

Codec Networks

Coding Threats. Decoding Solutions.

SPACE, SATELLITE & GEOSPATIAL SERVICES

Secure the Ground. Protect Every Mission.

Ground infrastructure security, API and cloud testing, identity controls and supply chain assurance for space, satellite and geospatial services businesses

Coding Threats. Decoding Solutions. · www.codecnetworks.com



What we will cover



The sector and its risks

Scale, players and the threats that matter most



What regulators now expect

Space Policy and IN-SPACe, telecom rules, CERT-In, geospatial and DPDP



How Codec Networks helps

Services, bundles and packages built for the sector



Proof in scenarios

Five new case studies and the controls that break the chain



Why Codec Networks and next steps

Our value add and how to start



India's space sector is opening fast, and so is its attack surface

Public figures show the scale of what must be protected

US\$44 bn

Space economy target for 2033

113

IN-SPACe authorisations to 52
private entities

100+

Cyber attacks a day on ISRO, per
its chairman (2023)

6 hours

To report cyber incidents to
CERT-In

What this means: Satellite makers and operators, launch firms, ground station and satcom providers and geospatial platforms must secure antennas, mission control and command keys, protect management networks and terminal updates, test every API that sells imagery or location data, control privileged and vendor access, assure component and software suppliers, protect location data and report incidents to CERT-In within six hours.

Sources: IN-SPACe and PIB (October 2024), Lok Sabha reply (August 2026), ISRO chairman at c0c0n (October 2023), CERT-In Directions (2022).

Who we serve across space, satellite and geospatial services



Satellite manufacturers

Bus, payloads, subsystems, components



Satellite operators

Communication, EO and constellation fleets



Launch start-ups

Launch vehicles, engines, ranges



Ground stations and teleports

Antennas, TT&C, ground-station-as-a-service



Satcom providers

VSAT, broadband, maritime and aero links



Earth observation

Imagery, tasking, analytics platforms



Geospatial platforms

Maps, GIS, surveys, digital twins



Navigation and location

GNSS receivers, NavIC, location APIs

The threats that cost space and geospatial businesses the most

Six priorities from our 18-threat space, satellite and geospatial assessment



Ground station intrusion

Antennas, baseband, teleports



Command and key misuse

Mission control, TT&C, keys



Terminal and NMS attacks

Management VPNs, update servers



API and cloud flaws

EO tasking, geospatial, location



Supply chain compromise

Components, software, integrators



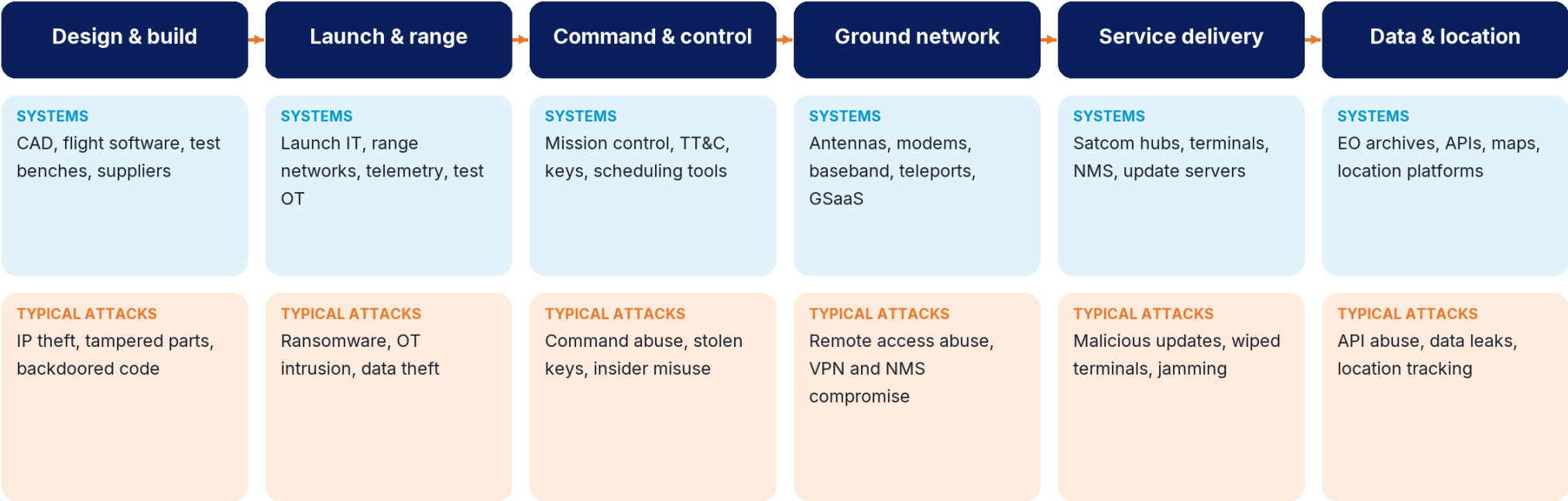
Location data exposure

Tracking, movement histories

Attacks target every step from design to data delivery

Where Cyber Risk Sits Across the Space Mission Lifecycle

Every step from design to data delivery carries its own attack surface



A satellite service is only as secure as its ground network: one breached update server, vendor tunnel or API can silence it or leak its data.

Source: Codec Networks analysis

Codec Networks

What regulators now expect

Space Policy and IN-SPACe, telecom rules, CERT-In, geospatial and DPDP

The rules shaping space and geospatial security

Requirement	Frequency / deadline	Source
Space activity authorisation	Space objects, launch, ground systems	Space Policy 2023; IN-SPACe NGP 2024
Foreign satellite capacity	IN-SPACe authorisation needed	IN-SPACe NGP; from 1 Apr 2025
Foreign investment	74% satellites, 49% launch, 100% parts	FDI policy amendment, 2024
Satcom services	Licence, spectrum, security conditions	Telecom Act 2023; DoT licences
Telecom cyber security	Incident reports, CTSO, security operations	Telecom Cyber Security Rules 2024
Cyber incident reporting	To CERT-In within 6 hours; 180-day logs	CERT-In Directions, 2022
Independent audits	Risk-based audits, including OT and ICS	CERT-In guidelines, Jul 2025
Geospatial data and maps	No prior approval; sensitive attributes	Geospatial Guidelines, 2021
Personal and location data	Safeguards and breach intimation	DPDP Act 2023; Rules 2025

Key dates on the regulatory timeline

Legal and Regulatory Timeline Shaping Space and Geospatial Security

Space, telecom, geospatial, cyber, data and export-market instruments that reach satellite, launch, ground segment, satcom, EO and navigation businesses

● In force ● Upcoming (from Oct 2026)

Feb 2021	● Geospatial Data Guidelines remove prior approval for most mapping; sensitive attributes listed
Feb 2022	● AcidRain wiper hits KA-SAT modems on 24 Feb; about 5,800 wind turbines lose remote access
Apr 2022	● CERT-In Directions: 6-hour incident reporting and 180-day ICT logs kept in India
Dec 2022	● National Geospatial Policy 2022 notified, building on the 2021 guidelines
Apr 2023	● Indian Space Policy 2023 approved: roles of IN-SPACe, NSIL, ISRO and private entities
Dec 2023	● Telecommunications Act 2023 enacted; First Schedule allows administrative spectrum assignment
Feb 2024	● FDI eased: 74% satellites, 49% launch vehicles, 100% components via automatic route
May 2024	● IN-SPACe releases Norms, Guidelines and Procedures for authorising space activities
Nov 2024	● Telecom Cyber Security Rules 2024 notified: incident reporting, CTSO and security operations
Apr 2025	● Only IN-SPACe-authorised foreign satellites may provide capacity in India
Jun 2025	● European Commission proposes an EU Space Act with cyber rules for space and ground assets
Jul 2025	● CERT-In Comprehensive Cyber Security Audit Policy Guidelines, including OT and ICS
Nov 2025	● DPDP Rules notified, with most obligations phased in over 18 months
May 2027	● Most DPDP Rules obligations, incl. security safeguards and breach intimation, apply

Sources: Department of Space, IN-SPACe, DST, DoT, PIB, CERT-In, MeitY, European Commission. Confirm against the official instruments.

Codec Networks

How Codec Networks helps

Ground stations · Satcom · APIs & cloud · Identity · Supply chain · SOC

One partner from ground station to API



Ground Station Security

Antennas, TT&C, mission control



Satcom Network Security

Hubs, NMS, terminals



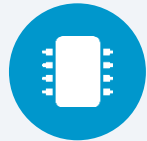
API & Cloud Testing

EO, geospatial, location APIs



Identity & Access

Privileged, key, vendor access



Supply Chain Assurance

Components, software, SBOMs



24/7 SOC & Response

Monitoring, CERT-In, forensics

Eleven bundles from the Codec Networks catalogue

Business-ready bundles instead of 180 separate services



Bundle numbers follow the Codec Networks Bundled Service Models. Scope, frequency and pricing are confirmed during scoping.

Three packages, sized to where you are

Foundation

Space start-ups and geospatial platforms

- API and web platform test (B2)
- Cloud ground segment review (B3)
- Location data privacy check (B6)
- IR retainer (B8)

Assurance

Satellite operators and ground station firms

- Ground network VAPT (B1)
- Privileged access review (B3)
- CERT-In empanelled audit (B4)
- 24x7 managed SOC (B7)

Continuous Resilience

Satcom providers and large space groups

- Red team of ground and NMS (B1)
- Supply chain assurance (B9)
- ISO 27001 and telecom rules (B5)
- SOC with OT and NMS (B7)

Every obligation mapped to a bundle

Requirement	How Codec Networks helps	Bundle
Authorisation for space objects and ground systems (IN-SPACE NGP)	Authorisation security review	B4, B5
Licence security conditions for satcom services (DoT)	Gateway and network assessment	B1, B3
Incidents to CERT-In in six hours; 180-day logs (CERT-In)	SOC, IR retainer, reporting support	B7, B8
Risk-based independent audits incl. OT (CERT-In guidelines 2025)	CERT-In empanelled audit	B4
Sensitive attributes kept off maps (Geospatial Guidelines 2021)	Data handling and API review	B2, B6
Safeguards and breach intimation for location data (DPDP Act)	DPDPA programme	B6
Supplier and component assurance where contracts require it	Supply chain assessment	B9

Five new case studies, five broken chains

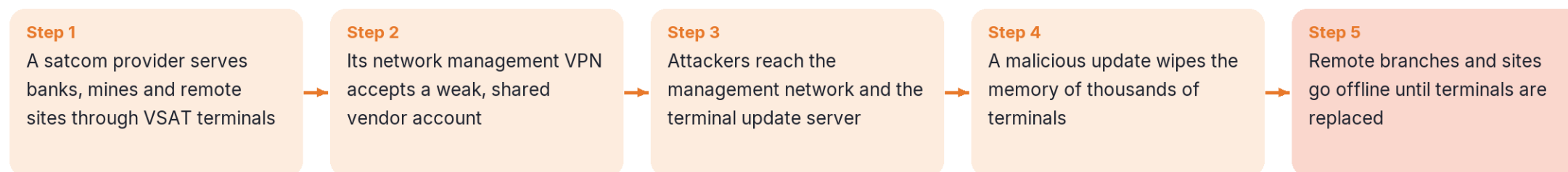
Illustrative composite scenarios written for 2026—not client engagements

1	The Update That Silenced the Terminals	A weak vendor VPN account lets attackers wipe thousands of terminals; MFA and signed updates stop it	B3 · B7 · B8
2	The Ground Station Nobody Owned	An infected vendor tunnel brings ransomware to a teleport; brokered access and segmentation stop it	B1 · B3 · B9
3	The API That Gave Away the Map	A trusted order number exposes other clients' imagery; server-side checks prevent it	B2 · B6 · B1
4	The Component With a Second Owner	A breached supplier ships a hidden function in subsystem software; integrity checks catch it	B9 · B2 · B5
5	The Location Trail Anyone Could Follow	An old API leaks drivers' movement histories; API inventory and minimisation prevent it	B2 · B6 · B7

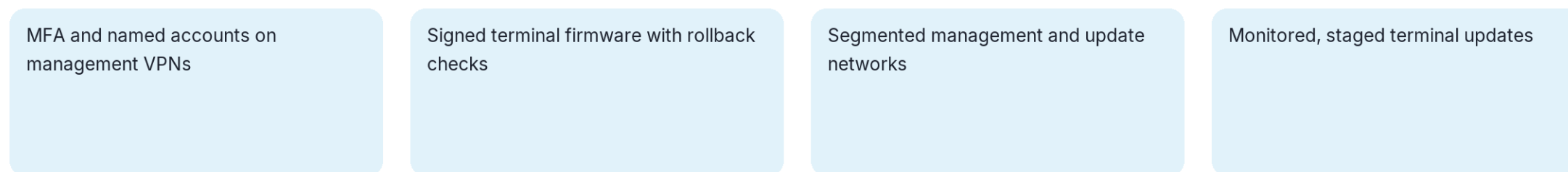
Example: stopping a malicious terminal update

Case 1: The Update That Silenced the Terminals

ILLUSTRATIVE ATTACK PATH



WHERE CONTROLS BREAK THE CHAIN



Illustrative composite scenario prepared by Codec Networks. Not a client engagement.

Codec Networks

What we test: who can reach the satcom management network and how, whether vendor and staff accounts use MFA, whether the update server is segmented and monitored, whether terminals reject unsigned or downgraded firmware, how updates are staged and watched, and how the provider would recover terminals, investigate and report to CERT-In and customers.

Why space and geospatial businesses choose Codec Networks



CERT-In empanelled

For information security auditing services; NICS empanelled for application audits



Certified

ISO 9001:2015, ISO/IEC 27001:2022, ISO/IEC 20000-1:2018



Regulation-mapped

Mapped to the Space Policy and IN-SPACe norms, the Telecom Act and Telecom Cyber Security Rules, CERT-In Directions and audit guidelines, the Geospatial Guidelines and DPDP



Tests the whole chain

Technical, process and monitoring tests together



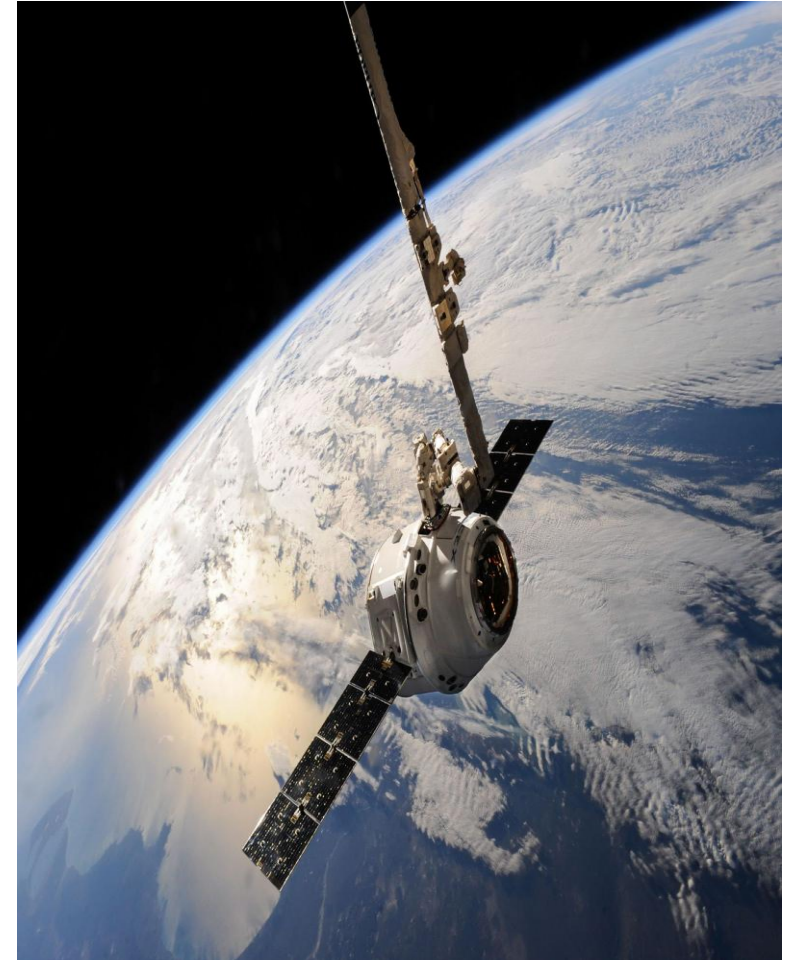
Full stack, one partner

VAPT, audits, SOC, forensics, privacy and Board advisory connected



Specialist experts

CEH, OSCP, CPENT, CISA, ISO 27001 LA/LI, CHFI; OWASP, MITRE ATT&CK, NIST



How we deliver, and what you receive

Codec Networks Delivery Methodology

Nine stages, from scoping to continuous improvement



Source: Codec Networks project and service delivery methodology

Codec Networks

- Executive summary for the Board or its committee
- Technical findings with evidence and CVSS ratings
- Compliance gap matrix mapped to your obligations
- Prioritised remediation roadmap and retest reports
- Audit evidence tracker for regulators and partners
- SOC dashboards with MTDD and MTTR metrics

Let's start with a scoping session

1 Scoping session

Ground stations, teleports and mission control, command keys, satcom hubs, management networks and terminals, cloud ground segment, EO and location APIs, privileged and vendor access, suppliers, data

2 Proposal

Regulation-mapped scope, methodology, timeline and deliverables

3 Kick-off

Testing, audit or SOC onboarding, with Board-ready reporting

 New Delhi: 507, 5th Floor, New Delhi House, Barakhamba Road, Connaught Place – 110001

 Gurugram: 707, 7th Floor, Silverton Tower, Golf Course Extension Road, Sector 50 – 122018

 011 430 496 96 · 011 437 522 99 · +91 99716 76124 · +91 88007 88220 · +91 88003 31124

 mktg@codecnetworks.com · www.codecnetworks.com

Regulatory references reflect public instruments as of October 2026; applicability depends on each entity's licence, category and activities.