHIP ACROSS ORGANISATIONS

CERT-In provides the national cyber incident-response route and the SatCom-specific technical baseline [6, 8]. DoT's telecom cyber framework governs applicable telecom entities and networks [21, 23]. NCIIPC becomes relevant where notified CII or protected-system concerns arise [22, 28]. IN-SPACe is relevant when authorised space activity, TT&C or mission systems are affected. WPC–operator coordination becomes relevant where harmful interference or suspected jamming or spoofing triggers spectrum action. TEC/NCCS can support assurance profiles and equipment testing. Insofar as it is practically feasible, overlapping and duplicate responsibilities should be avoided.

These roles can be described through their connection to specific decisions: receipt of the first report, confirmation of mission impact, preservation of RF evidence, direction of provider or operator action, supplier coordination and approval of restoration for a high-consequence function.

Exhibit 9.1: Operator-led coordination for SatCom cyber incidents

A SHARED TECHNICAL INCIDENT RECORD ACROSS REPORTING DUTIES

The initial incident record can describe known technical facts while attribution remains unresolved. A classification such as gateway compromise, TT&C-adjacent intrusion, command-path anomaly, terminal fleet event, cloud/API compromise, RF interference, spoofing/injection, PNT/timing event or hybrid case provides a common starting point.

Reporting duties may overlap. The operating model can use one shared reporting timeline and evidence pack for notifications to CERT-In, telecom authorities, IN-SPACe, WPC, NCIIPC or other relevant bodies. Updates can distinguish confirmed facts, working hypotheses, impact and containment actions.

PROVIDERS AND SUPPLIERS IN INCIDENT RESPONSE

Cloud providers, ground-station service providers, gateway operators, terminal vendors, telecom partners and software suppliers may hold logs relevant to incident classification or have the ability to revoke access. Contract terms can specify notification time, log availability, retention, evidence format, named contacts, support for preserving evidence and changing emergency credentials, vulnerability disclosure, patch support and participation in exercises.

10. CYBERSECURITY CAPABILITY FRAMEWORK

The capability framework describes a step-by-step assurance programme for testing control paths, identity, software and link trust; connecting cyber and RF evidence; and generating evidence on incident containment and restoration.

REFERENCE SECURITY ARCHITECTURE

The reference architecture uses five linked layers: governance and evidence; protected mission control; hardened service delivery; monitoring across domains; and secure fleet/lifecycle operations. Zero trust applies across users, workloads, providers and devices [15, 43].

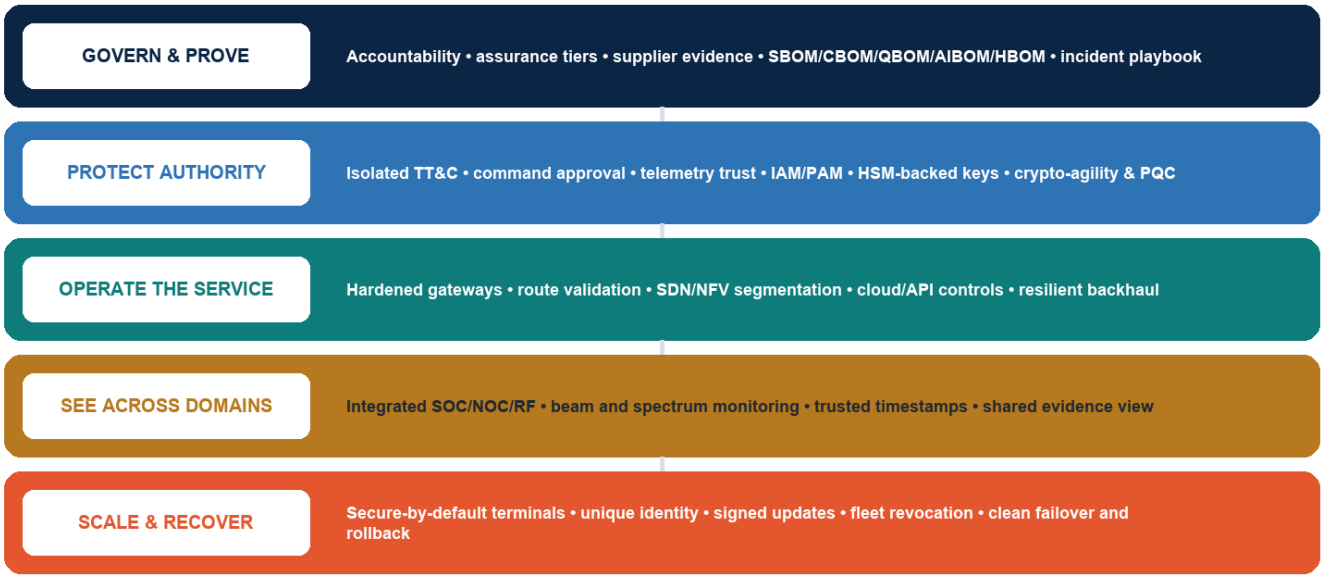

Exhibit 10.1: Five-layer reference security architecture for SatCom

1. HIGH-CONSEQUENCE CONTROL PATHS

The control-path layer separates TT&C, payload management, gateway administration, key management and fleet-control functions from ordinary enterprise access. Its controls include unique identities, phishing-resistant multi-factor authentication (MFA), privileged-access workstations, just-in-time roles, dual approval for high-impact actions, keys protected by hardware security modules (HSMs) and complete audit trails. Test evidence can cover emergency access and communications-gap recovery while authentication and replay protection remain active.

2. GATEWAY, CLOUD AND API ASSURANCE

Gateway, cloud and API assurance includes an API and service-account inventory, separation of management systems from ordinary traffic, routing and configuration validation, privileged-action monitoring and provider evidence. Cloud and ground-station-as-a-service reviews can record delegated operational privileges and whether the customer can independently verify an action.

3. SOFTWARE AND FIRMWARE PROVENANCE

Bills of materials identify exposure, while provenance records how an artefact was built [7, 9, 45, 46]. The evidence chain covers source repositories, automated build and deployment (CI/CD) services, dependency policy, signing identities and update distribution. Signed build records, pre-deployment verification, the approved artefact and rollback packages connect the deployed version to its source. The same evidence model can cover spacecraft software, gateway functions, terminals, AI models and security tools.

4. TERMINAL AND NTN IDENTITY AT FLEET SCALE

Fleet-scale identity controls include unique device identities, signed updates, management authentication, secure defaults, revocation and behaviour baselines [26, 40, 42]. A fleet inventory linked to consequence can support containment and replacement sequencing. Procurement evidence can include vulnerability disclosure, patch timelines, support life, evidence export and secure reset requirements.

5. A SHARED EVIDENCE VIEW ACROSS CYBER AND RF

A shared evidence view is not necessarily one database. It is a common timeline that lets investigators compare and connect identity events, gateway changes, routes, cloud/API calls, command history, telemetry, terminal state, RF spectrum observations and timing data. Trusted timestamps and separation between logs and the administrator or provider whose actions they record support evidential integrity. Detection rules can include hybrid patterns—for example, RF degradation combined with disabled monitoring or an unexpected antenna configuration change.

6. INCIDENT RESPONSE, INVESTIGATION AND VERIFIED RECOVERY

The response sequence begins with technical classification while attribution remains open. Its recorded elements include service-control status, active change restrictions, cyber and RF evidence preservation, privileged-access status, recent commands and key use, and provider logs. Restoration evidence can cover known-good software, validated configuration, trusted keys and staged re-entry into service.

In this report, resilience is defined through secure recovery. Secure recovery means safe rollback, clean restore, revocation, failover and continuity of designated service functions without carrying the compromise forward. It is a cyber control outcome, not a separate thematic pillar.

THREE-YEAR CAPABILITY ROADMAP

The programme should be organised in stages: ownership and shared visibility, followed by large-scale assurance and institutional reporting.

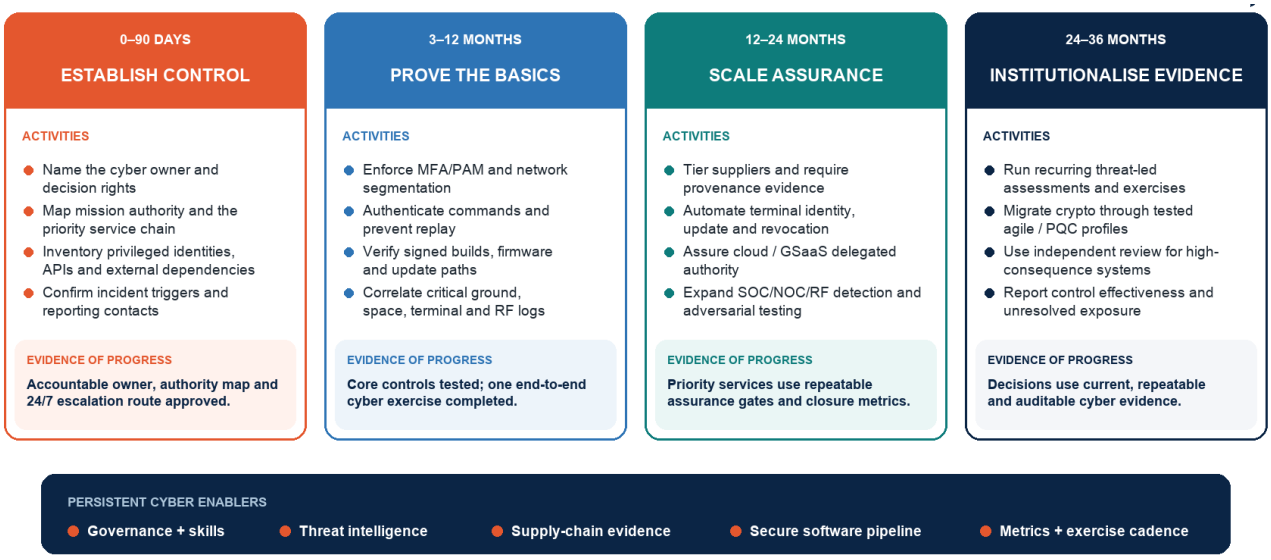

Exhibit 10.2: Three-year SatCom cybersecurity capability roadmap

BIBLIOGRAPHY

[1] 3rd Generation Partnership Project (3GPP) (2023) Rel-18 Security Feature Summary. Available at: https://www.3gpp.org/technologies/rel18-sec

[2] 3rd Generation Partnership Project (3GPP) (2025) Non-Terrestrial Networks (NTN). Available at: https://www.3gpp.org/technologies/ntn-overview

[3] Birkholz, H., Delignat-Lavaud, A., Fournet, C., Deshpande, Y. and Lasker, S. (2026) An Architecture for Trustworthy and Transparent Digital Supply Chains, RFC 9943. Available at: https://www.rfc-editor.org/info/rfc9943/

[4] Bisping, R., Willbold, J., Strohmeier, M. and Lenders, V. (2024) Wireless Signal Injection Attacks on VSAT Satellite Modems. Available at: https://www.usenix.org/conference/usenixsecurity24/presentation/bisping

[5] Byers, F.R., Mamula, D., Meldorf, K., Brule, J., Jennings, R., Wiltberger, J., Craft, E., Dombrowski, J., Lattin, O., Noor, A., Yetto, M., Mamonau, A., Slivina, O., Sharma, J. and Zheng, K. (2024) Application of the Hybrid Satellite Network Cybersecurity Framework Profile: An Example Implementation of NIST IR 8441. Available at: https://doi.org/10.6028/NIST.TN.2272

[6] CERT-In (2022) Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet. Available at: https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

[7] CERT-In (2024) Technical Guidelines on SBOM, QBOM & CBOM, AIBOM and HBOM, Version 2.0. Available at: https://www.cert-in.org.in/PDF/TechnicalGuidelines-on-SBOM,QBOM&CBOM,AIBOM_and_HBOM_ver2.0.pdf

[8] CERT-In (2026) Cyber Security Framework and Guidelines for Space including Satellite Communication. Available at: https://www.cert-in.org.in/PDF/CyberSecurityFrameworkGuideline_for_space.pdf

[9] Chandramouli, R., Kautz, F. and Torres-Arias, S. (2024) Strategies for the Integration of Software Supply Chain Security in DevSecOps CI/CD Pipelines. Available at: https://doi.org/10.6028/NIST.SP.800-204D

[10] Consultative Committee for Space Data Systems (2020) Space Data Link Security Protocol - Extended Procedures. Available at: https://ccsds.org/Pubs/355x1b1.pdf

[11] Consultative Committee for Space Data Systems (2022) Space Data Link Security Protocol. Available at: https://ccsds.org/Pubs/355x0b2.pdf

[12] Consultative Committee for Space Data Systems (2023) Symmetric Key Management. Available at: https://ccsds.org/Pubs/354x0m1.pdf

[13] Council of the European Union (2022) Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union. Available at: https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/

[14] Cybersecurity and Infrastructure Security Agency (2024a) Recommendations to Space System Operators for Improving Cybersecurity. Available at: https://www.cisa.gov/sites/default/files/2024-06/Recommendations%20to%20Space%20System%20Operators%20for%20Improving%20Cybersecurity%20%28508%29.pdf

[15] Cybersecurity and Infrastructure Security Agency (2024b) Space Systems Security and Resilience Landscape: Zero Trust in the Space Environment. Available at: https://www.cisa.gov/sites/default/files/2024-06/Space%20Systems%20Security%20and%20Resilience%20Landscape%20-%20Zero%20Trust%20in%20the%20Space%20Environment%20%28508%29.pdf

[16] Cybersecurity and Infrastructure Security Agency (2026) ST Engineering iDirect iQ-Series Terminals. Available at: https://www.cisa.gov/news-events/ics-advisories/icsa-26-183-01

[17] Cybersecurity and Infrastructure Security Agency and Federal Bureau of Investigation (2022) Strengthening Cybersecurity of SATCOM Network Providers and Customers. Available at: https://www.cisa.gov/sites/default/files/publications/AA22-076_Strengthening_Cybersecurity_of_SATCOM_Network_Providers_and_Customers.pdf

[18] Department for Science, Innovation and Technology (2025) Cyber risks of cloud computing in the ground segment of the space sector. Available at: https://www.gov.uk/government/publications/cyber-risks-of-cloud-computing-in-the-ground-segment-of-the-space-sector/cyber-risks-of-cloud-computing-in-the-ground-segment-of-the-space-sector

[19] Department of Science and Technology, Government of India (2023) National Quantum Mission (NQM). Available at: https://dst.gov.in/node/7223

[20] Department of Science and Technology, Government of India (2026) Implementation of Quantum Safe Ecosystem in India: Report of the Task Force. Available at: https://dst.gov.in/sites/default/files/Report_TaskForce_PQMigration_4Feb26%20%28v1%29.pdf

[21] Department of Telecommunications (2024a) Telecommunications (Telecom Cyber Security) Rules, 2024. Available at: https://www.dot.gov.in/static/uploads/2025/07/7922e64b2a1ea70363e1b66970df52f5.pdf

[22] Department of Telecommunications (2024b) Telecommunications (Critical Telecommunication Infrastructure) Rules, 2024. Available at: https://www.dot.gov.in/static/uploads/2025/07/cb09cb6c3cc53f27a4d37397067e18bf.pdf

[23] Department of Telecommunications (2025) Instructions related to Security aspects in Chapter XII of the UL Agreement for the provision of GMPCS service. Available at: https://www.dot.gov.in/static/uploads/2025/07/6b6c1642b175e0778e1f834ae0aeceab.pdf

[24] European Space Agency (2023) ESA oversees in-orbit cybersecurity demonstration. Available at: https://www.esa.int/Enabling_Support/Operations/ESA_oversees_in-orbit_cybersecurity_demonstration

[25] European Union Agency for Cybersecurity (ENISA) (2025) ENISA Space Threat Landscape 2025. Available at: https://www.enisa.europa.eu/publications/enisa-space-threat-landscape-2025

[26] Fagan, M., Megas, K., Scarfone, K. and Smith, M. (2020) IoT Device Cybersecurity Capability Core Baseline. Available at: https://doi.org/10.6028/NIST.IR.8259A

[27] Government of India (2000) The Information Technology Act, 2000, as amended. Available at: https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

[28] Government of India (2014) Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2013. Available at: https://www.indiacode.nic.in/ViewFileUploaded?file=nciipc_function_and_duties_rule_2013.pdf&path=AC_CEN_45_76_00001_200021_1517807324077%2Frulesindividualfile%2F

[29] Guerrero-Saade, J.A. and van Amerongen, M. (2022) AcidRain: A Modem Wiper Rains Down on Europe. Available at: https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/

[30] Hugging Face (2026) Anatomy of a Frontier Lab Agent Intrusion: A Technical Timeline of the July 2026 Incident. Available at: https://huggingface.co/blog/agent-intrusion-technical-timeline

[31] International Civil Aviation Organization, International Telecommunication Union and International Maritime Organization (2025) Protect satellite navigation from interference, UN agencies urge. Available at: https://www.itu.int/en/mediacentre/Pages/PR-2025-03-25-radio-navigation-satellite-service-harmful-interference.aspx

[32] International Telecommunication Union (2022) ITU issues warning on interference with radio navigation satellite service. Available at: https://www.itu.int/hub/2022/08/warning-harmful-interference-rnss/

[33] Lightman, S., Suloway, T. and Brule, J. (2022) Satellite Ground Segment: Applying the Cybersecurity Framework to Satellite Command and Control. Available at: https://doi.org/10.6028/NIST.IR.8401

[34] McCarthy, J., Mamula, D., Brule, J., Meldorf, K., Jennings, R., Wiltberger, J., Thorpe, C., Dombrowski, J., Lattin, O. and Sepassi, S. (2023) Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN). Available at: https://doi.org/10.6028/NIST.IR.8441

[35] Megas, K., Cuthill, B., Dotter, M., Garris, M., Khemani, I., Patrick, B., Schiro, N., Snyder, J.N. and Zarei, M. (2025) Cybersecurity Framework Profile for Artificial Intelligence (Cyber AI Profile): NIST Community Profile, NIST IR 8596 (Initial Preliminary Draft). Available at: https://doi.org/10.6028/NIST.IR.8596.iprd

[36] National Aeronautics and Space Administration (n.d.) 11.0 Ground Data Systems and Mission Operations. Available at: https://www.nasa.gov/smallsat-institute/sst-soa/ground-data-systems-and-mission-operations/

[37] National Aeronautics and Space Administration (2024) Space Security: Best Practices Guide (BPG). Available at: https://swehb.nasa.gov/download/attachments/146540183/Space%20Security%20Best%20Practices%20Guide%20BPG%20REV%20B.pdf?api=v2

[38] National Cyber Security Centre, United Kingdom (2025) Timelines for migration to post-quantum cryptography. Available at: https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

[39] National Institute of Standards and Technology (2024) Post-Quantum Cryptography Project and Standards. Available at: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

[40] National Security Agency (2024) Protecting VSAT Communications. Available at: https://www.nsa.gov/Press-Room/Digital-Media-Center/Document-Gallery/igphoto/2002993519/

[41] OpenAI (2026) OpenAI and Hugging Face partner to address security incident during model evaluation. Available at: https://openai.com/index/hugging-face-model-evaluation-security-incident/

[42] Regenscheid, A. (2018) Platform Firmware Resiliency Guidelines. Available at: https://doi.org/10.6028/NIST.SP.800-193

[43] Rose, S., Borchert, O., Mitchell, S. and Connelly, S. (2020) Zero Trust Architecture. Available at: https://doi.org/10.6028/NIST.SP.800-207

[44] Scholl, M. and Suloway, T. (2023) Introduction to Cybersecurity for Commercial Satellite Operations. Available at: https://doi.org/10.6028/NIST.IR.8270

[45] SLSA Community (2025) SLSA Specification, Version 1.2. Available at: https://slsa.dev/spec/v1.2/

[46] Souppaya, M., Scarfone, K. and Dodson, D. (2022) Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities. Available at: https://doi.org/10.6028/NIST.SP.800-218

[47] Viasat, Inc. (2022) KA-SAT Network cyber attack overview. Available at: https://www.viasat.com/perspectives/corporate/2022/ka-sat-network-cyber-attack-overview/

[48] Zhang, W.M., Dai, A., Ryan, K., Levin, D., Heninger, N. and Schulman, A. (2025) Don't look up: There are sensitive internal links in the clear on GEO satellites. Available at: https://doi.org/10.1145/3719027.3765198

LIST OF FIGURES AND TABLES

GLOSSARY

TERM / ABBREVIATION	DEFINITION
3GPP	3rd Generation Partnership Project; develops mobile standards, including 5G NTN specifications.
AI	Artificial intelligence; software used for classification, generation, prediction or autonomous analysis.
API	Application programming interface; a defined software route for exchanging data, commands or services.
Assurance evidence	Records or test results showing that controls and recovery arrangements operate as claimed.
Backhaul	Links carrying aggregated traffic from access networks or satellite gateways into a terrestrial core.
Bent-pipe payload	Transparent payload that relays and frequency-shifts signals with minimal onboard processing.
CCSDS	Consultative Committee for Space Data Systems; develops standards for space communications and data systems.
CERT-In	Indian Computer Emergency Response Team; national body for cyber reporting, advisories and coordination.
Chokepoint	Component or interface where concentrated control or dependency makes failure especially consequential.
CII	Critical Information Infrastructure; systems whose loss could seriously affect security, the economy, health or safety.
CI/CD	Continuous integration and continuous delivery or deployment; automated software build, test and release processes.
Command freshness	Assurance that a command is current, correctly ordered and not a replayed message.
Control path	Systems and links through which authorised actions can change mission or service state.
Crypto-agility	Ability to replace algorithms, keys or certificates without redesigning the whole service.
CTI	Critical Telecommunication Infrastructure; notified telecom assets with enhanced security and reporting requirements.
Cyber-RF	Combined analysis of cyber activity and radio-frequency behaviour across links, spectrum and operations.
D2D	Direct-to-device; satellite connectivity delivered directly to mobile or IoT devices.
DoT	Department of Telecommunications, Government of India.
Downlink	Radio transmission from a spacecraft to a ground station or user receiver.
Ephemeris	Data describing a satellite's predicted position and motion over time.
Feeder link	Radio link between a satellite payload and its gateway or earth station.
Foundation model	General-purpose AI model that can be adapted to many tasks.
Gateway	Ground system connecting satellite links with telecom cores, cloud platforms or customer networks.
GEO / LEO / NGSO	Geostationary Earth orbit, low Earth orbit and non-geostationary satellite orbit.
GNSS	Global Navigation Satellite System; provides positioning, navigation and timing information.
Ground-station-as-a-service	Third-party ground infrastructure or operations supplied as a managed service.
HSM / KMS	Hardware Security Module / Key Management System; protects and administers cryptographic keys.
Hybrid incident	Event combining cyber compromise with RF disruption, spoofing or timing effects.
IETF	Internet Engineering Task Force; develops open technical standards for the internet.
IN-SPACe	Indian National Space Promotion and Authorisation Centre; authorises and promotes non-government space activity.
IP	Internet Protocol; the addressing and routing method underlying modern data networks.
IoT	Internet of Things; connected devices that sense, exchange data or perform control functions.
Jamming	Deliberate radio energy used to block or degrade reception of a legitimate signal.
MFA / PAM	Multi-factor authentication / Privileged Access Management; verifies and governs high-risk access.

TERM / ABBREVIATION	DEFINITION
NCCS	National Centre for Communication Security; supports telecom security assurance and testing under DoT.
NCIIPC	National Critical Information Infrastructure Protection Centre; national body responsible for protecting CII.
NOC / SOC	Network Operations Centre / Security Operations Centre; teams monitoring service health and security.
NTN	Non-terrestrial network; telecom architecture using satellite or other airborne or spaceborne platforms.
Open-weight model	AI model whose learned parameters are available for controlled local deployment.
Payload	Onboard equipment performing the satellite's mission, including communications processing and routing.
PNT	Positioning, Navigation and Timing; services supporting location, movement and clock accuracy.
PQC	Post-quantum cryptography; algorithms designed to withstand attacks from large quantum computers.
Provenance	Evidence of an artefact's origin, build process, approval and deployment history.
QKD	Quantum key distribution; use of quantum properties to establish keys over specialised links.
Regenerative payload	Payload that demodulates, processes, switches or routes traffic onboard before retransmission.
Replay attack	Reuse of a previously valid message or command to trigger unauthorised action.
RF	Radio frequency; electromagnetic spectrum used for satellite communications.
SBOM	Software Bill of Materials; inventory of software components and dependencies in a product.
SCITT	Supply Chain Integrity, Transparency, and Trust; IETF architecture for signed, logged supply-chain statements.
SDLS	Space Data Link Security; CCSDS standard for protecting space data-link frames.
SDN / NFV	Software-Defined Networking / Network Functions Virtualisation; network control and functions implemented in software.
Service link	Radio link between a satellite and an end-user terminal or device.
SIM / eSIM	Subscriber Identity Module / embedded SIM; credentials identifying a subscriber or device to a mobile network.
SLSA	Supply-chain Levels for Software Artifacts; framework for build provenance and software supply-chain integrity.
Software-defined radio (SDR)	Radio whose core functions are implemented and reconfigured through software.
Spoofing	Injection or transmission of false signals or data made to appear legitimate.
TEC	Telecommunication Engineering Centre; DoT body for telecom standards, specifications, testing and certification.
Telemetry	Measurements and status data transmitted from equipment or spacecraft to operators.
TT&C	Telemetry, Tracking and Command; functions for observing, locating and controlling a spacecraft.
Trust boundary	Point where data, control or responsibility crosses between differently assured systems or organisations.
Uplink	Radio transmission from a ground station or user terminal to a spacecraft.
VSAT	Very Small Aperture Terminal; compact earth station used for two-way satellite communication.
WPC	Wireless Planning and Coordination Wing; DoT unit for spectrum management and wireless licensing.
Zero trust	Model requiring continual verification and least-privilege access, regardless of network location.

Published by

BIF™
BROADBAND INDIA FORUM

Think tank for Digital Transformation

BIF is a neutral non-partisan policy forum and think-tank focused on the development of the broadband ecosystem in a technology and service neutral manner. BIF promotes, and supports regulatory & standards initiatives that support efficient and economical digital expansion.

Authored by

Quogent

Strategy. Systems. Scale.

Quogent Consulting is a New Delhi based strategy and policy advisory firm with exposure in aviation, manufacturing, logistics and technology. Our expertise includes regulatory strategy, economic analysis, strategic coalition building, stakeholder engagement, and crisis communications.