

TC260-TR-003-2026

网络安全标准化技术研究报告

——卫星通信网络安全标准化研究

v1.0-202603

全国网络安全标准化技术委员会秘书处

全国网络安全标准化技术委员会通信安全标准工作组
(WG6)

2026 年 3 月

本文档可从以下网址获得：

www.tc260.org.cn/



全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC



前 言

《网络安全标准化技术研究报告》（以下简称《技术报告》）是全国网络安全标准化技术委员会（以下简称“网安标委”）秘书处组织编制和发布的技术研究类文件。本文件立足新技术新应用领域网络安全前沿动态，通过系统的技术研究、产业调研、标准分析与综合研判，梳理关键领域网络安全风险与挑战，提出标准化发展趋势及相关工作实施建议，为网络安全国家标准制修订与网络安全保障实施提供前瞻性的技术参考与决策支撑。





声 明

本《技术报告》版权属于网安标委秘书处，未经秘书处书面授权，不得以任何方式抄袭、翻译《技术报告》的任何部分。凡转载或引用本《技术报告》的观点、数据，请注明“来源：全国网络安全标准化技术委员会秘书处”。



全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC



技术支持单位

本《技术报告》得到信通数智量子科技有限公司、中国电子技术标准化研究院、国科量子通信网络有限公司、长春吉大正元信息技术股份有限公司、四川大学、国家计算机网络应急技术处理协调中心、中国移动通信集团有限公司、中国电信集团有限公司、中国信息通信研究院、华为技术有限公司、中兴通讯股份有限公司、安徽国科量子通信网络有限公司、中国汽车工程研究院股份有限公司、北京邮电大学等单位的技术支持。

主要编写人员：魏瑛、王秉政、姜世昌、李武璐、王祥通、李炜、杜海涛、张屹、陈悦、舒敏、程明、赖俊森、杨洋、李明翰、周继华、谷勇浩。



摘 要

卫星通信网络是我国网络基础设施的重要组成，卫星通信利用高、中、低轨卫星可实现广域或区域覆盖。根据《建立卫星通信网和设置使用地球站管理规定》，“卫星通信网，是指利用卫星空间电台进行通信的地球站组成的通信网。本规定所称的地球站，是指设置在地球表面或者地球大气层主要部分以内的、与空间电台通信或者通过空间电台与同类电台进行通信的电台。”

卫星通信网可由航天器、地面测控站、运控站、信关站（关口站）、卫星通信应用设备（用户终端/地球站）等组成，实现全球或区域、大时空范围的通信互联，提供卫星专线通信、卫星接入互联网等通信服务。卫星通信网络的安全性、健壮性及可靠性要求高，其自身固有特点与传统地面网络相比，具有航天器高动态、大延时、广分布、轨道规律性等特点，使得卫星通信网络易受到攻击和干扰，如空间链路信息截获、信息伪造、干扰入侵等。卫星通信网络将与地面网络，如移动通信网络、地面固定网络、互联网等形成互联，因此存在跨域、多网融合、境外接入及应用等挑战及风险。由于智能终端直连卫星的应用发展，对卫星通信网络接入的攻击面及卫星通信基础设施面临的挑战及安全威胁进一步加大。

本报告聚焦卫星固定业务(FSS)与卫星移动业务(MSS)的网络安全标准，研究范围包括卫星通信网络的空间段、地

面段及用户段通信互联的网络和通信安全、与地面网络互联安全、卫星用户应用安全。本报文不涉及传统航天安全保障内容，如火箭发射可靠性、轨道入轨精度、卫星平台热控与电源稳定性、安全管理、物理安全等。

本报告梳理了卫星通信技术产业和相关政策标准现状，分析了研究范围相关的卫星通信网络安全风险和问题，研究了卫星通信网络安全标准需求，提出了卫星通信网络安全标准体系框架。本报告可为卫星通信的卫星固定与移动业务等领域网络安全标准制修订工作提供参考。



目 录

1 引言	1
1.1 研究背景	1
1.2 研究范围	1
1.3 研究思路及报告内容	4
2 国内外发展现状	7
2.1 国外发展现状	7
2.2 国内发展现状	15
2.3 小结	23
3 安全风险与重大问题分析	24
3.1 安全风险概述	24
3.2 安全问题分类	26
3.3 重大风险分析	31
3.4 小结	37
4 安全相关政策与标准分析	38
4.1 安全相关政策	38
4.2 标准分析	41
4.3 小结	50
5 卫星通信网络安全标准框架和需求分析	52
5.1 卫星通信系统组成与接口	52
5.2 标准框架分析	55
5.3 卫星通信网络安全架构实例	58

5.4 网络安全标准化需求分析	66
5.5 小结	68
6 卫星通信网络安全标准化工作建议	69
6.1 总体思路	69
6.2 标准体系设计说明	70
6.3 标准体系建议	71
6.4 小结	83
附录 A 相关政策法规清单（国际/国内）	84
A.1 国内概览	84
A.2 国际概览	85
附录 B 相关标准列表（国际/国内）	87
B.1 国际标准	87
B.2 国内标准	93
参考文献	100



卫星通信网络安全标准化技术研究报告

1 引言

1.1 研究背景

卫星通信网络是国家网络基础设施的重要组成。基于“安全是发展的前提，发展是安全的保障”的指导思想，在推进卫星通信网络建设的同时，必须同步构建网络安全保障体系。

卫星通信网络作为通信的关键基础设施，其网络的安全性、健壮性及可靠性要求高。区别于传统地面网络，卫星通信网络主要面临以下风险：

- (1) 卫星通信网络与传统地面网络相比，具有高动态、大延时、广分布、轨道规律性等特点，使得空间链路易遭截获、伪造、干扰等攻击。
- (2) 卫星通信网络将与移动网络、互联网等地面网络互联，因此存在跨域、多网融合、境外接入等安全风险和挑战。
- (3) 智能终端直连卫星扩大了接入面，对卫星通信网络接入安全及网络基础设施构成更大威胁。

本文件聚焦卫星固定业务（FSS）与卫星移动业务（MSS）的共性网络安全标准，针对上述风险，系统阐述安全需求及标准化建议。

1.2 研究范围

1.2.1 卫星通信网络范畴

本文件所称卫星通信及业务范畴，主要参考文件《工业和信息化

部关于优化业务准入促进卫星通信产业发展的指导意见》（工信部信管〔2025〕180号，2025年8月25日）、《工业和信息化部关于印发“十四五”信息通信行业发展规划的通知》（工信部规〔2021〕164号）和《建立卫星通信网和设置使用地球站管理规定》（中华人民共和国工业和信息化部令 第7号，2009年3月1日）。

本报告聚焦卫星固定业务（FSS）与卫星移动业务（MSS）的网络安全标准，研究范围包括卫星通信网络的空间段、地面段及用户段通信互联的网络和通信安全、与地面网络互联安全、卫星用户应用安全。

《建立卫星通信网和设置使用地球站管理规定》中指出：“本规定所称的卫星通信网，是指利用卫星空间电台进行通信的地球站组成的通信网。本规定所称的地球站，是指设置在地球表面或者地球大气层主要部分以内的、与空间电台通信或者通过空间电台与同类电台进行通信的电台。”《工业和信息化部关于优化业务准入促进卫星通信产业发展的指导意见》在“有序扩大市场开放”中提出“一是支持低轨卫星互联网加快发展。二是支持开展终端设备直连卫星业务。三是支持探索新型卫星通信业务：组织开展卫星物联网商用试验，支持符合条件的企业依托低轨卫星物联网星座，为天空、海洋、偏远地区等地面网络无法覆盖的区域，提供广域物联网连接服务。”

从上述政策文件中可见，卫星通信的范畴更宏观，卫星互联网属于卫星通信产业发展中有序扩大市场开放的一种，低轨卫星互联网、卫星物联网等是当前卫星通信网络主要发展及应用的方式。

1.2.2 主要服务区

依据GB/T 12364-2007《国内卫星通信系统进网技术要求》中6.1指出：“工作在C、Ku 和 Ka 频段上的国内通信卫星天线主瓣，应能覆盖我国的全部领域，其中包括大陆、台湾和海南岛等 90%（考虑到指向误差在内）以上地区为主要服务区。中沙、西沙、南沙群岛为降级服务区。在主要服务区内，卫星性能必须满足各种传输系统规定的技术指标。”

1.2.3 主要卫星业务

采用国际电信联盟（ITU）对卫星业务的分类方式，本文件提到的主要卫星业务包括卫星固定业务（FSS）和卫星移动业务（MSS）。

传统的卫星通信典型业务包括且不限于：基于地球静止轨道（GEO）卫星开展的卫星固定通信、卫星移动通信、卫星中继通信等；基于中地球轨道（MEO）、倾斜地球同步轨道（IGSO）卫星开展的覆盖范围更广的卫星通信、中继通信等。

工业和信息化部于2025年3月发布《卫星网络国内协调管理办法（暂行）》中指出：“卫星网络国内协调（以下简称国内协调）是指在国际电联《无线电规则》框架下，我国卫星网络之间、卫星网络与地面无线电台（站）之间的频率协调”；其附件1《国际电联空间无线电业务常用建议书》中描述的“卫星固定业务”的无线电业务的建议书涵盖的业务类型及协调关系中，包括且不限于：

- (1) 卫星固定业务的卫星网络，含对地静止轨道/卫星固定业务；

非对地静止轨道/卫星固定业务；非对地静止轨道/卫星移动业务馈线链路；

(2) 非对地静止轨道/对地静止轨道卫星间链路之间、对地静止轨道/对地静止轨道卫星间链路之间；

(3) 非对地静止轨道卫星间链路；

(4) 卫星固定业务的地球台站与固定业务中的站点之间。

1.3 研究思路及报告内容

1.3.1 研究思路

本研究围绕我国卫星通信网络安全标准体系建设开展。

首先，系统开展我国卫星通信网络行业、技术及产业发展现状调研，全面跟踪国内外的技术演进与发展趋势，厘清产业基础、技术能力和应用格局。

第二，结合卫星通信网络发展趋势、政策法规要求及现有标准基础，深入分析研究对象面临的新型安全威胁与挑战，识别关键风险点，研判当前及未来一段时期的重大安全问题。

第三，在梳理国内外卫星通信网络安全相关标准化进展的基础上，从基础共性、网络安全技术、设备与应用安全、检测评估等维度，开展网络安全技术标准体系研究，明确重点领域的标准化需求。

第四，基于上述分析，提出符合我国卫星通信网络安全发展需求的标准化工作建议，为后续标准研制、政策制定和产业引导提供支撑。

在标准体系建设上将具体考虑：

- (1) 在结构上，采用国际、国内标准常见的卫星通信系统结构描述习惯；
- (2) 在内容上，对卫星通信网络安全的内容需涵盖星-间、星-地、地-星、地-星-地、地-星-星-地等通信互联方式下的数据与传输安全、地面网络互联安全、卫星用户应用安全等，其中与“星”相连的“地”广义应用场景上还包括航空器、无人机等；
- (3) 在方法上，参考我国网络安全等级保护、密码应用基本要求、关键基础设施保护要求、个人信息保护等相关要求；
- (4) 在先进性及标准体系协调上，兼顾 ISO、ITU、3GPP、NIST、ETSI 等相关标准化推进及内容的协调，在考虑兼容的同时，条件成熟时可推进我国卫星通信网络安全标准研究的国际化。

1.3.2 报告内容概述

第1章：引言。主要进行了课题范围、研究思路的综述。

第2章：国内外发展现状。主要从国内外通信卫星、星座的技术发展、行业应用与产业发展等维度，描述了卫星通信行业及网络安全相关的国内外发展现状。

第3章：安全风险与重大问题分析。主要从卫星通信网络面临的安全风险、安全问题分类、重大风险等进行了分析。

第4章：安全相关政策与标准分析。主要调研了卫星通信领域相关国内外政策、标准化组织及其网络安全相关标准研究与制定情况。

第5章：卫星通信网络安全标准架构和需求分析。主要分析了卫星通信系统架构、网络安全标准架构的多种模型方法与实例，经分析

提出了网络安全标准化需求。

第6章：卫星通信网络安全标准化工作建议。主要从标准体系总体思路、标准体系设计说明、卫星通信网络安全标准体系描述及标准制定建议。

附录A：相关政策法规清单（国际/国内）。

附录B：相关标准列表（国际/国内）。

参考文献。



全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

2 国内外发展现状

2.1 国外发展现状

欧美国家卫星通信领域技术发展较为领先。随着各国相继发布卫星通信网络建设部署计划，波音、空客、亚马逊、谷歌（Google）、一网（OneWeb）、美国太空探索技术公司（SpaceX）等高科技企业纷纷投资卫星通信领域，提出了OneWeb、Starlink等10余个卫星通信系统方案及建设。据不完全统计，截至2025年10月国外卫星发射和在轨数量统计如表2-1。

表 2-1 截至 2025 年国外卫星发射和在轨数量统计

国家或地区	2024年发射数量	占比	2025年发射数量 (1-10月)	占比	当前在轨数量	占比
美国	2296	87.43%	2875	91.39%	9713	81.29%
欧州	36	1.37%	42	1.34%	1092	9.14%
俄罗斯	103	3.92%	43	1.37%	318	2.66%
日本	19	0.72%	17	0.54%	105	0.88%
印度	12	0.46%	11	0.35%	72	0.60%
其他	160	6.09%	135	4.29%	649	5.43%
合计	2626	100%	3146	100%	11949	100%

国外由于移动通信基站数量较少，基站覆盖率不足，许多偏远地区的通信需求未能得到满足，这部分通信需求的弥补是国外卫星通信市场发展的短期驱动力。

2.1.1 通信卫星系统

美国的通信卫星发展水平处于世界领先地位，拥有完整的天基侦察、预警、通信系统，并在继续发展新技术以满足未来的探测、覆盖、通信、目标特性及定位精度的需求。美军积极推进“大规模弹性太空体系”建设，发展能力更为先进、更具弹性抗毁的新一代军事通信卫

星体系。

主要卫星通信的星座包括商用宽带通信卫星、军事通信卫星、低轨卫星星座等。其中安全能力较多体现在军事通信卫星。

(1) 美军军事通信卫星

2006年，美国国家航空航天局（National Aeronautics and Space Administration，简称NASA）发布的《2005~2030年NASA空间通信与导航体系结构建议》中对空间通信中安全机制给出了框架性的指导建议。建议使用对称加密算法来进行认证与加密。

先进极高频军用通信卫星系统（AEHF）是美国2010年至2020年期间逐步建设的新一代高防护性能的地球静止轨道军事通信卫星系统。可满足实时图像、战场地图和跟踪数据传输等战术通信需求，成为美国国防部在军用卫星通信体系结构中期阶段使用的骨干系统，为美军关键战略和战术部队提供防截获、抗干扰、高保密和高生存能力的全球卫星通信。

(2) 美军新一代军事卫星通信系统

美军新一代军事卫星通信系统包括窄带、宽带和受保护卫星等三大部分，负责为美军提供多维信息连接和通信服务。

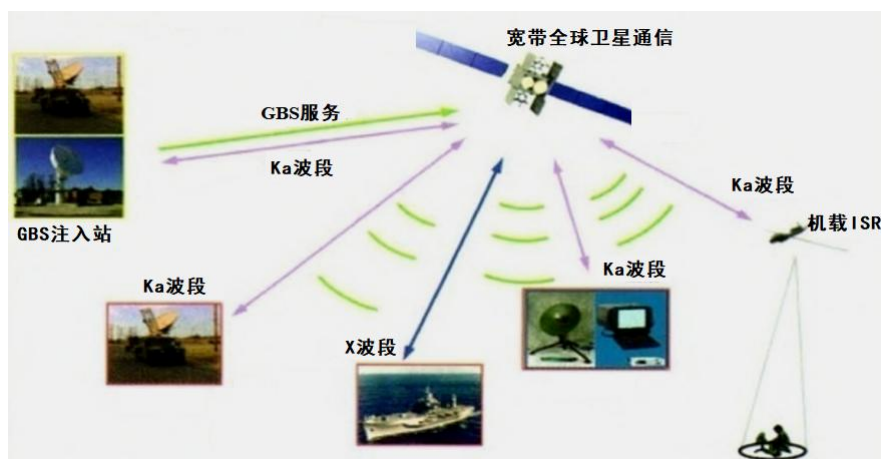
a) 窄带系统

窄带系统采用UHF频段，主要为用户提供话音、低速率数据、移动通信等服务；卫星上搭载有特高频和极高频（EHF）的通信载荷，实现与“军事星”的互联互通，可用于全球战略、战术通信。卫星采用抗干扰与抗电磁脉冲加固措施，可提供全球范围内的舰-舰、舰-岸，

舰-机话音、数据通信。

b) 宽带系统

采用X频段和Ka频段，主要实现大容量、高速率数据通信；美军宽带全球卫星通信系统（WGS）示意图如图2-1所示。



（图注：GBS（Global Broadcast Service）在卫星通信中指全球广播服务；机载ISR指机载情报、监视与侦察。）

图 2-1 宽带全球卫星通信系统示意图

卫星采用先进的数字信道化技术和相控阵天线技术，可形成9个X频段500MHz和10个Ka频段1GHz波束。根据频率规划分为数个125MHz信道。WGS-1～3卫星可利用125MHz带宽支持137Mbps的无人机传输速率。WGS-1 卫星在轨测试期间表明，在125MHz信道上使用16APSK调制（16进制振幅移相键控，通过调整信号的振幅和相位来传输数据的一种调制方式）可以实现440Mbps的传输速率。

c) 受保护系统

采用 EHF 频段的先进极高频卫星通信系统（AEHF）主要解决了保密、抗干扰、防探测和防非授权进入等问题，适用于保密通信。每颗卫星的通信容量 430Mbps；用户数据速率：战术用户 8.192Mbps，

战略用户 19.2kbps 可以服务 6000 个终端和 4000 个网络；星间链路数据速率 60Mbps，星间链路增强了路由功能和抗干扰能力。采用的保护措施包括且不限于抗干扰措施、低截获概率、低检测概率，以及先进的加密系统。

2.1.2 低轨卫星星座

相较于传统的地面通信网络，低轨卫星通信网络能减少信号传输延迟，从而提供更高效率的通信服务，尤其适合为偏远地区、海洋、航空等地面网络覆盖不佳的区域提供网络连接。当前以美国太空探索技术公司（SpaceX）“星链”（Starlink）星座、亚马逊公司（Amazon）

“柯伊伯”（Kuiper）星座为代表的低轨通信卫星星座，不仅推动了航天产业变革，也对各国的巨型星座监管制度提出了全新挑战^[28]。

国外主要卫星互联网星座计划及部分参数如图2-2所示。

国家	公司	星座名称	卫星数量/颗	建成年份	轨道高度/km	频段	用途
美国	SpaceX	StarLink	11927	2027	1130	Ku, Ka, V	宽带
美国	依星公司	第二代依星	75	2018	780	-	宽带、STL
美国	波音	波音	2956	2022	1200	V	宽带
美国	亚马逊	Kuiper	3236	-	590/610/630	Ka	宽带
美国	Facebook	Facebook Athena Project	77	-	1200	-	-
韩国	三星	三星	4600	-	1400	-	宽带
英国	OneWeb	OneWeb	2468	2027	1200	Ku, Ka, V, E	宽带
加拿大	Tolesat	Tolesat	298	2023	1248/1000	Ka	宽带
加拿大	ACC Clyde	Kepler	140	2022	-	Ku/Ka	物联网
印度	Astrome	Space Net	150	2020	1400	毫米波	宽带
俄罗斯	Yaliny	Yaliny	135	-	600	-	宽带
德国	KLEO Connect	KLEO	624	-	1050/1425	Ka	工业物联网

（图注：数据来源中国信通院、东吴证券研究所）

图 2-2 国外主要卫星互联网星座计划

(1) SpaceX 星链（Starlink）计划

2016年11月15日，美国太空探索技术公司SpaceX向美国联邦通讯委员会（FCC）提交了星链（Starlink）小卫星星座计划，建立小卫星

互联网星座，并在全球范围内提供互联网接入服务。星链（Starlink）通信通过地面接收器和距地表550KM的低轨卫星实现信号的传输，传输速率最高可达到100Mbit/s。星链已支持百万级用户的访问、美国地区峰值时段下行链路速率中值达200Mbit/s；即便是低速套餐，也能稳定提供100Mbit/s的下载速率与20Mbit/s的上传速率，满足高清视频、云协作等带宽密集型应用需求。在时延控制上，通过部署激光星间链路和优化网关布局，美国用户的网络平均时延降至25.7毫秒，其中99%的测量值低于55毫秒，这一指标已接近地面光纤网络水平。

截至2025年9月底，SpaceX已完成311次“星链”卫星专项发射，共9922颗星链卫星被发射升空，其中8195颗带有激光星间链路，674颗具备直连手机能力。在全球已建成151座信关站，在全球140余个国家或地区提供服务，SpaceX通过“星链”全方位进军卫通市场，将大众消费宽带（toC）作为主营模式，快速抢占人口及流量，2024年9月用户数量突破400万；2025年9月底，用户数量突破700万。Starlink卫星系统结构示意图如图2-3所示。

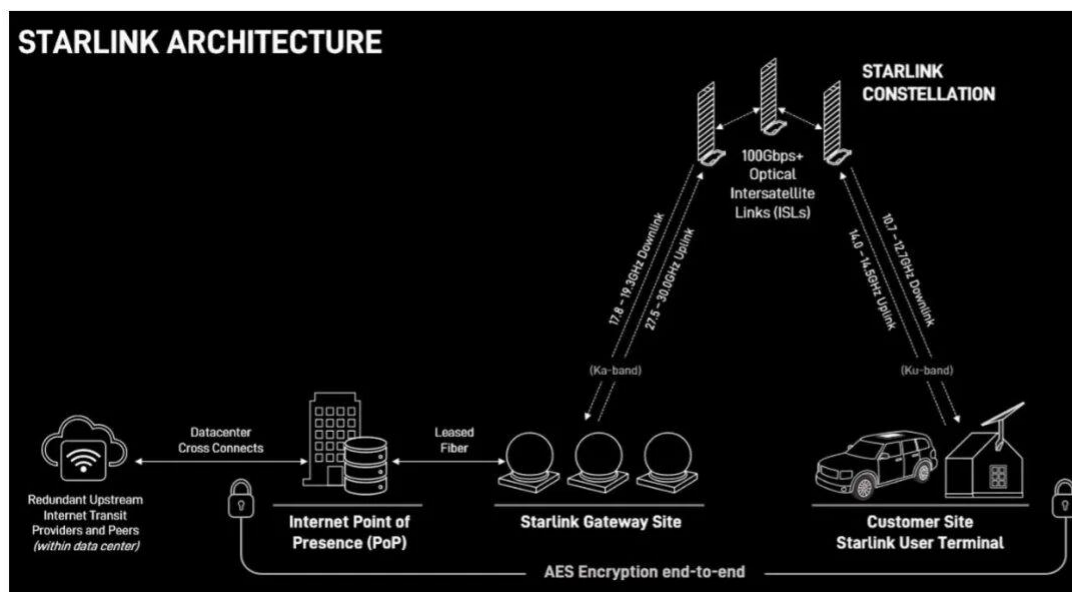


图 2-3 Starlink 卫星系统结构示意图^[33]

图 2-4 中，Starlink 卫星系统结构中包括了用户节点的 Starlink 用户终端通过 Ku 频段上下行链路接入 Starlink 星座；Starlink 星座再通过 Ka 频段上下行链路，与 Starlink 关口站（Starlink Gateway Site）连接；关口站通过光缆与互联网接入点 PoP 节点（Internet Point of Presence，简称 PoP）连接，从而实现与上游丰富的互联网传输提供商的数据中心连接。Starlink 星座具有 100Gbps 可选的星间链路（ISLs）。通过卫星通信的 Starlink 用户终端与数据中心应用之间采用 AES 算法的端到端加密。

(2) 亚马逊公司柯伊伯计划（Project Kuiper）

柯伊伯星座（Project Kuiper）是美国亚马逊公司发起的一个低轨卫星互联网项目，旨在提供全球宽带覆盖。柯伊伯星座共规划 3296 颗卫星，已发射 131 颗卫星。

在卫星地面站领域，亚马逊公司利用网络服务地面站（AWS Earth Station，简称 AWS 地面站）已广泛开展“地面站即服务”业务，该

业务主要针对遥感卫星产生的数据，并与黑色天空公司（BlackSky）等多个遥感卫星企业展开合作。Kuiper 星座地面站用于连接 Kuiper 卫星提供宽带接入服务，同时未来可与 AWS 地面站联合组成亚马逊公司的全球云服务网络。Kuiper 除地面站服务外，还在美国 5G 业务中提供回程传输服务，以持续深化其捆绑式服务商业模式^[45]。

(3) 欧洲航天局“6G 在轨实验室”

欧洲航天局（European Space Agency，简称ESA）建设“6G在轨实验室”（6G LINO），用于欧洲6G标准化工作，处于6G应用的早期阶段。ESA选择德国 Tesat 公司建立“6G在轨实验室”，利用16U立方星，开展端到端连接、卫星和地面移动网络整合相关研究，使卫星行业能够调整技术、产品和使用案例，与地面通信基础设施同步进行 6G 工作。

2.1.3 空间安全技术与应用

为确保卫星通信网络的健壮、可靠与安全，国际和国内卫星通信网络采取了若干系统方法或开展了关键技术验证，相应的技术工程包括且不限于：

- (1) **建设卫星星座：**卫星采用了模块化和组合设计，独立功能形成单独小卫星，运行在主卫星附近，一旦某颗卫星失效，新卫星将很快更换上去，这些飞得很近的小卫星共同组成一个星座，星座间用无线网络互连；
- (2) **低轨道卫星星座：**节省功率、携带推进剂少和小卫星便于发射；
- (3) **采用扩展频谱和跳频等抗干扰技术：**卫星通信系统采用多种扩

频方法，通过扩频及跳频等技术途径提高抗干扰能力；

(4) **卫星轨道机动技术**：利用卫星自身机动能力，既能够机动灵活地在轨道上运行，躲避反卫星武器的攻击进行被动防御，又可以在其上安装空间监视装置，攻击告警装置和针对威胁的对抗装置，部署在主卫星周围进行伴飞，当发现有针对卫星的攻击行为时，可以针对攻击进行诱骗、阻挡或拦截等主动防御；

(5) **建立自我修复的网络NTDR**（Near Term Digital Radio 近场数字电台）：NTDR网络功能提供多跳通信，利用多跳通信，NTDR可以构建多级网络，而每一级的网络又分为若干群，每一个群有一个群首。群成员可以在各个群之间漫游，而当群首出现故障时，网络系统会自动推选出新的群首，从而使得NTDR网络的稳定性和持续性特别好；

(6) **空间量子网络**：欧洲 LaiQa项目（关键密钥分发空间组件）项目是欧洲多个机构联合参与的量子通信项目，2024年启动，为期3年，旨在构建适用于太空环境的量子密钥分发网络。由雅典通信与计算机系统研究所、荷兰国家应用科学研究院等机构合作，并获得欧盟资助。聚焦量子通信关键技术研发，包括量子密钥分发、量子加密通信等，计划突破太空环境下的技术限制，获得空间量子网络的应用与试验；

(7) **“坚定太空2025”建立空间作战演习与网络战靶场**：2025年7月到8月，美太空军组织开展“坚定太空2025”全领域太空战演习，涉及电磁战、轨道战与网络战靶场，并实现轨道战、电

磁战、网络战三大作战域深度融合，系统性演练了太空态势感知、卫星通信、定位、导航与授时、情报、监视与侦察、导弹预警、指挥控制等关键任务领域。该演习采用全球分布式部署架构，美太空军位于分散地区的不同部门可通过云端开展联合训练，验证了美太空军全球一体化联合作战能力^[34]。

2.2 国内发展现状

2.2.1 发展概述

2020年4月国家发展改革委将卫星互联网纳入新型基础设施建设范畴。2021年，工信部在《“十四五”信息通信行业发展规划》中提出“要加快布局卫星通信：加强卫星通信顶层设计和统筹布局，推动高轨卫星与中低轨卫星协调发展；推进卫星通信系统与地面信息通信系统深度融合，初步形成覆盖全球、天地一体的信息网络，为陆、海、空、天各类用户提供全球信息网络服务。”

我国卫星通信产业链示意图如图2-4所示。

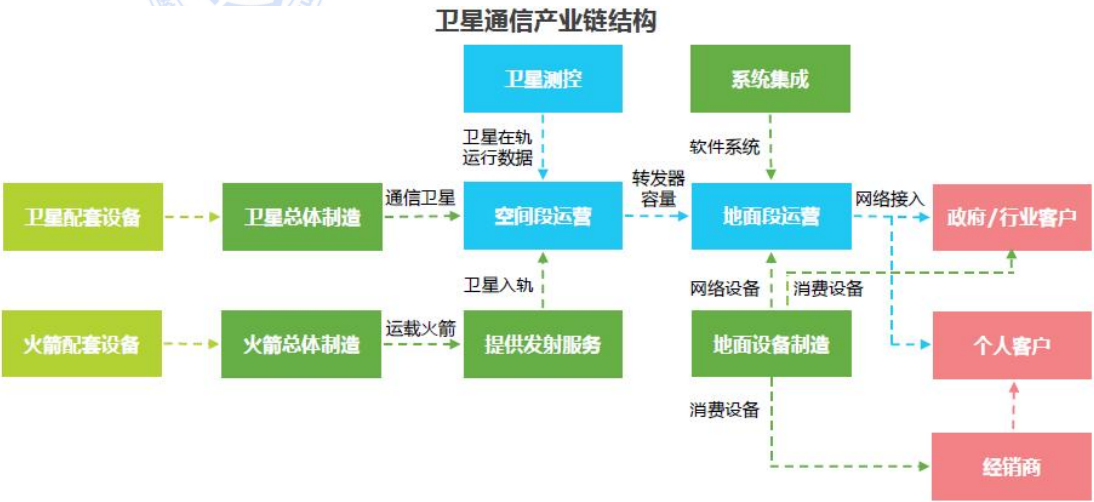


图 2-4 卫星通信产业链^[8]

我国卫星通信的技术与应用不断发展，主要体现在：单任务向高密度、多任务网络化发展；任务频度由偶发低密度向常态高密度发展；卫星通信承载能力从窄带向宽带、高速率、大连接、综合业务发展；卫星通信应用设备从传统固定、移动、车载、船载、手持等专用卫星通信设备，逐步向智能化、综合型的固定终端、移动终端卫星应用、多网互联互通方向发展。

当前卫星通信的发展，面临频谱资源的逐步紧缺；受到国际上高通量卫星、新一代先进技术卫星、低轨商业卫星星座的快速发展，抢占卫星轨道、频率资源；为可持续利用空间资源、确保卫星通信安全；并开展新一代信息技术，如6G技术的发展演进等是国内卫星通信市场发展的主要驱动力。

2.2.2 卫星通信应用发展

图2-5展示了近年来代表性的卫星星座、提供的卫星通信服务及卫星下载通信速率的基本情况。



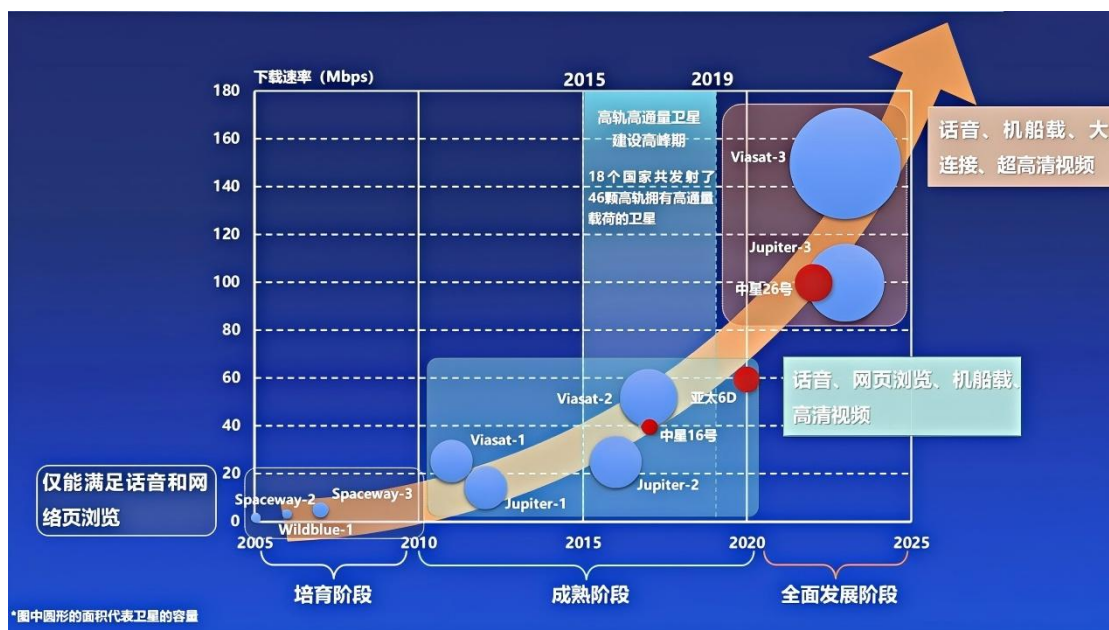


图 2-5 卫星通信发展代表星座及应用^[12]

图2-5中可见，国际国内卫星互联网行业经过培育与发展，在2020年后迎来了全面发展阶段。业务类型从仅满足语音及窄带通信，逐步发展到支持语音、窄带通信、宽带通信、大连接，满足高清/超高清视频应用等。

目前，我国由中星、亚太、亚洲、天通系列等构成在轨商用通信卫星已达几十颗，信号覆盖了全球主要国家和地区。

2.2.3 卫星通信安全技术发展

我国在航天领域方面安全管理和密码应用开展了积极的研究和实践工作。我国航天密码应用及安全管理发展分为多个阶段，包括但不限于：

- (1) 单星地面端到端防护，主要解决卫星通信信道保护问题；
- (2) 星地安全防护阶段，主要解决航天器遥控、遥测和载荷（业务）等安全防护；

- (3) 多星多系统融合，主要解决星地、星间的测控、载荷（业务）、星间组网等安全防护；
- (4) 天地一体业务融合阶段，主要面向空间互联网、低轨卫星星座等航天系统应用发展，构建适应天基、地基天地一体化综合安全防护能力，满足大范围时空域、多层次、广泛互联、自主可控、抗毁顽存的安全防护及管理能力，含星间通信的卫星通信应用示意图如图2-6。

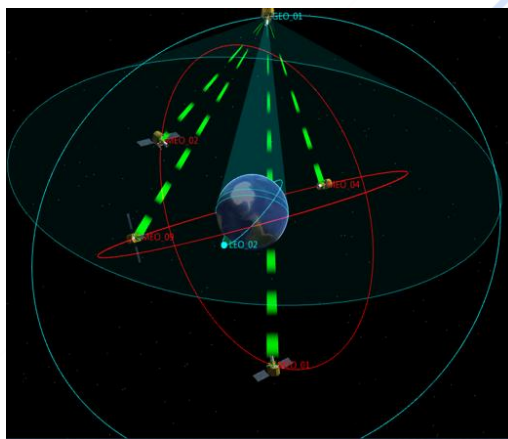


图 2-6 含星间通信的卫星通信应用示意图

2.2.4 卫星通信业务

2.2.4.1 卫星固定业务（FSS）

卫星固定业务（Fixed Satellite Service, FSS）是利用1颗或多颗卫星，在位于各特定的固定点上的地球站之间的无线电通信，包括空间无线电业务的馈电链路、星间业务等。

无线电业务中的卫星固定业务是利用一个或多个卫星在处于给定位位置的地球站之间的无线电通信业务；该给定位置可以是一个指定的固定地点或指定区域内的任何一个固定地点；在某些情况下，这种

业务也可包括运用于卫星间业务的卫星至卫星的链路；也可包括其他空间无线电通信业务的馈线链路^[46]。

GEO地球静止轨道卫星位于赤道平面中的圆轨道上，稳定点处距地面的标称距离约为36000km。理论上3颗就能覆盖全球；对空间指向保持固定。但因距离地球较远，通信延时达到几百毫秒。GEO卫星广泛提供了甚小口径卫星终端站VSAT（Very Small Aperture Terminal）通信、电视直播到户、电视节目传播、应急通信等卫星通信服务。

国内在轨民用卫星如中星系列、鑫诺（4颗）、亚太（4颗）、亚洲（6颗）等。覆盖区域包括大部分亚太地区、大部分非洲地区、一部分欧洲地区、大部分印度洋地区、太平洋亚太部分地区。FSS业务服务主要包括卫星通信、电视直播、转发器租赁；运营机构包括中国卫通、亚太卫星、中信卫星等。卫星运营商提供转发器租赁业务，由用户自行构建语音、视频、数据等业务系统，可实现静中通、动中通功能。

2.2.4.2 卫星移动业务（MSS）

卫星移动业务MSS（mobile-satellite service）是在移动地球站和一个或多个空间电台之间的一种无线电通信业务，或该业务所利用的各空间电台之间的无线电通信业务；或利用一个或多个空间电台在移动地球站之间的无线电通信业务^[46]。

MSS可通过订购商用卫星（如天通、海事、铱星、瑟拉亚、亚洲蜂窝等）信道资源实现。地面站设备包括车载、船载、机载设备，便

携的手持移动终端等。移动卫星业务系统的管控及资源分配由卫星运营组织，终端所属的频段区间、波束位置均为公开信息。支持电话、视频、数据交换等业务，可提供与公共交换电话网络（PSTN）、公共陆地移动通信网（PLMN）互通。

我国自主建设的移动通信卫星“天通一号”已于2020年正式商用，支持1.2Kbps 电路域话音、最高分组域384Kbps 数据业务。主要服务覆盖范围是我国境内、领海及其外延200km。2020年、2021分别成功发射02星、03星，主要服务覆盖范围在西太平洋、东南亚地区。天通卫星应用示意图如图2-7所示。

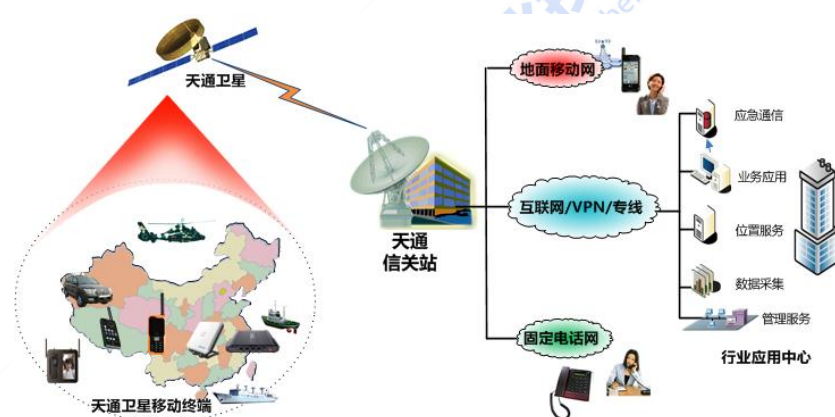


图 2-7 天通卫星应用示意图^[15]

天通卫星通信应用支持卫星电话、短信、窄带数据传输等，典型业务参数如下：

- (1) 卫星电话：可拨打全球任意地面固定和移动电话，业务速率：1.2kbps、2.4kbps和4kbps；
- (2) 短信：可与地面移动通信终端互通；
- (3) 传真（G3类传真）：传真速率：9.6kbps；
- (4) 位置服务：系统提供自主定位和北斗/GPS等定位方式，支持位

置管理和追踪功能；

(5) 数据传输/互联网接入/视频回传：速率能达到384Kbps；

(6) 低数据速率（Low Data Rate）数据功能：支持9.6kbps分组和9.6kbps物联网等。

卫星机动通信系统多采用甚小口径卫星终端站VSAT（Very Small Aperture Terminal）体制，通过自主建设卫星系统实现。卫星机动通信系统采用的网络安全管理目前集中于业务传输层，利用信道加密技术实现对业务数据、信令信息等进行加密保护。采用信道加密保护能保证VSAT组成的卫星通信信息传输安全，便于话音、传真、IP数据等不同类型的业务的透明接入，不影响系统链路的有效带宽。利用卫星转发器作为中继反射或转发无线电信号的通信方式。

2.2.4.3 卫星广播业务（BSS）

卫星广播业务（broadcasting-satellite service），是利用空间电台发送或转发信号，以供公众直接接收（包括个体接收和集体接收）的无线电通信业务^[46]。截至2023年10月，中国卫通向边远地区累计超过上亿户家庭提供直播到户服务，为近千套广播电视节目提供传输服务。

2.2.5 典型卫星系统

2.2.5.1 高通量宽带卫星系统

2017年发射的首颗高通量Ka宽带卫星“中星16号”，标志着我国进入高通量卫星通信新时代。容量达到 20Gbps，主要面向远程教育、医疗、机载和船舶通信、应急通信等领域的互联网接入，不面向个人

移动用户。由中国航天科技集团五院2019年发射成功的“中星20号”高通量试验星验证了高通量激光通信、新型通信卫星平台等技术试验任务。我国2023年2月成功发射“中星26”，共94个用户波束，整星通信容量100Gbps。计划“中星27号”整星容量近300Gbps^[11]。

2.2.5.2 低轨卫星星座

低轨卫星在典型高度160km~2500km的圆轨道上运行，单颗卫星的通信窗口时间在几分钟~十几分钟。为实现覆盖全球或较大区域，需要多个LEO卫星构成的星座，星座内卫星相互连接，满足通信要求，也带来了系统的复杂度。

LEO卫星的特点主要包括且不限于：

- (1) 星地链路短，路径损耗低，可使用低功率，小口径天线的地球站；
- (2) 传输时延较小，可覆盖两极地区；数据传输延迟可实现50ms内时延，与地面光纤网络相当，路径损耗小；
- (3) 多个卫星组成的星座可以实现真正的全球覆盖，实现三维空间信号普遍覆盖与服务能力；
- (4) 支持广域复杂网络拓扑的构成能力、可扩展能力，支持与地面云（数据）运营服务商的接入、互联网接入、广域广播或多组播能力；
- (5) 多星座的组合形成在故障恢复、容错等方面的优势。

LEO卫星面临的挑战包括且不限于：频谱资源有限，多星座的造价高；大型星座增大了设计与管理难度；有待提升卫星应用效率；推

广 LEO星座的普遍通信服务，以及具备与地面通信网络有竞争力的消费成本。

中国计划2024年~2030年部署3个“万星座”计划（总规模超3.7万颗），以获取6万~10万颗低轨容量中的资源份额，其中包括上海垣信1.4万多颗低轨宽频多媒体卫星组成“千帆星座”（G60），中国星网1.3万颗卫星组成的“GW星座”，蓝箭鸿擎1万颗卫星组成的“鸿鹄-3星座” [25]。

其他星座还包括长光卫星计划在轨卫星数量将增加至 300 颗。实现对偏远和网络不发达地区的宽带互联网接入。之江星座构建天基智能计算基础设施，通过算力分布式调度，实现数据在轨实时传输和运算，为通信、导航、遥感和空间科学等卫星提供天基计算服务。东方慧眼（Oriental Smart Eye, OSE）智能遥感卫星星座计划将开展通导遥一体化、卫星星座组网观测、在轨处理和人工智能等关键技术。

2.3 小结

卫星通信系统所形成天地组网可以在广域信息感知、通信和指控支持、信息中继和太空对抗等方面起到非常关键的作用，卫星通信网络应用随着军事和社会用途的不断丰富，为指挥控制、载荷应用、网络空间异构互联、通信服务、空间资源利用等核心能力提供支撑。新一代卫星通信系统向通信宽带化、业务综合化、移动终端多样化、广泛互联互通方向发展，在面临新的市场与产业发展机遇的同时，也面临着安全威胁、风险与挑战。

3 安全风险与重大问题分析

卫星通信系统面临着自身特点带来的网络安全风险、工程实现安全共识不足带来的隐患，智能手机直连卫星加剧了卫星通信系统接入面临的数量上的急剧增大、复杂性的提升与风险的加剧。同时，技术发展、软件故障、空间环境的威胁始终对卫星通信系统的稳定和安全应用带来了挑战。

3.1 安全风险概述

卫星通信系统是一个规模庞大、结构复杂的空间与地面共同构成的网络，具有大时域、大空域、外层空间运行的特点；具有高动态、长寿命，广域无线网络空间通信链路暴露、易干扰、高延时；具有节点运动快，拓扑变化快、网络时延抖动较频繁，网络的安全状态保持面临挑战。

根据卫星通信网络的建设及应用特征，使得其在面临传统的物理和环境威胁、网络与通信威胁、设备和计算安全威胁、应用与数据安全威胁的基础上，还存在以下挑战，为保证卫星通信网络可用、可信、可控、可管，面临巨大难题。

（1）受限于天地网络的大时空管域：难度大、攻击面广

融合天地一体化网络，地面移动通信网、电话网、互联网等多种异构网络，卫星通信网络容易受到来自各种网络、跨境、跨域，多网系的互联带来的风险。

以无线电通信系统为主的天网、地网存在较大攻击干扰面。包括物理攻击、链路、网络攻击，传输/控制层到应用层的各种攻击。

跨境、跨域面临接入认证、授权服务、协议转换、传输安全、内外域隔离、跨不同安全层级的互联、隔离等风险及安全防护需求。

(2) 技术依赖性强，难以直接通过物理管理手段

空中卫星面临节点多、环境特殊。在地面难以实施物理管控防护手段。存在管不到、管控窗口短、管控手段有限、时延大、境外留存时间长等。

航天器运行具有规律性、实体及空间信息传输易受到窃听、毁坏等攻击威胁。

(3) 太空环境资源有限，空间环境适应性

针对有限信道、通信资源的卫星通信网络为不同用户提供差异化的通信服务，包括服务质量 QoS (Quality of Service)、服务带宽、通信安全要求等差异化需求。适应空间环境干扰(太阳辐照、单粒子翻转等)、满足不同轨道卫星在与地面或星间链路进行长距离传输时的空间信息传输的有效性、可靠性及安全性给安全带来了挑战。

(4) 卫星寿命长，面临不断增长的新的安全威胁

卫星通信网络设计和建设周期超过十年，安全防护系统随着系统规模、组网架构和服务应用的拓展，以及针对系统新型安全威胁的出现，安全防护系统面临的安全威胁也不断增长、增多。卫星通信系统及整体安全防护设计将与时俱进，在建设阶段能为抵御已知的各类威胁做好体系设计，在常管运行阶段，能随着攻击手段干扰威胁的不断发展，具备系统升级、局部重构、分系统冗余等软硬件重组重构能力，满足和应对不断发展中的网络空间攻击及威胁攻防能力提升和发展。

3.2 安全问题分类

基于攻击视角的卫星通信网络安全性问题分类：安全是一个贯穿整个技术体系、各子领域相互交织的复杂概念，涉及网络管理、物理、策略等多个维度。而卫星通信网络安全因其同时融合了传统航天工程安全与现代网络安全的双重属性。为聚焦讨论范围，本文不涉及传统航天安全保障内容（如火箭发射可靠性、轨道入轨精度、卫星平台热控与电源稳定性、安全管理、物理安全等），而是重点从网络安全的视角出发，分析卫星通信网络所面临的威胁。站在通信网络的视角来抵御外部恶意攻击，而非保障航天任务全流程的工程可靠性。

传统安全性分类视角的局限与拓展：传统网络安全领域通常将安全性目标简化为机密性（Confidentiality）、完整性（Integrity）和认证/可用性（Authentication / Availability），这三者组合简称为 CIA 三元组。此外，一些文献还将运行安全性（Operational Security）作为补充维度^{[41][42]}。其中，CIA 三元组主要适用于保障通信会话的安全，而运行安全性则更贴近网络基础设施本身的防护需求。

CIA 三元组目标在各类系统中具有高度的普适性，为更深入地探讨卫星通信网络的安全性问题，并结合其战略敏感性与空间特殊性，以下采用一种基于攻击实体的安全性分类方法^[43]，将卫星通信网络安全威胁划分为以下四类：

- (1) 对通信会话的攻击；
- (2) 对卫星通信网络本身的攻击；
- (3) 对卫星通信网络主机（边缘节点/终端）的攻击；

(4) 拒绝服务/分布式拒绝服务攻击（DoS/DDoS）。

需要指出的是，这种基于攻击实体的卫星通信网络安全分类方法可以理解为第一种网络安全分类模型的运行安全性的进一步拓展延伸，而且这四类攻击并非彼此孤立，往往相互交织、协同作用，共同构成对卫星通信网络的复合威胁。

3.2.1 对通信会话的攻击

通信会话安全的核心目标，是确保利益一致的通信双方在交互过程中满足 CIA 三元组要求：信息不被未授权方窃取（机密性）、不被篡改（完整性）且通信实体身份可被验证（认证性）。这一目标在各类通信系统中具有高度一致性，卫星通信因卫星链路开放性强、信号易被截获，对加密和抗干扰的要求更高；高延迟特性对密钥协商协议提出了挑战。

3.2.2 对卫星通信网络本身的攻击

卫星通信网络运行于空间环境，具有高动态拓扑、资源受限、物理不可接触等特性，使其网络基础设施尤为脆弱。针对网络本身的攻击，可进一步分为两类：对网络实体的物理/逻辑控制攻击，以及对网络通信行为的操控攻击。

3.2.2.1 对网络实体的直接攻击

在低轨（LEO）卫星星座中，卫星以高速绕地球运行，其覆盖范围遍及全球，难以通过物理隔离手段加以保护。攻击者若能非法获取卫星的控制权限，可能强行改变其轨道、姿态或关闭有效载荷，导致

局部甚至全局服务中断。极端情况下，单颗卫星的异常行为可能通过星间链路卫星间业务（Inter-satellite service，在人造地球卫星之间提供链路的无线电通信业务^[46]）引发级联故障，造成整个星座功能瘫痪。

3.2.2.2 对网络通信行为的攻击

更常见且隐蔽的攻击方式，是不干扰卫星物理状态，而仅操控其通信行为，从而破坏网络的逻辑连通性，其包括多种手段。

(1) 虚假路由通告攻击

若卫星通信网络采用域间路由机制（如基于自治系统（Autonomous System，AS）的架构），攻击者可控制某一非法网关节点，伪造路由通告，谎称其可达任意目标网络。其他节点若未验证路由来源，将把流量错误转发至攻击者控制的节点，导致数据被窃听、篡改或丢弃。

(2) 路由劫持与污染

攻击者通过发布“更优”路由（如更低跳数、更短延迟），诱使网络选择其控制的路径。在 LEO 星座中，攻击者可操控某颗卫星或地面站，虚假宣称其到关键网关的路径延迟更低，从而劫持军事或商业敏感流量。

(3) 女巫攻击（Sybil Attack）

由于部分卫星身份认证机制依赖简单 ID 或未加密信标，攻击者可伪造多个虚假卫星身份，加入路由协议。这将扭曲整个星座对网络拓扑的认知，导致路由决策严重偏离真实状态。

(4) 动态性管理攻击

LEO 卫星需频繁切换地面站与星间链路，依赖复杂的移动性管理协议维持连通性。若该机制被攻破，攻击者可制造虚假切换指令，导致用户终端无法正确接入网络，甚至引发大规模连接中断。

(5) 集中控制平面攻击

随着软件定义网络（SDN）理念引入卫星通信网络，控制平面与数据平面解耦成为趋势。控制功能常部署于中高轨（MEO/GEO）卫星，因其对地可见时间长、链路稳定。这也使其成为高价值攻击目标一旦被攻陷，攻击者可一次性瘫痪其管理下的所有转发卫星节点，造成区域性甚至全局性服务中断。

上述攻击均依赖攻击者对卫星路由机制的深入了解或预测。因此，在路由协议细节、拓扑结构等敏感信息应采取严格保密措施。

3.2.3 对网络边缘节点与终端的攻击

聚焦于网络的边缘设备，包括用户终端（如卫星电话、VSAT 小站）、地面网关、各类卫星收发设备等。攻击者可能通过以下方式实现目标：

- (1) 获取未授权访问权限（如远程控制、权限提升）；
- (2) 窃取、篡改或破坏本地数据；
- (3) 植入恶意软件（木马、后门、勒索软件）；
- (4) 向终端发起 DDoS 攻击或横向渗透；
- (5) 破坏终端正常功能，导致服务中断。

在传统地面网络中，单个终端被攻破通常影响有限，主要涉及用户隐私或局部业务中断，最大的利益损失往往是用户群体。但在卫星

通信网络中，边缘终端往往承载关键任务，由于卫星通信网络用户的多样性与特殊性，某些用户权益远比地面网络由于潜在的涉及国家安全与战略利益，其对于来自恶意攻击的防护机制需远高于普通地面设备标准，需要有对应的技术要求的标准及制度。

3.2.4 拒绝服务/分布式拒绝服务攻击（DoS/DDoS）

拒绝服务/分布式拒绝服务攻击旨在通过耗尽网络资源（如带宽、处理能力、连接数），使合法服务退化或完全中断。卫星通信网络在此类攻击面前尤为脆弱，原因包括：

- (1) 链路带宽有限：上行/下行链路极易被伪造请求饱和；
- (2) 全球可访问性：攻击者可从任意地点发起攻击；
- (3) 扁平化网络结构：缺乏多层防御纵深；
- (4) 路由确定性强：最优路径易被预测，便于精准打击瓶颈链路。

其潜在的攻击形式包括但不限于：1）向地面网关发起大规模DDoS，切断用户接入入口；2）利用LEO星座的动态切换机制，实施移动式DoS，持续干扰特定区域；3）控制全球分布的僵尸终端，协同注入流量至关键星间链路或热点区域链路，以最小成本造成最大范围的服务中断。

尤其值得警惕的是，攻击者可通过基础的流量工程分析，识别网络中的“关键瓶颈链路”（如两大高吞吐量地面站之间的最优卫星中继路径），集中攻击这些节点，实现“四两拨千斤”式的高效破坏，影响大范围网络的可用性。

3.2.5 总结

综上所述，卫星通信网络的安全威胁，根据攻击实体可系统性地划分为具体的四类：通信会话攻击、网络本体攻击、卫星通信网络主机（边缘节点/终端）攻击与拒绝服务攻击。这四类威胁相互关联、可能协同作用，共同挑战卫星通信网络的管理与控制、经济性以及社会需求等方面。

3.3 重大风险分析

3.3.1 卫星通信网络风险

卫星通信网络覆盖广域、网元架构复杂，面临的信息攻击、传输干扰、设备故障、环境威胁等，其攻击方法包括且不限于表 3-1 所述。

表 3-1 信息攻击威胁

类别	攻击方法
信息攻击及威胁	信息欺骗，篡改、伪造、重放信息
	信息特征分析（如流量监听、特征提取等）
	病毒、蠕虫、炸弹、木马植入、预置引擎等
	能量攻击、侧信道攻击
	干扰入侵攻击
传输攻击及威胁	信号干扰、抑制或使中断。利用电磁、红外、激光等干扰武器对卫星星地、星间通信系统进行干扰或压制、信息阻拦
	伪节点入侵，伪造，攻击者发动中间人攻击
	路由攻击、网络欺骗
	多卫星系统联合通信威胁
密码设备故障	自身设备出现故障

	密码不同步故障
	设备受物理攻击使失效
环境因素威胁	地面不可抗力因素等导致的威胁
	空间环境威胁，如太阳风暴等空间环境干扰、单粒子、辐射累积效应等，导致局部或全局异常或设备损坏
	通信网络故障、瘫痪
	时统攻击
拒绝服务 Dos/DDos攻击	平台及载荷服务受到威胁。如攻击者利用路由协议处理大量更新消息的资源消耗特性，可持续发送伪造的路由更新报文，加剧拓扑动荡时期本已存在的控制平面负担，耗尽卫星或网关路由器的CPU和带宽资源，导致合法路由更新被淹没，全网通信中断。
路由攻击	可以是单个节点或两个以上恶意节点联合行动。如虫洞攻击，如诱使网络系统误认为该节点是通信路径中最佳路由，从而在网络中搜集、截获、复制转发、篡改或伪造节点信息或网管信息。相关节点实施拒绝转发特定的消息并将其丢弃；或在数据流传输路径上，修改特定节点传送的数据包，并转发
泄流攻击	攻击者在充分掌握通信路由协议的基础上引入伪造的节点，将某些特殊区域或特征的数据诱使其改变原有路由而流经伪造节点，造成网络流量受攻击者操纵
黑洞攻击	攻击者试图吞噬所有收到数据包，像黑洞一样，所有流经该节点的数据包都不会被转发，截留所有流经的数据包。 攻击者可广播虚假更新，宣称某关键卫星节点或重要网络前缀不可达，导致合法数据包被丢弃。拓扑的快速变化使得此类恶意宣告更难被即时验证和清除。
恶意代码攻击	利用节点软件漏洞通过植入木马、病毒和垃圾信息

3.3.2 外联接口风险

深度检测失效：卫星链路的加密、分片、特殊封装可能绕过地面

DPI 设备（业务数据流识别与控制的网络设备）的有效检测，使得隐藏在“合法”卫星数据流中的恶意软件、命令和控制 C&C（Command and Control）指令、扫描探测流量得以蒙混过关。

供应链与第三方依赖风险：卫星运营商通常依赖第三方基础设施（如国际互联网交换点（IXP）、云服务商内容分发网络（CDN）节点、运营商骨干网）进行数据交换和内容分发。对这些外部资源的访问路径和安全状态，卫星运营商缺乏直接的控制力和可见性。第三方网络的漏洞、配置错误或被入侵，均可成为攻击者迂回渗透进入卫星互联网的跳板。卫星通信系统涉及多个软硬件设备供应商带来的供应链风险，可包括卫星、地面设备以及相关软件的生产、研发、采购、继承和维护等环节。

传统网络攻击：通过非可控外联接口，地面互联网攻击手段得以直接侵袭卫星通信网络。

恶意软件渗透：勒索软件、蠕虫、僵尸网络木马等通过被感染的终端用户设备（经卫星接入）或通过受污染的地面网络数据流，侵入卫星用户段甚至信关站内部网络。

高级持续性威胁（APT）：APT 组织可利用外联接口作为初始入口，利用卫星通信网络协议的未知漏洞或配置弱点，进行长期潜伏、侦察，最终目标直指窃取卫星控制权或敏感数据。

用户隐私数据保护不足：用户通信内容、位置信息、身份标识等隐私数据，在外联传输链路上（如信关站到互联网服务提供商）保护不足，将面临泄露风险。

网络拓扑及配置暴露：攻击者通过监控外联接口流量，可分析推断卫星通信网络的内部拓扑结构、节点 IP 地址、路由策略等关键信息，为后续精准攻击绘制蓝图。

3.3.3 卫星通信设备风险

常见的卫星地面站接入应用与安全：

- (1) **基于窄带或宽带卫星的接入设备：**实现卫星通信服务，满足卫星固定业务FSS、卫星移动业务MSS（如车载、船载、机载等），需解决窄带或宽带卫星通信过程中，节点的认证，通信链路加密、授权使用等。
- (2) **卫星通信终端：**具有卫星通信的智能手机、专业终端等。实现点对点、群组通信、视频采集回传等，需解决卫星通信终端认证、端端数据传输加密、群组指挥通信加密服务等。

卫星通信设备、终端可能面临的安全威胁如表 3-2 所示。

表 3-2 卫星通信设备面临的威胁

卫星终端安全威胁	攻击方法	产生缘由
设备或重大存储信息泄露	后门	技术不自主，芯片、操作系统和应用软件提供者故意设置
	木马、病毒	软件设计缺陷被利用，或未按安全体系设计
	终端被恶意使用者接触	用户界面缺乏使用控制
远程窃听、窃视	后门	技术不自主，芯片、操作系统和应用软件提供者故意设置

卫星终端安全威胁	攻击方法	产生缘由
	木马、病毒	软件设计缺陷被利用，或未按安全体系设计
无意或有意泄密	终端具有摄像头等外设，可以存储或实时传输相关信息	缺乏终端外设控制技术和后台管理支撑系统
话音、数据通信泄密	空口截获、干扰	通过无线接口传送的数据很容易受到截听或干扰的威胁、通话端到端加密保障措施不完善
	假基站	只有网络对用户的单向认证机制
特殊用户被定位	用户识别码等身份信息泄露	通信接入设计缺陷

3.3.4 新技术的安全挑战

新一代信息技术带来的风险与挑战加剧，包括量子计算、人工智能、网络攻防技术等不断演进、发展与应用。针对卫星通信系统的安全，需考虑相应的影响，对涉及的范围需考虑抗量子计算的相应威胁与技术措施。后量子算法（Post-Quantum Cryptography, PQC）的应用、密钥分发协议、在轨卫星的密码算法及服务可重构能力。

(1) 量子计算对经典密码带来威胁

2020年2月美国国家量子协调办公室发布《美国量子网络战略愿景》。2021年3月，英国量子通信中心先后宣布资助“即插即用量子安全系统项目”、“高性能集成单光子源项目”和“空间量子通信项目”。即插即用量子安全系统项目利用量子密钥分发（Quantum Key Distribution, QKD）和高速光学加扰技术开发高速光通信网络中的即插即用安全模块，实现量子安全和数据传输中的物理级安全。英国在

实施第二阶段国家量子技术计划中主动布局后量子密码平滑迁移。欧盟正在实施量子技术旗舰计划，并部署了量子通信基础设施先导工程 OPEN QKD 项目。中国密码行业标准化技术委员会（CSTC）陆续开展了量子密码领域的标准研制和课题研究，内容涵盖 QKD 系统检测、量子保密通信中继安全、QKD 技术规范等。

(2) 后量子密码技术迁移

在后量子密码技术迁移方面，中国密码学会在 2018 年起开展了全国密码算法设计竞赛；2025 年 2 月商用密码标准研究院发布关于开展新一代商用密码算法征集活动公告。美国国家标准与技术研究院（NIST）于 2024 年 8 月发布三项后量子密码算法标准 FIPS 203、FIPS 204、FIPS 205。同年 10 月，NIST 启动第二轮后量子算法征集活动。NIST 近年来发布的相关研究报告包括且不限于：

——NIST.IR.8528 Status Report on the First Round of the Additional Digital Signature Schemes for the NIST Post-Quantum Cryptography Standardization Process（后量子密码学标准化进程第一轮附加数字签名方案实施进展报告）；

——NIST.IR.8547 Ipd-Transition to Post-Quantum Cryptography Standards（向后量子密码标准的过渡）。

(3) 深入融合 AI 的安全防护

在 AI 迅猛发展的今天，对卫星通信网络的防护也应当与 AI 深度融合，从静态的防御策略转向动态的信任评估，主动进行防御。如对卫星拓扑时变风险利用 AI 实时分析星地协同网络流量，动态识别拓

扑突变引发的路由攻击；基于情境感知进行自动安全策略调优，如在卫星过境高危区域时提升防护等级；通过联邦学习在加密数据上训练威胁检测模型，打破数据孤岛；通过云化资源池与轻量化 AI，破解星上算力约束。

3.3.5 空间环境风险

空间环境中，由于太阳黑子、耀斑等空间现象活动频繁时，将释放大量的高能粒子引发宇宙空间中卫星上的电子元器件出现运行异常、单粒子翻转，辐照累积效应下导致的电子元器件失效或局部失能等风险。

星载部件应具备相应的环境适应能力，包括但不限于：

- (1) 抗辐射（Rad-Hard）、适应单粒子翻转（SEU）、单粒子门锁（SEL）、总剂量效应（TID）等严苛宇航环境测试，确保在轨长期可靠运行；
- (2) 具备一定物理安全防护，如具备防旁路攻击（SPA/DPA）、电磁泄露、故障注入等物理探测能力；
- (3) 逐步具备网络安全的基本防护，如异常流量检测/过滤、入侵行为模式匹配、弹性策略与自主维护等。

3.4 小结

卫星通信网络是通信的关键基础设施，其网络的安全性、健壮性及可靠性要求高，其自身固有特点与传统地面网络相比，具有航天器高动态、大延时、广分布、轨道规律性等特点，使得卫星通信网络易

受到攻击和干扰，如空间链路信息截获、信息伪造、干扰入侵等。

卫星通信网络将与地面网络，如移动通信网络、固定网络、互联网等形成互联，因此存在跨域、多网融合、境外接入及应用等面临的挑战及风险。

由于智能终端直连卫星的应用发展，对卫星通信网络接入的攻击面及卫星通信基础设施面临的挑战及安全威胁进一步加大。

因此开展有关卫星通信系统的网络安全标准化研究十分必要。

4 安全相关政策与标准分析

4.1 安全相关政策

4.1.1 国内安全相关政策

2020年4月，国家发展改革委将卫星互联网纳入新型基础设施建设范畴。

2024年1月，工业和信息化部等七部门《关于推动未来产业创新发展的实施意见》要求前瞻布局 6G、卫星互联网、手机直连卫星等关键技术，推进高通量卫星与低轨星座协同发展。

2025年4月，国家互联网信息办公室等七部门联合发布《终端设备直连卫星服务管理规定》（国信办发文〔2025〕1号）。规范手机直连卫星服务全流程管理，提出“终端设备直连卫星服务提供者应当依照相关法律法规的规定和国家标准的强制性要求，履行网络安全、数据安全和个人信息保护义务，落实网络安全等级保护、通信网络安全防护、数据分类分级保护和商用密码应用安全性评估等制度，采取

必要措施保障数据和个人信息安全。支持终端设备直连卫星技术研发和基础设施建设，规范终端设备直连卫星服务发展和应用。”

2025年7月21日，国家航天局发布《关于加强商业航天项目质量监督管理工作的通知》。

2025年8月25日，工业和信息化部发布《工业和信息化部关于优化业务准入促进卫星通信产业发展的指导意见》（工信部信管〔2025〕180号），该文件在“加强卫星通信监管（十四）筑牢网络和数据安全防线”中指出“指导督促企业依法履行国家安全主体责任，在相关系统的设计、建设、运行中同步规划、同步建设、同步运行安全技术措施，落实通信网络安全防护、数据分类分级保护、关键信息基础设施保护、网络安全等级保护以及个人信息保护等要求，建设信息安全技术措施，保障网络、数据和信息安全，加强用户实名制管理，做好防范治理电信网络诈骗相关技术保障措施。”

2025年11月25日，工业和信息化部发布《工业和信息化部关于组织开展卫星物联网业务商用试验的通知》（工信部信管函〔2025〕307号）。

2025年11月25日，国家航天局官发布《国家航天局推进商业航天高质量发展安全发展行动计划（2025—2027年）》，提出“到2027年，商业航天产业生态高效协同，科研生产安全有序，产业规模显著壮大，创新创造活力显著增强，资源能力实现统筹建设和高效利用，行业治理能力显著提升，基本实现商业航天高质量发展。”

4.1.2 国外安全相关政策

2018年6月，美国总统特朗普出席了国家航天委员会第三次公开会议，并签署了3号航天政策令《国家太空交通管理政策》（也称《太空政策3号令》）。美国在商业航天领域的探索起步较早，基本形成战略政策、管理执行双层结构的监管模式^[28]。

2022年4月，美国国会通过《卫星网络安全法》，该法案要求美国网络安全和基础设施安全局（CISA）面向美国卫星运营商制定网络安全建议，并开发公开在线资源，以确保企业能够访问特定的卫星网络安全资源和建议，以保护其卫星网络。同时，该法案还要求政府问责办公室对联邦政府如何支持商业卫星行业网络安全进行研究，这将确保更好地了解商业卫星中的网络漏洞如何影响关键基础设施^[27]。根据法案要求，CISA 将起草旨在协助商业卫星系统的开发、维护和运营的自愿型网络安全建议，包括风险监控、系统复原及防止未经授权访问等指南。评论称，商业卫星运营商按照 CISA 建议，建设和完善相关卫星网络，可有效实现美国政府对各企业商业卫星的统一监管及卫星网络安全防护。

2022年5月，美国网络安全和基础设施安全局（CISA）宣布成立“太空系统关键基础设施工作组”。

2024年4月，美国防部、天军联合发布《商业航天集成战略》^[19]。

2025年6月25日，欧盟委员会公布了欧盟《空间法案》提案^[28]。

4.2 标准分析

4.2.1 国际标准研究情况

4.2.1.1 ISO/TC20

国际标准化组织航空航天器技术委员会（ISO/TC20）下设空间数据与信息传输分技术委员会 ISO/TC20/SC13，先后发布了若干空间数据与信息传输标准，涉及术语，空间网络、链路，任务操作及交互等90多项标准。相关标准见附录B。

ISO 21324：2016 Space data and information transfer systems — Space data link security protocol（空间数据和信息传输系统-空间数据链路安全协议）中图 7-1 描述了空间数据与传输系统的分层结构与对应安全协议的基本结构。

4.2.1.2 CCSDS

国际空间数据系统咨询委员会 CCSDS（Consultative Committee for Space Data Systems）是一个国际性空间组织，先后发布160余项标准。CCSDS是 ISO TC20/SC13 空间数据和信息传输系统分技术委员会，主要负责开发和采纳适合于空间通信和数据处理系统的各种通信协议和数据处理规范。CCSDS 推出了一系列建议和技术报告，内容涉及分组遥测、遥控、射频、调制、时码格式、遥测信道编码、轨道运行、标准格式化数据单元、无线电外测和轨道数据等。中国国家航天局（CNSA）是其正式成员国单位。

根据我国航天科技发展规划，在航天测控通信领域逐渐采用 CCSDS标准。中国航天标准化研究所副总师周玉霞曾担任ISO TC20

SC13主席，为推动空间网络互联业务标准化做出了积极努力。 航天五院总体部何熊文研究员担任了航天器相关接口业务标准化工作组的副组长工作，他牵头提出的 **CCSDS星载软件参考架构** 已于2016年发布橙皮书(试验, Experimental) (CAST FLIGHT SOFTWARE AS A CCSDS ONBOARD REFERENCE ARCHITECTURE) 以推进国际空间数据通信协议及星地、星内、星间接口的标准化。

在网络层安全方面，CCSDS推荐 IP over CCSDS 技术为天地一体化网络的主要标准。针对物理层安全防护，提出了整包加密 (Bulk Encryption) 和 TRANSEC 的技术框架。

2010年5月，CCSDS发布了《空间任务密钥管理概念报告》绿皮书 (CCSDS绿皮书代表信息报告 (Informational Reports))，对天基安全管理进行了探讨和规划。提出“已经实现电子安全管理的情况下，正在实施综合网络环境中的安全管理基础设施建设，解决自动安全管理、快速灵活的自动分配问题，实现24小时内为全球范围的任何用户提供实时安全保障。”

CCSDS与IETF共同制定时延容忍网络 (Delay Tolerant Networks, DTN) 和束协议 (Bundle Protocol, BP) 的标准，解决空间的长时延等问题。CCSDS制定的系统架构及安全相关的部分标准或研究报告见附录B。

4.2.1.3 ITU

国际电信联盟 (ITU) 是主管信息与通信技术的联合国专门机构。ITU 包括3 个部门：无线电通信部门 (ITU-R)、电信标准化部门

(ITU-T) 以及电信发展部门 (ITU-D)，如图4-1所示。

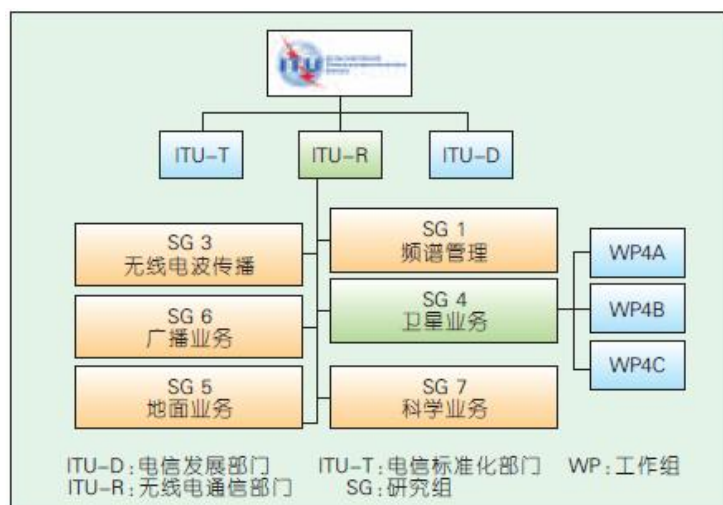


图 4-1 ITU 组织架构

ITU-R第4研究组负责制订卫星业务的技术建议书。该研究组包括3个工作组：4A工作组研究卫星固定业务（FSS）和卫星广播业务（BSS）的高效轨道或频谱利用；4B工作组研究卫星固定业务、卫星广播业务以及卫星移动业务（MSS）的系统、空中接口、性能和可用性目标，包括IP应用和卫星新闻采集；4C工作组研究卫星移动业务和卫星无线电测定业务（RDSS）的高效轨道或频谱利用。

ITU针对卫星与地面5G融合的问题，提出了星地5G融合的4种应用场景，包括中继到站、小区回传、动中通及混合多播场景，并提出支持这些场景必须考虑的关键因素，包括多播支持、智能路由支持、动态缓存管理及自适应流支持、延时、一致的服务质量、网络功能虚拟化（NFV）/软件定义网络（SDN）兼容、商业模式的灵活性等。

4.2.1.4 3GPP

3GPP（第三代合作伙伴计划）从R14着手开展星地融合的研究工

作，目前已正式发布Rel-19。在3GPP名为“面向‘非地面网络’中的5G新空口”研究项目中，定义了包括卫星通信网络在内的非地面网络（NTN: Non-terrestrial networks）的部署场景。

3GPP 研究的各阶段及内容包括且不限于：

- (1) R-15 讨论卫星议题包括 Integration of Satellite in 5G（整合卫星与 5G）、NR in non-terrestrial（非地面网路的新无线电）等，定义“5G 使用卫星接取之连续性服务”、“无所不在服务”和“扩展性服务”等三大类应用案例，讨论卫星终端特性的建立、配置与维护，以及在卫星通信网路与地面网路间的跨系统协定、漫游及通信系统切换问题，并在 2017 年底发布 TS22.822 技术报告；
- (2) R-16 展开非地面网路 5G 新空口架构，讨论包括 5G Service Satellite in 5G system Architecture, 以及持续从 RAN 架构及访问控制层、物理层等讨论 NR 应用在非地面网络；
- (3) R-17 自 2020 年至今进一步讨论 5G system supports satellite 及 IoT & NR over NTN, R-17 规划把卫星通信纳入 5G 网路，研究 5G NR 支援卫星通信相关标准化，定义包括卫星网路在内的非地面网路部署情境, 5G 的 NTN 应用场景包括 8 个增强型行动宽频（eMBB）和 2 个大规模机器通信（mMTC）情境，借助卫星广域覆盖能力，使运营商在地面网路不发达地区，还能提供 5G 商用服务，尤其是在紧急通信、海运通信、航空通信及铁路沿线通信等情境中发挥作用, R-17~ R-19 持续讨论

B5G 研究与标准制定；

(4) R-19 ~ R-21 将讨论 6G 可行性研究与标准制定,ITU-R 及 3GPP 也将进行技术标准整合。

4.2.1.5 NIST

美国国家标准与技术研究院 (NIST) 发布的卫星相关标准或研究报告包括且不限于：

NIST 发布了《卫星地面段用于卫星控制的网络安全框架》(NIST.IR.8401 Satellite Ground Segment Applying the Cybersecurity Framework to Satellite Command and Control)，重点为卫星总线和有效载荷的指挥和控制，将协助航天部门商业地面部分的运营商为其系统提供网络安全，并为利益相关者提供一种评估其网络安全态势的方法。该框架建立在网络防御的通用方法之上，包括五项主要功能：太空地基资产及其网络风险识别、保护技术与程序的资产开发、攻击检测、应急响应所需基础设施的建设以及复原力提升等。

2023 年 7 月，发布 NIST IR 8270 July 2023 interagency Report Introduction to Cybersecurity for Commercial Satellite Operations (NIST 跨机构报告 商业卫星运行网络安全导论)。在该报告 2.2.1 中，描述卫星空间段、地面段和用户段几个标准的作用。

2023 年 9 月，NIST 下设的国家网络安全卓越中心发布 NIST.IR.8441 September 2023 Cybersecurity Framework Profile for Hybrid Satellite Networks(HSN) (混合卫星网络 (HSN) 的网络安全框架轮廓) [26]。

NIST 发布的 NIST IR 8401 December 2022 Satellite Ground Segment Applying the Cybersecurity Framework to Satellite Command and Control (卫星地面段 网络安全框架在卫星命令和控制中的应用)。NIST IR 8401 中图 1 中描述了地面段组成,图 2 中描述了配置文件内外的组件及相互关系。

4.2.1.6 ETSI

欧洲电信标准化协会 (ETSI) (European Telecommunications Standards Institute)是由欧共体委员会于1988年批准建立的一个非营利性的电信标准化组织,总部设在法国。ETSI的标准化领域主要是电信业,并涉及与其他组织合作的信息及广播技术领域。ETSI是被欧洲标准化协会 (CEN) 和欧洲邮电主管部门会议 (CEPT) 认可的电信标准协会,其制定的推荐性标准常被欧共体作为欧洲法规的技术基础而采用并被要求执行。

ETSI下设13个技术委员会,其中与安全及卫星通信相关的技术委员会包括:

- (1) **TC SEC (SECurity)** 安全技术委员会: 负责提供关于安全方面的ETSI技术报告和标准,向其他技术委员会提供关于安全方面的建议和援助;
- (2) **TC SES (Satellites Earth Stations &System)** 卫星地面站及系统技术委员会: 负责所有与卫星通信相关的技术工作,包含各类卫星通信系统 (移动的和广播式的)、地面站及设备的无线频率接口和网络用户接口,卫星及地面系统的协议。

ETSI已发布卫星相关标准包括且不限于：

—— ETSI TR 101 984 V1.2.1 Satellite Earth Stations and Systems (SES) Broadband Satellite Multimedia (BSM) , Services and architectures (卫星地球站和系统 (SES) 宽带卫星多媒体 (BSM) , 服务和架构) 。该文件中图4.1、图5.1分别描述了接入网、内容分发网络及卫星核心网的系统拓扑示意图，以及卫星相关机构角色的关系。

—— ETSI TS 103 275 V1.1.1 (2015-05) Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Common air interface specification; Satellite Independent Service Access Point (SI-SAP) interface: Services (卫星地球站和系统 (SES) ; 宽带卫星多媒体 (BSM) ; 通用空中接口规范; 卫星独立业务接入点 (SI-SAP) 接口: 服务) 。该文件中描述了ETSI 宽带卫星多媒体 (BSM) 说明文档的结构，其中与安全相关的文档涉及通用安全架构 (**Security General Security Architecture**) 、安全方面 (**Security aspects**) 、多点传输安全体系结构 (**Multicast Security Architecture**) 。

—— ETSI TR 102 287 V1.1.1(2004-05)Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); IP Interworking over satellite; Security aspects (卫星地球站和系统 (SES) ; 宽带卫星多媒体 (BSM) ; 卫星IP互连; 安全方面) ，该文件中图2中描述了典型的卫星系统结构。BSM系统由空间段一个或多个卫星和地面段组成，地面段包括网络控制中心 (NCC) 及操作用户、互联网网关

(Gateway) 及用户, 以及独立的卫星地面站 (ST) 及与之连接的局域网用户等组成。

4.2.2 国内卫星通信领域标准化进展

在卫星通信领域, 国内主要标准化组织包括全国宇航技术及其应用标准化技术委员会 (SAC/TC425)、全国通信标准化技术委员会 (SAC/TC485)、全国网络安全标准化技术委员会 (SAC/TC260) 和中国通信标准化协会CCSA等。

4.2.2.1 SAC/TC425

SAC/TC425下设的空间数据与信息传输分技术委员会 (SC3) 具体负责空间数据与信息传输领域的国家标准制修订工作, 包括空间数据与信息传输基础标准、空间链路标准、空间网络标准、航天器接口标准、任务操作与信息管理标准、交互支持标准等。SAC/TC425/SC3直接对口国际标准化组织ISO/TC20/SC13。截止2025年7月, 已发布的国家标准包括30余项。与卫星领域安全有关的标准项目计划如: 2025年4月30日国家标准计划 20251139-T-469《空间数据与信息传输系统 网络安全总体技术要求》。

4.2.2.2 SAC/TC485、CCSA

全国通信标准化技术委员会 (SAC/TC485) 主要负责通信网络、系统和设备的性能要求、通信基本协议和相关测试方法等国家标准制定。中国通信标准化协会 (CCSA) 是国内从事信息通信技术领域标准化科研、技术开发、设计、产品制造、运营等企、事业单位及高等院校、社会团体自愿组成的行业性、全国性、非营利性社会组织。

CCSA承担SAC/TC485秘书处工作，是3GPP会员。

2024年11月，CCSA航天通信技术组/协同组网通信技术（CCSA/TC12/WG3）提交TC485推荐国标立项计划《卫星互联网网络安全技术指南》。

2025年，CCSA发布《信息通信行业技术标准体系建设指南(2025-2027)》，对卫星通信及相关标准化工作，该指南中指出“卫星通信是利用人造地球卫星作为中继站来转发或反射无线电信号，以此实现两个或多个地球站之间的通信。这种通信方式具有覆盖区域广、通信容量大、传输质量高不受地理条件限制等显著优点，特别适用于远距离、大范围的通信需求。卫星通信在广播电视、电话网络、数据传输等多个领域都发挥着重要作用，是实现全球通信和信息化建设的重要基础设施。随着卫星技术的不断发展和创新，卫星通信的性能和效率也在不断提升，未来将为人们提供更加优质、高效的通信服务。”该指南提出的卫星通信标准体系和空间信息标准体系。

4.2.2.3 SAC/TC260

SAC/TC260是在信息安全技术专业领域内，从事信息安全标准化工作的技术工作组织，负责组织开展国内信息安全有关的标准化技术工作。2025年8月，发布《关于28项网络安全国家标准项目立项的通知》（网安字〔2025〕15号）中，下达一项国家标准制定计划，名称为《网络安全技术 卫星互联网网络安全框架》。

4.2.2.4 IMT-2020/IMT-2030

我国 IMT-2020（5G）推进组于2023年4月成立了NTN工作组，

主导30余项 5G卫星通信标准(5G NTN)的标准立项、制定或研究^[44]。

ITU-R于2023年发布6G愿景总目标及框架，相关研究建议如：

在 Recommendation ITU-R M.2160-0 (11/2023) M Series: Mobile, radiodetermination, amateur and related satellite services Framework and overall objectives of the future development of IMT for 2030 and beyond", June 2023。(ITU-R M.2160-0号建议书(2023年11月)M系列：移动、无线电测定、业余及相关卫星服务，2030年及以后未来移动通信技术发展的框架和总体目标)中，分别描述了 IMT-2030的使用场景和总体方面，和 IMT-2030增强的能力。

2024年2月发布报告 NGMN Alliance，“ITU-R framework for IMT-2030: Review and Future Direction”，Feb. 2024。(NGMN联盟，ITU-R IMT-2030框架：回顾与未来方向)，下一代移动网络联盟 (NGMN (Next Generation Mobile Networks) Alliance) 组织成立于2006年，由中国移动、英国Vodafone、Orange、NTT DoCoMo、T-Mobile、KPN 和 Sprint 等七大运营商联合发起，旨在推动下一代移动网络技术的发展。

4.3 小结

ISO/TC20/SC8 主要制定航空航天术语的国际标准。
ISO/TC20/SC14 主要制定空间系统和操作相关的国际标准。
ISO/TC20/SC13 是制定空间数据与信息传输国际标准的主要标准化组织，CCSDS 主要制定空间数据系统的国际标准，其制定的标准建议书可在ISO组织通过快速程序直接转化成ISO国际标准。其标准化

的目的是形成行星际的空间互联网，与地面互联网相融合，使空间资源可共享，并能互操作。相关的国际标准已经广泛应用，如将IP协议应用在CCSDS网络中。CCSDS与IETF共同制定DTN和BP协议有关的标准，解决空间传输长时延、抖动等问题。国际电信联盟（ITU）是主管信息与通信技术的联合国专门机构。3GPP组织主要制定国际移动通信网络相关的标准，在5G\6G移动通信网络标准体系中逐步开展星地融合、NTN相关标准体系的规划与演进，为基于空间资源、卫星平台的移动通信标准体系演进与应用起到了关键作用，其陆续发布Rel-19相关标准及研究成果，并陆续发布了Rel-19和Rel-20相关标准时间规划及进展。

国内相关的标准化组织主要有全国航天技术及其应用标准化技术委员会（SAC/TC425）、全国通信标准化技术委员会（SAC/TC485）、全国网络安全标准化技术委员会（SAC/TC260）、中国通信标准化协会CCSA等。相关标准列表见附录B。



5 卫星通信网络安全标准框架和需求分析

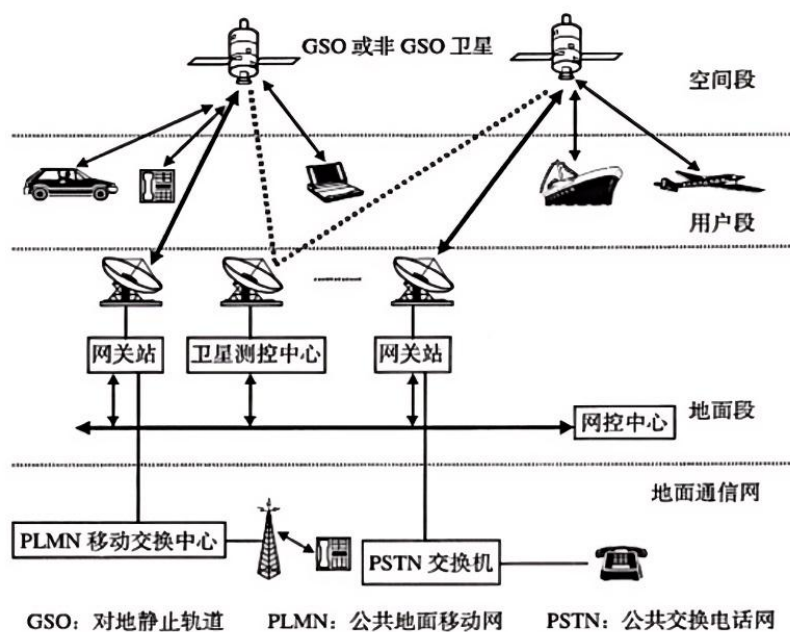
卫星通信通过天基组网，在短时间内实现全球范围的用户接入，为灾害救援、联合作战、远洋编队等提供广域通信支持，实现跨地域、跨领域的联合行动。

由GEO通信卫星、中继卫星，中低轨的卫星星座等通过卫星通信网络互联技术演进，逐渐在天基形成星际交换网络，并与地基网络结合，实现了异构星座组网、链路互备、星地、星间链路与地面有线网络、无线网络等互联互通的能力，可为海、陆、空、天各类用户提供全球大范围、全时空域（或大时空域）范围的天地互联通信网络。卫星通信系统可以为广域信息感知、通信和指控支持、信息中继、卫星广播和太空对抗等方面起到非常关键的作用，为广域互联、应急通信、网络补盲、资源勘测、国防安全等起到十分重要的作用。

针对卫星通信网络通信潜在威胁和风险，有必要规划并建设安全可靠、自主防御、抗毁顽存的卫星通信网络基础设施与服务。本章主要开展卫星通信网络安全的标准框架和需求分析。

5.1 卫星通信系统组成与接口

卫星通信系统组成的典型实例见图5-1，不同系统可以有不同的结构关系和组成。



(图注: 图片来源中国知网, 东北证券)

图 5-1 卫星通信系统组成的典型实例

图5-1中体现了与地面PSTN电话网互联的应用示意。如天通移动通信卫星终端已具备与4G/5G移动通信终端, 固定通信终端等在通话、短信等业务上的互联网互通。

卫星通信网络与地面网络互联的主要接口实例见图5-2, 不同系统可以有不同的结构和接口。

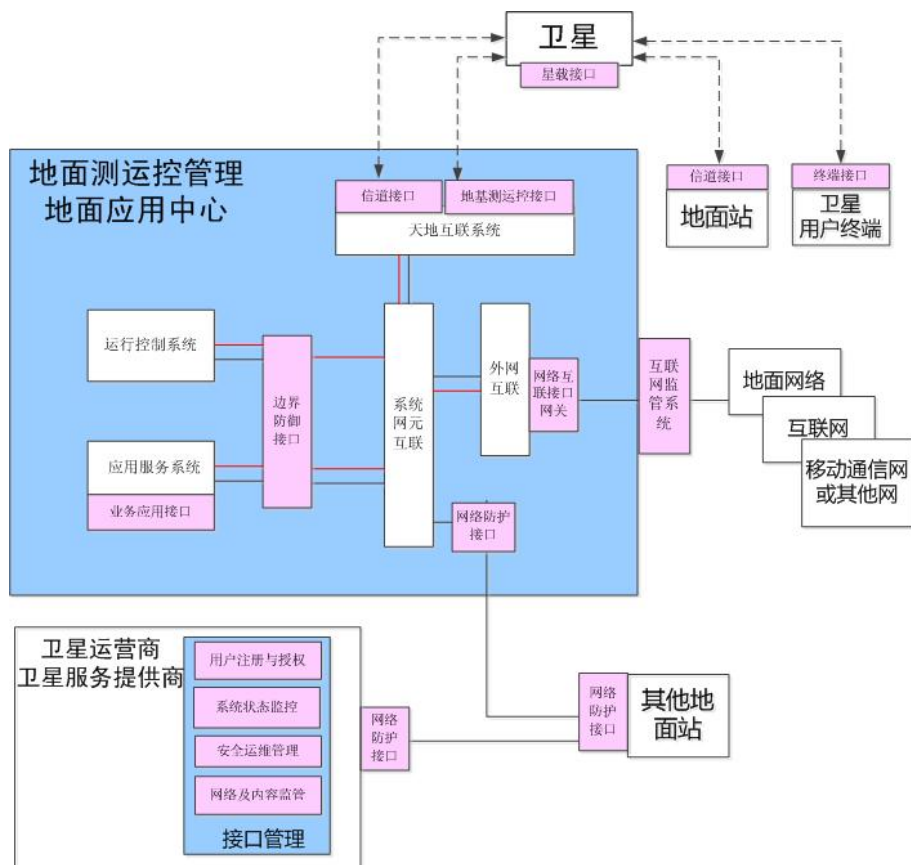


图 5-2 卫星通信网络与地面网络互联接口实例

图5-2中体现了卫星通信系统的空间段、地面段、用户段等的相关接口，这些接口包括且不限于：

- (1) 空间段：空间段星载接口包括且不限于遥控(TC)、遥测(TM)、数传、中继、星间通信、对地通信载荷、通信转发器等。
- (2) 地面段：地面段接口包括且不限于：

——地面站天地信道接口：如上行（前向链路）遥控、下行（反向链路）遥测、数传等；

——地基测运控接口：如地面测控系统接口、地面运控系统接口；

——地基网络防护接口：如网络边界防御接口、网络互联接口（如与地面有线网络、电话网络、移动通信网等互联）。

(3) 用户段：用户段接口主要包括卫星接入设备、卫星终端接口：

如终端直连卫星、终端通过信关站连接卫星。用户终端包括如手持、车载、船载、机载、舰载等。

综合上述接口的可能性，从卫星通信的空间段、地面段及用户段不同的接口配置组合下，将存在对应接口（参考点）下的安全机制及应用策略。并受到相应卫星通信所服务的系统及对象的安全要求、安全等级及基础条件等带来的差异，最终形成不同安全机制及配置的组合，并具备不断完善与修正、扩展的能力，从而应对卫星通信系统长期安全性的要求。

5.2 标准框架分析

本研究主要面向FSS和MSS的共性安全标准范畴，基于前述卫星通信网络标准化现状，安全风险及重大问题分析，借鉴国际国内卫星通信标准架构体系的研究方法，这些方法及标准架构包括且不限于：

- (1) 基于CCSDS空间数据与信息传输系统架构，简称**A模型**。该模型方法符合CCSDS、ISO/IEC TC20 /SC13标准体系，并在我国航天领域有关空间数据与信息传输的标准化中发挥了重要作用；
- (2) 基于我国网络安全技术体系的安全标准，简称**B模型**。此模型方法参考我国网络安全等级保护、密码应用基本要求、关键基础设施安全保护，以及网络安全相关标准架构及要求；
- (3) 基于NIST安全框架轮廓的安全标准，简称**C模型**。此模型方法采用安全架构保护轮廓的分析方法，呈现出具有安全对照表

(Checklist) 特点的多维度分析方法及要求，并在我国针对信息系统保护轮廓的标准化方法中应用；

(4) 基于3GPP 5G/6G NTN相关架构及标准要求，简称**D模型**。此模型方法主要参考3GPP NTN 安全相关标准、IMT2030等标准研究中安全接入、NTN架构及应用场景、安全业务、协议算法等要求。

参考标准体系及其代表性的安全标准说明见表5-1。

表 5 - 1 参考标准体系说明

标准范畴	参考标准	主要特征
A：ISO 空间数据与信息传输系统架构	ISO 20214:2015 空间数据与信息传输系统 空间数据系统的安全架构 Space data and information transfer systems — Security architecture for space data systems	以 CCSDS 分层的空间数据通信协议体系架构为主要特征
	ISO 21324: 2016 空间数据与信息传输系统 空间链路安全协议 Space data and information transfer systems — Space data link security protocol	
	GB/T 42037—2022空间数据与信息传输系统 参考体系架构	
B：我国信息安全技术体系	GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求	以网络安全等级保护、密码应用安全性评估、关键基础设施安全保护等安全架构及要求为主要特征
	GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求	
	GB/T 39204—2022 信息安全技术 关键信息基础设施安全保护要求	
	GB/T 20984—2022 信息安全技术 信息安全风险评估方法	
	GB/T 32914—2023 信息安全技术 网络安全服务能力要求	
	GB/T 29234—2012 基于公用电信网的宽带客户网络安全技术要求	
C：NIST 安全框架轮廓	NIST IR 8441 September 2023 NIST跨机构报告 混合卫星网络（HSN）网络安全框架轮廓 Cybersecurity Framework Profile for	以安全架构保护轮廓的

	Hybrid Satellite Networks (HSN)	分析方法，呈现出检查表结构的多维度分析及要求方法
	NIST IR 8401 December 2022 NIST跨机构报告 卫星地面段 网络安全框架在卫星命令和控制中的应用 Satellite Ground Segment Applying the Cybersecurity Framework to Satellite Command and Control	
	NIST IR 8270 July 2023 NIST跨机构报告 商业卫星运行网络安全导论 NIST interagency Report Introduction to Cybersecurity for Commercial Satellite Operations	
D : 3GPP 5G/6G NTN 安全	3GPP Rel-19 SP-241780 Security Aspects of 5G Satellite Access Phase 3 (5G卫星接入的安全目标)	以 5G/6G 中 NTN 的体系架构、应用场景、加密清单、安全业务流程、抗量子算法迁移等为主要研究特征。
	3GPP Rel-19 TR 33.700-29 V19.1.0 (2025-07) Study on security aspects of 5G satellite access in the 5G architecture phase 3 (Release 19) (5G架构阶段3中5G卫星接入安全研究)	
	3GPP Rel-20 SP-250654 3GPP New Study on Transitioning to Post Quantum Cryptography in 3GPP (向后量子密码学过渡的新研究)	
	3GPP Rel-19 SP-241771 New Study on 3GPP Cryptographic Inventory (关于3GPP加密清单的新研究)	
	3GPP Rel-20 SP-250653 New WID (Work Item Description) on mission critical security enhancements for release 20 (发布版本20中新工作项：关键任务安全增强措施)	
	3GPP Rel-20 SP-250876 New WID on Security related Events Handling (发布版本20中新工作项：安全事件处理)	
	3GPP Rel-20 SP-250877 New WID on Security Assurance Specification for 5G-Advanced (发布版本20中新工作项：5G-Advanced安全保证规范)	
	IMT 2030 ITU-R发布的2030年(6G)网络要求 Recommendation ITU-R M.2160-0 (11/2023) M Series: Mobile, radiodetermination, amateur and related satellite services Framework and overall objectives of the future development of IMT for 2030 and beyond", June 2023。(ITU-R M.2160-0号建议书(2023年11月)M系列：移动、无线电测定、业余及相关卫星服务，2030年及以后未来移动通信技术发展的框架和总体目标)	

5.3 卫星通信网络安全架构实例

以国际、国内已经发布的卫星通信相关的架构标准为研究参考，包括且不限于：

- (1) ISO 20214-2015 空间数据和信息传输系统 - 空间数据系统的安全架构；
- (2) GB/T 42037-2022 空间数据与信息传输系统 参考体系架构；
- (3) NIST CSF2.0 网络空间安全框架；
- (4) NIST IR 8441 Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN)（混合卫星网络（HSN）网络安全框架轮廓）；
- (5) 3GPP NTN 架构及安全标准。

5.3.1 ISO 20214-2015

ISO 20214-2015《空间数据和信息传输系统 - 空间数据系统的安全架构》中3.6.1提出，每个航天任务应按以下顺序编制安全文件，包括系统安全要求、安全互联要求、任务安全风险评估、任务安全架构、安全操作规程。

5.3.2 GB/T 42037-2022

GB/T 42037-2022《空间数据与信息传输系统 参考体系架构》中图11描述了复杂空间数据系统的连接视图，见图5-3所示。

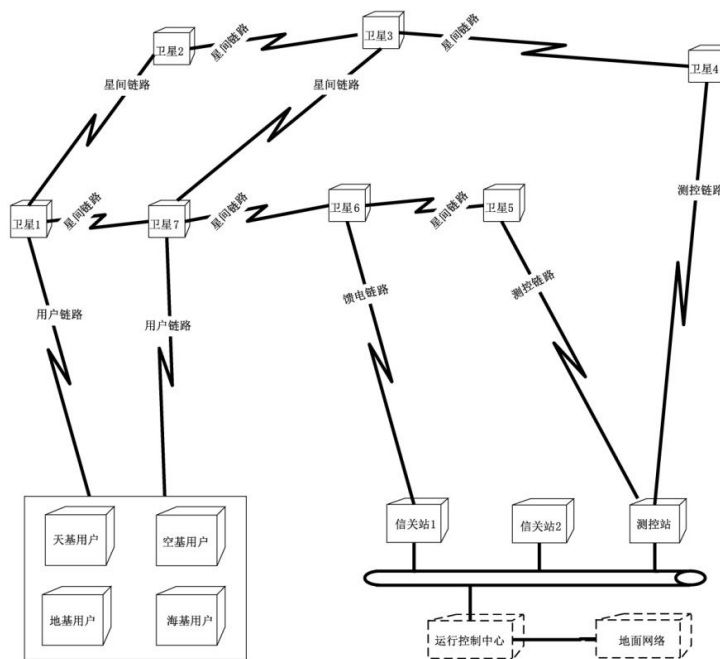
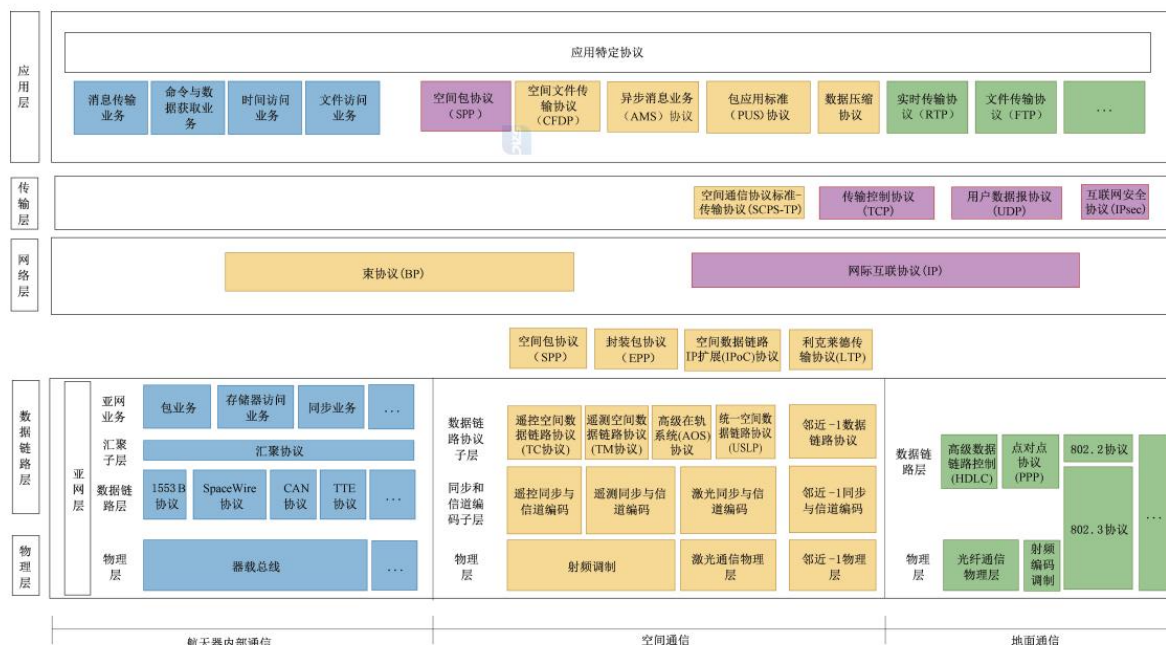


图 5-3 GB/T 42037-2022 中描述的复杂空间数据系统连接视图示例

在GB/T 42037-2022《空间数据与信息传输系统 参考体系架构》中7.4.3描述了空间通信协议体系，见图5-4。



说明：
 ■ 地面、空间和航天器内三个部分通用；
 ■ 地面特有；
 ■ 空间链路使用，其中 BP 协议和 LTP 协议为 DTN 体系特有；
 ■ 航天器内通信协议。

图 5-4 GB/T 42037-2022 中提出的空间通信协议体系

GB/T 42037-2022中描述了空间数据系统典型协议，并考虑空间数据系统中物理实体之间的多层安全协议和安全应用。可根据任务的安全级别在一个或多个层级实施通信安全。另外从信息视角看，应考虑星地上行操作或航天器自主操作的安全性，指令的认证，上下行数据及航天器之间数据通信的保密性等。

5.3.3 NIST CSF2.0 安全框架

NIST关于网络空间安全框架采用CSF(Cybersecurity Framework, CSF)架构描述，该架构提供一个组织对网络安全核心能力的框架轮廓^[32]。CSF2.0中图3网络安全框架轮廓，该方法通过任务目标、相关方期望、威胁环境、需求与主导实践等角度出发，提出包括识别、检测、保护、响应与恢复等维度的NIST网络安全框架，并给出当前的配置轮廓及目标的配置轮廓建议。NIST CSF2.0 的方法呈现出具有检查表Checklist特点的多维度分析方法及要求。

NIST IR 8270 July 2023 interagency Report Introduction to Cybersecurity for Commercial Satellite Operations (NIST跨机构报告 商业卫星运行网络安全导论) 中表2中描述了空间系统中的主要通信链路 (Major communication links used in space systems)。航天器内部网络安全特指卫星飞行器自身的网络安全能力，包括抵御网络威胁、检测攻击行为、应对网络攻击以及必要时恢复系统等核心功能。这些安全功能应在系统开发生命周期的早期阶段进行设计并集成。通常情况下，小型商业卫星的所有者和运营商主要负责内部网络安全，而其余架构部分则由外部系统或供应商解决。

NIST IR 8441 September 2023 Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN) (混合卫星网络 (HSN) 网络安全框架轮廓) 中图1描述了一个简单的混合卫星网络架构。HSN架构可能较为复杂, 涉及多方利益相关方。物理与虚拟架构中可能包含多个独立运营的卫星、无人平台、地面设施及支持多个独立HSN的交叉链路。

5.3.4 3GPP NTN 架构及安全标准

3GPP NTN 研究及标准化过程中面临的挑战主要包括:

- (1) 卫星通信的高动态性和长传播延迟与地面 5G 网络的低延迟、高稳定性要求之间存在矛盾, 需要进一步优化通信协议和算法来解决;
- (2) 卫星与地面设备之间的互操作性和兼容性也需要不断改进;
- (3) 卫星的频率使用、轨道资源分配等问题需要国际间的协调和合作;
- (4) 卫星通信的安全和隐私问题需要制定相应的监管措施。

5.3.4.1 标准化进展情况

第三代合作伙伴计划 (3GPP) 在非地面网络 (NTN) 有关的架构研究、安全研究阶段报告, 以及在Release20 新开展的安全工作项进行了涉及非地面网络有关卫星通信安全标准现状及演进研究。

3GPP在 Release-17中规定了支持固定无线、手持设备 (支持新空口New Radio (NR)、窄带物联网 (NB-IoT) 和增强型机器类型通信 (eMTC) [37]) 的 NTN。

3GPP小组 / 服务与系统方面 (SA) / SA WG3负责安全和隐私 (3GPP Groups /Service & System Aspects (SA) /SA WG3 -Security and Privacy)。与卫星通信安全有关的标准化研究包括且不限于:

(1) 3GPP Rel-19中的管理和编排 (Management and Orchestration)

中指出, NTN管理(NTNM)研究NTN场景中管理再生卫星(含星上处理)、存储转发(S&F)卫星以及端到端网络(包括RAN域和CN域)的管理要求和潜在解决方案^[38];

(2) 3GPP Rel-19 SP-241780 5G卫星接入的安全目标 (Security Aspects of 5G Satellite Access Phase 3)

中指出重点考虑安全与隐私方面2个关键问题: 一是EPS系统中存储转发卫星操作的安全防护(支持分片MME架构与完整EPC架构); 二是EPS系统中存储转发卫星操作的隐私保护;

(3) 3GPP TR 33.700-29 V19.1.0 (2025-07) Study on security aspects of 5G satellite access in the 5G architecture phase 3 (Release 19)

(5G架构阶段3中5G卫星接入安全研究)中, 研究内容包括一是识别并研究5GS/EPS再生载荷通用架构中的安全与隐私关键问题。二是识别并研究存储转发(S&F)卫星操作在非实时通信(NR NTN, 5GS)和物联网通信(EPS)中的安全与隐私关键问题。三是识别并研究5GS(5G卫星)用户终端-卫星-用户终端通信增强技术的安全与隐私关键问题。四是分析5G卫星接入环境下监管服务的影响, 特别是评估再生式通信、存储转发(S&F)以及“用户终端-卫星-用户终端”通信增强架

构对合法监听的潜在影响；

(4) 3GPP Rel-20 SP-250654 3GPP 向后量子密码学过渡的新研究

(New Study on Transitioning to Post Quantum Cryptography in 3GPP)。该文件描述了SA3已经开始通过识别和分类3GPP 5G规范中使用的所有加密技术来准备PQC过渡，并在TR 33.938“研究3GPP加密清单”中记录。该研究基于现有的加密技术清单展开，并探讨为有效准备和更新3GPP加密配置文件所需采取的行动与协调措施。还将研究聚焦于理解新型加密算法对3GPP规范提出的复杂性挑战。通过这些工作，目的是确保3GPP安全协议能及时且顺利地向PQC过渡，为后续发展提供支持；

(5) 3GPP Rel-19 SP-241771 New Study on 3GPP Cryptographic Inventory (关于3GPP加密清单的新研究)。

3GPP Rel-19 SP-241771研究目标是列出3GPP规范中用于5G独立模式系统的加密安全协议，包括协议采用的加密类型(对称/非对称)，提供相关协议规范的引用链接，包含对应的3GPP加密配置文件链接，并注明使用类型(如完整性保护、保密性或认证)。在背景中指出ETSI量子安全委员会(QSC)工作组已制定了一份关于量子安全加密迁移策略及建议的文件(ETSI TR 103 619 V1.1.1 (2020-07), Migration strategies and recommendations to Quantum Safe schemes)。作为迁移策略的重要环节，需要建立协议清单以制定准备方案、抗量子算法(PQC)迁移计划以及实际执行方案。ETSI QSC正在征集补充信息，

例如“加密算法和/或协议实现的详细清单”。该清单可能包含“算法公开性指导、有效密钥长度、混合部署潜力及加密敏捷性潜力”等内容。根据ETSI QSC 和 GSMA的描述，3GPP SA3的目标是生成涵盖3GPP规范（在3GPP定义的函数和接口中）所要求/使用的全部加密算法的概览，包括它们的量子安全状态以及5G系统中适用的协议。通过列出相应的抗量子计算（PQ）算法及其引用的规范文档，提出了向抗量子计算时代迁移的潜在路径。该清单的制定部分依赖于IETF在3GPP协议规范中引入PQC算法的工作。

其他在 3GPP Release20 新开展的安全工作项还包括且不限于：

- (1) 3GPP Rel-20 SP-250653 发布版本20中新的工作项描述：关键任务安全增强措施（New WID（Work Item Description） on mission critical security enhancements for release 20）；
- (2) 3GPP Rel-20 SP-250876 新工作项描述：安全事件处理（New WID on Security related Events Handling）；
- (3) 3GPP Rel-20 SP-250877 新工作项描述：5G-Advanced安全保证规范（New WID on Security Assurance Specification for 5G-Advanced）。

5.3.4.2 网络架构

3GPP TR 38.811规定的卫星通信网络架构可包括NTN终端、链路、地面系统等，典型的组织如下：

- (1) 3GPP 用户终端（UE）和非3GPP UE（卫星终端）；
- (2) 用户链路(Service Link): UE和卫星之间的链路；

- (3) 空间平台(Space Platform): 搭载弯管或者具备星上处理能力的卫星;
- (4) 星间链路(ISL: Inter-Satellite Links): 具备星上处理能力卫星间的链路;
- (5) 信关站(Gateway): 连接卫星和地面核心网的网元;
- (6) 馈电链路。

3GPP 描述的几种NTN网络架构如下:

- (1) 透明转发卫星下一代无线接入网 (Next Generation-Radio Access Network, NG-RAN) 架构、用户平面协议栈和控制平面协议栈;
- (2) 带gNB (the next generation Node B, 简称gNB) 处理载荷再生卫星的NG-RAN架构、用户平面协议栈和控制平面协议栈;
- (3) 带gNB-DU (gNB Distributed Unit, 即gNB分布式单元) 处理载荷再生卫星的NG-RAN架构;
- (4) 基于再生NTN的NG-RAN (gNB-DU) 与蜂窝NG-RAN的多连接技术。

3GPP TR 38.821 V16.2.0 (2023-03) Solutions for NR to support non-terrestrial networks (NTN) (支持非地面网络 (NTN) 的NR解决方案) 中, 描述了非地面网络为用户设备提供接入服务的典型场景。包括透明转发载荷和再生有效载荷的NTN典型场景。

在 3GPP TS 22.261中6.2.3 Service连续性要求中, 对于具有卫星接入的5G系统, 5G系统应支持由同一运营商或由具有协议的两个不

同运营商拥有的5G地面接入网络和5G卫星接入网络之间的服务连续性。3GPP TS 22.261中描述的5G TN和5G NTN之间的服务连续性。

5.4 网络安全标准化需求分析

5.4.1 顶层安全架构及保护要求的标准需求

参考国际、国内有关卫星通信系统相关的标准化进展可见，对空间系统、卫星通信相关的顶层安全架构、安全需求、安全威胁、安全保护轮廓的标准制定或研究是本领域标准化的共性基础与研究重点。并已产生丰富的标准化文件。当前我国也已启动开展相关的顶层安全架构、总体安全要求等标准计划制定工作。

5.4.2 网络与传输安全标准需求

在卫星通信领域，通信网络与传输安全是保障系统可靠运行的核心需求，聚焦构建多层次防护体系。针对卫星通信网络应用发展趋势、自主可控航天安全的持续演进。网络安全技术应用需与卫星通信技术的发展、自身的发展紧密联系。在多中心、超长期、多层次、动态组网、自主运行等方面发挥安全防护作用。如图5-5所示。



图 5-5 卫星通信网络与传输安全需求发展示意图

如在物理层，可通过智能波束成形技术、信号指纹认证等抗欺骗策略、抗干扰编码等手段提升信号在开放环境中的鲁棒性；在链路层

通过鉴权、加密、认证，以及相应的密钥更新等技术策略；在网络层通过适应空间通信系统特点的 IPsec over CCSDS 的新的协议机制，或通过BPsec协议的设计优化，实现超远距离，无连接、超长延时等深空场景下的安全可靠通信；在系统层通过自主可控的平台技术、智能运行与监测防护技术、安全可重构技术、星座群组安全协同、安全路由协议等实现系统级协同安全目标的达成。

5.4.3 算法与加密协议安全标准指导性技术文件需求

实现网络安全、信息安全和数据安全的核心在于密码安全，已有的算法标准提供了加密、签名、杂凑、密钥协商等基础能力，能够满足卫星通信网络安全体系中对于密码算法的最基础要求。在新技术带来的安全挑战方面，如抗量子算法迁移、适应高带宽的新一代密码算法的引入、适应空间数据与传输系统在传输延时、通信可达性、空间数据协议体系、密钥分发及协商、空间计算与通信环境基础等方面与传统地面系统的差异及面对的特定的安全风险，需对相关的算法、加密协议进行适应性优化及改进。从而产生了对算法及加密协议安全标准指导性技术文件的需求。

5.4.4 对网络边缘节点与终端等设备安全防护标准化需求

随着低轨卫星星座的规模化部署与应用场景拓展，地面段作为卫星控制中枢和数据交换枢纽，卫星通信应用的主体，与空间系统连接的地面设备及系统、网络边缘节点、卫星通信终端等的安全风险及安全防护技术要求的标准化十分重要。

星载设备受限于空间环境的严苛条件和宇航用组件的使用，其安全需求主要聚焦于器件及系统的自主可控、内在的安全运行与计算环境、安全逻辑与数据的保护与使用、通信接口的安全，以及自身的可靠性、可用性。

当前研究还不断发展空间态势感知、智能化漏洞挖掘、器件全生命周期供应链保证、高弹性网络安全等。对网络边缘节点与终端等设备的安全技术要求的标准化将有利于相关设备安全技术应用的规范化设计；有利于安全互联接口的标准化与互通性。

5.4.5 对网络安全防护效能评估的标准化需求

对上述网络与传输安全标准、算法与协议的技术性指导文件、设备与终端安全防护标准化的工作，需要有相关的检测与安全评估标准与之对应，形成有效的闭环，满足用户及监管部门对卫星通信网络安全建设与实施工作的符合性的确认，以对过程或可交付成果满足既定特征或目标要求的接近度予以评估及保证。

5.5 小结

卫星通信系统的业务呈现多样性，不同运行轨道、不同卫星通信网络用途、不同能力的卫星（星座）以及相应的地面测控系统、运控系统、载荷管理系统、运营保障设施等，通过多通道多频段星地、星间通信链路构成天地、空间通信及传输系统。卫星通信网络可在广域信息感知、通信和指控支持、信息中继和太空对抗等方面起到非常关键的作用，卫星通信载荷应用可实现通信网络互联、基站回传、应急

通信等。卫星通信终端可与其他通信终端进行话音、短消息、窄带或宽带FSS或MSS等卫星通信业务。

本章从网络安全架构标准化进展、安全技术标准化需求进行了卫星通信网络安全标准框架与需求分析。卫星通信业务融合的网络安全包括且不限于网元标识与认证、安全通信、用户与群组管理、系统协同与容错等。需实现通信信息的安全，确保信息传输的保密性、完整性；指令抗重放；防信息窃取、篡改或伪造。实现通信实体的鉴别，防止身份假冒及信息伪造。通过合理的密钥分发与管理，提升密钥质量及密钥分发的安全性。满足卫星通信系统长期的安全可靠运行、互联互通与安全监管。相关系统应符合国家在密码及安全政策等相关方面的技术与管理要求开展工作。

6 卫星通信网络安全标准化工作建议

6.1 总体思路

在符合法律法规要求方面，应深入落实《中华人民共和国网络安全法》、《中华人民共和国密码法》、《中华人民共和国数据安全法》、《关键信息基础设施安全保护条例》、《中华人民共和国个人信息保护法》等法律法规和政策文件要求，建立健全卫星通信网络安全标准体系，加快弥补关键基础标准短板，强化重点急需标准供给，有效保障新兴通信基础设施网络安全的标准化制定与实施。

在网络安全标准化方面，在卫星通信总体安全架构及要求的基础上，研究必要、急需网络安全标准的范围，包括卫星通信网络的空间

段、地面段及用户段通信互联的网络和通信安全、与地面网络互联安全、卫星用户应用安全，提出满足与质量保证（QoS）相匹配的安全通信网络、安全区域边界、安全的数据与应用，以及互联安全等。

在管理与保障方面，符合相应安全等级下国家对密码应用及等级保护的安全管理等方面的要求。有利于市场监管和可持续发展，并顺应信息技术发展、国计民生发展的内需。

6.2 标准体系设计说明

遵循GB/T 13016-2018 《标准体系表编制原则和要求》，综合上述卫星通信不同标准体系下的系统结构、网络安全架构、安全要求分解维度等，本标准体系的结构划分采用以下考虑：

- (1) 在结构上，采用国际、国内标准常见的卫星通信系统结构描述习惯，分空间段、地面管控段、用户应用段等；
- (2) 在内容上，对卫星通信网络安全的内容需涵盖星-间、星-地、地-星、地-星-地、地-星-星-地等通信互联方式下的数据与传输安全、地面网络互联安全、卫星用户应用安全等；在航空器，无人机等卫通链路方面参考“地”；
- (3) 在方法上，参考我国网络安全等级保护、密码应用基本要求、关键基础设施保护要求、个人信息保护等相关要求；
- (4) 在先进性及标准体系协调上，兼顾ISO、ITU、3GPP、NIST、ETSI等相关标准化推进及内容的协调，在考虑兼容的同时，条件成熟时可推进我国卫星通信网络安全标准研究的国际化。

6.3 标准体系建议

通过前述研究，卫星通信网络安全标准体系按照基础共性、安全协议、产品与应用、测试评估 4 个一级框架，并下设 14 个二级框架的内容建议，具体标准体系如图6-1所示。

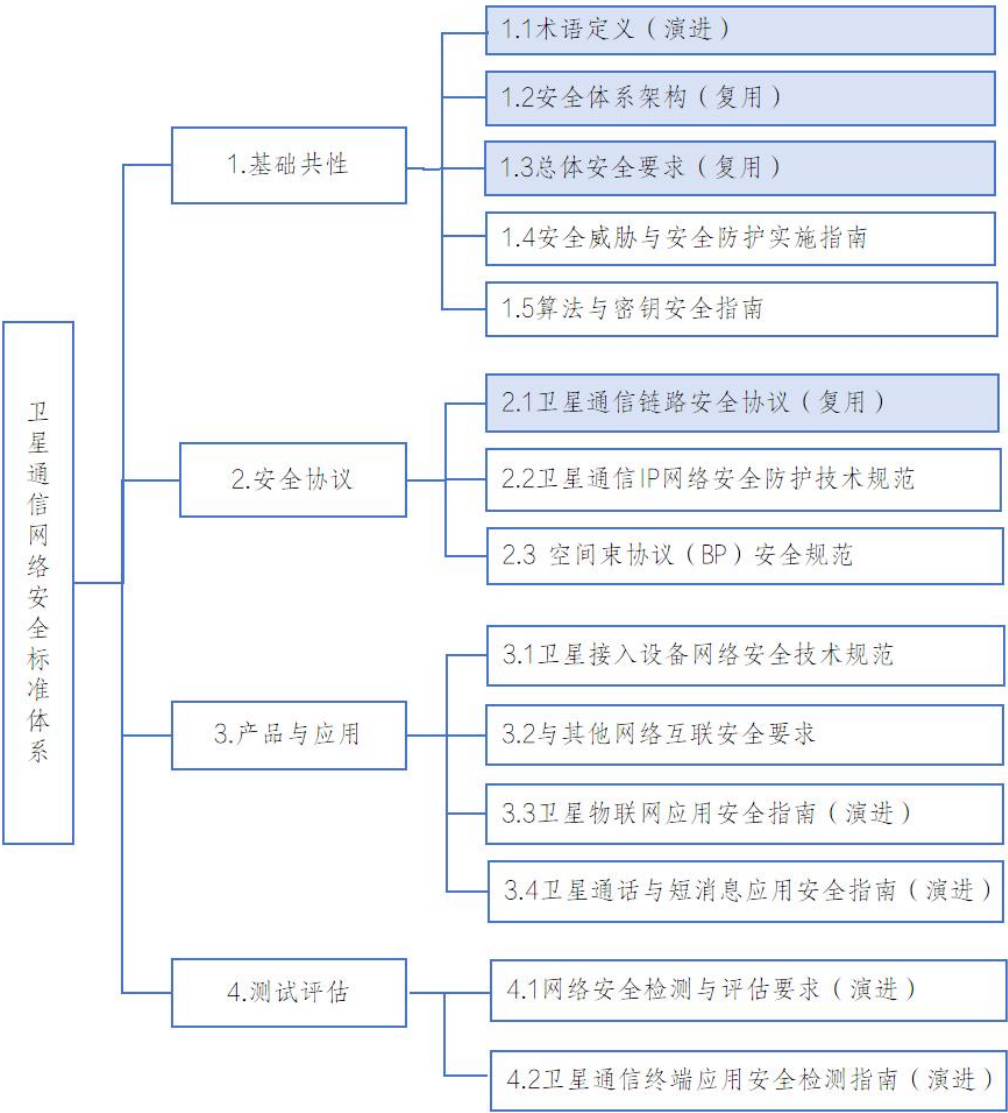


图 6-1 卫星通信网络安全标准体系

以下对卫星通信网络安全标准体系的一级框架、二级框架以及对应标准建议的主要内容进行了说明，见表6-1。

表 6-1 卫星通信网络安全标准体系说明及标准制定建议

一级框架	二级框架	主要内容（核心内容）	拟解决问题和解决思路	标准制定建议
1. 基础共性	1.1 术语定义	界定卫星通信与安全相关的术语及定义	通过术语和定义的界定,使得行业内的专有名词及含义通过本文件制定能达成共识,形成共同认可的术语范畴及含义。 解决思路: (1) 参考行业政策文件,如无线电管理局制定的43种无线电业务^[47]。 (2) 复用已有标准 (GB/T 42041、GB/T 25069) ; (3) 复用拟立的国家标准计划《卫星互联网应用服务术语》; (4) 可按需修订补充卫星通信网络安全有关术语	复用: (1) GB/T 42041-2022 《航天术语 空间数据与信息传输》 (2) GB/T 25069-2022 《信息安全技术 术语》 (3) 国家标准制定立项计划《卫星互联网应用服务术语》 (SAC/TC425/WG2)
	1.2 安全体系架构	提出卫星通信网络安全框架,包括网络安全架构组成、参考点、主要功能模块及安全能力、网络安全实施与评估过程。	通过提出卫星通信安全体系架构,参考模型,以此明确安全体系架构的范畴、主要内容、边界和逻辑组成、必要的安全防护实施与评估过程。 解决思路: (1) 参考ISO 20214-2015 空间数据和信息传输系统 - 空间数据系统的安全架构 (2) 参考GB/T 42037-2022 空间数据与信息传输系统 参考体系架构; (3) 参考NIST CSF2.0网络空间安全框架;	复用: (1) 国家标准项目计划《网络安全技术 卫星互联网网络安全框架》 (SAC/TC260)

		采用包括多维度分析及对应核心功能的明确； (4) 参 考 NIST IR 8441 Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN)（混合卫星网络（HSN）网络安全框架轮廓）； (5) ETSI TS 103 中 宽 带 卫 星 多 媒 体（BSM）文档结构中安全相关的通用安全架构（Security General Security Architecture [i.8]）、多点传输安全体系结构（Multicast Security Architecture [i.7]） (6) 与3GPP NTN架构及安全标准在定义或研究中能相互协调。	
1.3 总体安全要求	规定卫星通信网络总体安全要求,主要包括卫星通信空间段、地面段、应用段的总体安全范畴、安全基线、安全技术要求与评估,安全管理总体要求。	通过规范卫星通信网络安全总体要求,为相关的研制方、建设方、用户及监管部门提供针对该领域的总体安全技术与管理规范化指导。有利于卫星通信领域网络安全防护的提前预计、提升卫星等航天器及地面系统自身的网络安全防护能力,如抵御传统及新型网络攻击威胁、检测攻击行为、应对网络攻击以及必要时恢复系统等核心能力目标的达成。并关注需求、安全能力、安全技术措施、安全的实施、检测与评估。 解决思路： (1) 采取复用已开展的国家标准项目计划20251139-T-469《空间数据与信息传输系统	复用： (1) 20251139-T-469《空间数据与信息传输系统 网络安全总体技术要求》（SAC/TC425/SC3） 该文件规定了空间数据与信息传输系统网络安全总体技术要求,适用于空间段、空间链路部分的网络安全相关要求。 (2) 国家标准项目计划《卫星互联网网络安全技术指南》（SAC/TC485） 该文件主要内容包括卫星互联网

		网络安全总体技术要求》和《卫星互联网网络安全技术指南》 (2) 参 考 3GPP TR 33.700-29 V19.1.0 (2025-07) Study on security aspects of 5G satellite access in the 5G architecture phase 3 (Release 19) (5G架构阶段3中5G卫星接入安全研究) 等3GPP NTN架构相关的安全标准研究。	体系结构、卫星互联网安全需求、安全域划分（物理域、控制域、数据域、应用域等）安全需求、卫星互联网安全架构、卫星互联网物理域安全技术指南（抗干扰安全技术、防窃听安全技术、欺骗避免安全技术、物理层抗太空辐照安全技术、太空防碰撞安全技术）、卫星互联网控制域安全技术指南（含测控安全技术、身份认证与密钥管理技术、访问控制安全技术、链路控制安全技术、路由控制安全技术、传输控制安全技术等）、卫星互联网数据域安全技术指南（源地址验证技术指南、数据机密/完整性保护技术、数据转发安全技术、异常流量检测、溯源与过滤技术、抗DDoS攻击技术）、卫星互联网业务域安全技术指南。
1.4 卫星通信安全威胁与安全防护实施指南	提出卫星通信系统星间、星-地、地-星、地-星-地等双向通信过程中可能面临的安全威胁与对应的防护实施建议(其中地泛指地球表面设备以及航天器)。	本文件参考已有的相关标准规范与研究成果,提出卫星通信面临的安全威胁的针对性地分析,综合安全架构、总体安全要求的规范性指导,提出应对对应安全威胁的具体防护实施方法。 解决思路:参考以下国内外相关标准或标准研究成果: (1) CCSDS 350.1-G-1 绿皮书 Security	建议制定标准: 《网络安全技术 卫星通信安全威胁与安全防护实施指南》

		Threats against Space Missions. Report Concerning Space Data System Standards (空间任务的安全威胁.空间数据系统标准报告) (2) GB/Z 30286-2013 信息安全技术 信息系统保护轮廓和信息系统安全目标产生指南 (3) NIST CSF2.0 网络安全保护轮廓 (4) GB/T 37027-2025 网络安全技术 网络攻击和网络攻击事件判定准则 (5) GB/T 30279-2020 信息安全技术 网络安全漏洞分类分级指南 (6) GB/T 20986-2023 信息安全技术 网络安全事件分类分级指南 (7) ETSI TR 102 287 V1.1.1 中描述的宽带卫星多媒体 (BSM) 系统面临的威胁	
1.5 算法和密钥安全指南	提出卫星通信采用密码技术进行网络安全保护所需密码算法配置、密钥配置与安全建议,适应于不同轨道通信卫星延时、抖动等技术差异;不同卫星通信业务(实时/非实时、指令/数据、窄带/宽带、优先级等)安全需求差异;以及抵抗新技术安全挑战(如抗量子计	在采用国家法律法规和相关主管部门核准的算法条件下,卫星通信网络安全涉及的算法及密钥设计与实施面临如卫星互联网、卫星物联网的网络化进程的驱动,在泛在连接、宽带通信、高速传输、抗量子计算、6G (3GPP NTN) 对高速大并发等新的技术需求及挑战下,提出有不同业务特征、技术特征需求下的有针对性的密码算法配置、密钥配置与安全建议。 解决思路:参考以下国内外相关标准或标准	建议制定标准: 《网络安全技术 卫星通信算法和密钥安全指南》

		算、Ai流量特征分析等)挑战等对密码算法及密钥防护能力等的不同需求及配置指南。	研究成果： (1) GB/T 17901《信息技术 安全技术 密钥管理》系列标准 (2) CCSDS Crptographic Algorithms.Recommendation for Space Data System Standards, CCSDS 352.0-B-0.Blue Book (CCSDS 密码算法 空间数据系统标准建议 蓝皮书) . Issue 0. Washington, D.C: CCSDS forthcoming. (3) 3GPP 加密清单 (3GPP Rel-19 SP-241771 New Study on 3GPP Cryptographic Inventory) (4) NIST及我国抗量子密码、6G新一代密码算法等研究成果	
2. 安全协议	2.1 卫星通信链路安全协议	本文件规定了协议数据单元和协议数据单元执行的流程。适应于CCSDS遥测(TM)、遥控(TC)和先进轨道系统(AOS)空间数据链路协议。	CCSDS遥测(TM)、遥控(TC)和先进轨道系统(AOS)空间数据链路协议等是目前国际、国内主流的空间数据与传输系统链路层协议。对链路层协议进行安全协议进行规范化有利于卫星通信链路层数据通信与传输的安全性及互操作性。 解决思路： 制定空间数据与信息传输系统的空间数据链路安全协议标准。该协议引标自： ISO 21324:2016 Space data and information transfer systems — Space data link security protocol.	复用： SAC/TC425/SC3 制标计划 《空间数据与信息传输系统 空间数据链路安全协议》

			提出了一个安全数据报结构以及相关过程，可用于 CCSDS 遥测、遥控和先进轨道系统空间数据链路协议，以提供在数据链路层应用数据认证和/或数据机密性的结构化方法。	
2.2 卫星通信 IP 网络安全防护技术规范	本文件规定了基于IP协议的卫星通信网络安全防护要求和测试方法,包括通信网络与传输协议安全、网元设备安全、管理安全等方面。本文件适用于指导支持IPv4/IPv6 协议的卫星通信网络安全工作开展和实施。	当前，基于IP协议进行卫星通信网络传输的承载及技术应用十分广泛，IP over CCSDS在CCSDS协议体系获得共识。本文件制定用于卫星通信的IP网络安全协议，在非卫星通信段采用标准的地面段IP网络协议，在与卫星通信的通信链路采用适应空间通信链路的IPv4/IPv6网络安全协议。并在网络边缘节点网关等网元设备完成协议的适配与安全转换，满足对相关网元设备安全及管理安全的相关要求。 解决思路：可参考国际与国内相关标准及应用成果： （1）GB/T 45279.1-2025 IPv4/IPv6 网络安全防护技术规范 第1部分：IP承载网； （2）GB/T 45279.2-2025 IPv4/IPv6 网络安全防护技术规范 第2部分：移动通信网 （3）IP over CCSDS等技术成果，如CCSDS Network Layer Security Adaptation Profile（网络层安全适配轮廓）	建议制定标准： 《网络安全技术 卫星通信 IP 网络安全防护技术规范》	
2.3 空间束协	本文件规定了基于BP协议	制定适应卫星通信的BP安全协议，主	建议制定标准：	



	议（BP）安全规范	的卫星通信网络安全防护要求和测试方法,包括通信网络与传输协议安全、网元设备安全、管理安全等方面。本文件适用于指导支持BP协议的空间卫星通信安全工作开展和实施。	要用于深空通信、星际网络等存在高延迟、高误码率、间歇性连接等特点的网络,以支持在复杂空间网络环境下不同节点之间端到端的安全数据传输。 解决思路: 可参考: (1) ISO 21323:2016空间数据和信息传输系统 CCSDS束协议规范 (Space data and information transfer systems - CCSDS Bundle protocol specification)	《网络安全技术 空间束协议 (BP) 安全规范》
3. 产品与应用	3.1 卫星接入设备网络安全技术规范	本文件规定了卫星接入设备网络安全通用技术要求,包括应用场景与安全需求、安全功能要求、安全基本流程、相关检测方法等。 本文件适用于含卫星通信的电信网络提供的业务和应用通过卫星地面站、信关站、卫星接入终端、机载/船载卫星接入设备等在卫星客户网络内部实现的情况,对仅在客户网络内部设备之间信息流通的情况也可参考使用。	卫星接入设备主要包括地面段、用户段不同业务用途的卫星接入设备通过空间链路、空地链路或地面关口站等方式与航天器实现接入与通信应用。3GPP智能终端直连卫星应用及3GPP NTN 技术演进形成对卫星通信网络更广泛的接入及互联。因此有必要开展卫星接入设备网络安全技术规范的制定。 解决思路: 可参考: (1) GB/T 29234—2012 基于公用电信网的宽带客户网络安全技术要求 (2) 3GPP TR 33.700-29 V19.1.0 (2025-07)Study on security aspects of 5G satellite access in the 5G architecture phase 3 (Release 19) (5G架构阶段3中5G卫星接入安全研究)。该文件主要内容包括NR NTN (5GS) 和物联网 NTN (EPS) 相关载荷通	建议制定标准: 《网络安全技术 卫星接入设备网络安全技术规范》

			用架构的安全与隐私关键问题；5GS中用户设备-卫星-用户设备通信增强的关键安全与隐私问题；5G卫星接入对监管服务的影响。特别是对再生传输、存储转发（S&F）以及用户设备-卫星-用户设备通信增强架构中合法拦截潜在影响的评估。	
3.2 卫星通信网络与其他网络互联安全指南	提出卫星通信网络与其他网络互连（以下简称互联）的安全指南,主要包括互联网络结构及参考点、互联安全需求、网络边界安全、数据安全,安全QoS保障等安全技术与实施指南建议。	提出卫星通信网络与其他网络互连（以下简称互联）的安全指南,主要包括互联网络结构及参考点、互联安全需求、网络边界安全、数据安全,安全QoS保障等安全技术与实施指南建议。	提出卫星通信网络与其他网络,如不同的卫星通信网络、移动通信网、互联网、电话网络等其他网络进行互连互通,存在的安全风险、安全需求、安全防护技术建议。 解决思路: 可参考: (1) CCSDS Guide for Secure System Interconnection.Report Concerning Space Data System Standards, CCSDS 350.4-G-1. Green Book (CCSDS 安全系统互连指南.空间数据系统标准报告.CCSDS 350.4-G-1 绿皮书)。 (2) GB/T 44886.1-2024 网络安全技术 网络安全产品互联互通 第1部分: 框架	建议制定标准: 《网络安全技术 卫星通信网络与其他网络互联安全指南》
3.3 卫星物联网应用安全指南	提出卫星物联网应用场景下的应用安全指南,包括卫星物联网应用安全结构和组成、感知层接入卫星通信网络的安全需求、应用安全功能、基本实施过程等建议	提出卫星物联网应用场景下的应用安全指南,包括卫星物联网应用安全结构和组成、感知层接入卫星通信网络的安全需求、应用安全功能、基本实施过程等建议	根据《工业和信息化部关于组织开展卫星物联网业务商用试验的通知》(工信部信管函〔2025〕307号), 卫星物联网业务是指通过卫星通信技术连接各类物联网设备,为数据采集终端、穿戴设备、手持终端等各类终端, 以及汽车、船舶、飞机等交通工具提供广域物联网连接的一种低速数据业务。	建议制定标准: 《网络安全技术 卫星物联网应用安全指南》

		提出卫星物联网应用指南，通过提出应用场景安全需求、安全结构与组成、安全功能的建议，可为相关业务的研制、实施及评估提供规范化的指导或参考。 解决思路：可参考相关标准如： (1) GB/T 37044 信息安全技术 物联网安全参考模型及通用要求 (2) GB/T 37093 信息安全技术 物联网感知层接入通信网的安全要求 (3) GB/T 37025 信息安全技术 物联网数据传输安全技术要求 (4) GB/T 36951 信息安全技术 物联网感知终端应用安全技术要求 (5) GB/T 33474-2025 物联网 参考体系结构 (6) GB/T 40022-2021 基于公众电信网的物联网总体要求	
3.4 卫星通话与短消息应用安全指南	本文件提出了卫星通话与短消息应用的基本安全框架及安全控制措施，包括密码算法与应用安全、通信数据隐私保护、卫星通话与短消息入网鉴权与通信平台安全、应用设备（如卫星通信终端、调度台）安全、安全管理等措施与实施指南。	随着低轨卫星星座规模化部署，用户段是卫星应用主体，对卫星产业发展起到推动及扩大场景的核心作用。卫星通话和短消息有极大的用户基数及应用发展潜力。5G NTN及6G 将移动通信从地面移动通信网拓展到星地一体广域网络。卫星通信终端安全风险及安全防护技术要求的标准化十分重要。 解决思路：参考天地话音、短消息，以及移	建议制定标准： 《网络安全技术 卫星通话与短消息应用安全指南》

		本文件适用于卫星通话与短消息应用安全相关开发、部署和测试、运维等。	动卫星电话等卫星移动业务相关业务要求，通过场景与安全需求分析，提出卫星通话与短消息应用的基本安全框架及安全控制措施，包括密码算法与应用安全、通信数据隐私保护、卫星通话与短消息入网鉴权与通信平台及应用设备安全、安全管理措施与实施指南。	
4. 测试评估	4.1 卫星通信网络安全检测与评估要求	提出卫星通信网络安全检测与评估的过程、操作与实施任务建议。	对上述提出的网络安全标准化相关规范、指南建议等，提出对应的检测与安全评估方法，形成有效的闭环，以对过程或可交付成果满足既定特征或目标要求的接近度予以评估及保证。 解决思路：借鉴我国网络安全检测评估相关规范，如： (1) GB/T 30270-2024 网络安全技术 信息技术安全评估方法（引标自 ISO/IEC 18045:2022） (2) GB/T 43206-2023 信息安全技术 信息系统密码应用测评要求 (3) GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求 (4) GB/T 36627-2018 网络安全等级保护测试评估技术指南	建议制定标准： 《网络安全技术 卫星通信网络安全检测与评估要求》
	4.2 卫星通信终端应用安全检测指南	提出卫星通信终端（智能终端等）进行典型卫星应用，如卫星电话、卫星短消息通	根据提出的卫星通话与短消息应用安全指南、卫星物联网应用安全指南等建议要求或指导性技术文件。对卫星通信终端应用	建议制定标准： 《网络安全技术 卫星通信终端应用安全检测指南》



		信、卫星图传等卫星用户典型应用的安全检测方法建议。	安全相关的安全措施方法进行验证与检验，以确定其符合相关要求的能力符合性，并通过检测结果对技术措施的实施予以优化改进，以指导相关应用安全防护的持续完善。参考语音、消息等多类型通信应用安全检测方法、3GPP典型应用场景相关安全检测标准规范或研究成果。	
--	--	---------------------------	---	--



全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

6.4 小结

规范卫星通信网络安全的标准化体系及相关标准研制,包括且不限于从空间段、地面段、应用段,针对通信接入授权;与通信业务QoS相匹配的通信网络的可靠性与安全性;安全通信网络、安全区域边界、安全的数据与应用,以及互联安全通用要求等。本研究工作将有利于卫星通信网络安全防护的设计与应用,有利于网络安全的规范化与互操作性。本章从卫星通信网络安全标准化工作的总体思路、标准体系设计说明、标准体系结构框架及具体标准系列工作建议,提出了一级框架4个,下设14个二级框架的标准制定或复用演进等工作建议。

考虑主要针对卫星通信网络应用发展趋势、自主可控航天安全的持续演进、卫星通信网络安全监控与评估等,尚需不断探索、实践试点、进行大量艰苦细致的摸索和实践。针对高、中低轨卫星不同的发展路径及需求,兼顾航天强国稳健可靠、自力更生、严谨细实、可控可管的航天发展特点。在未来空间信息系统应用中,针对航天器自主可控,空间通信资源、载荷资源等的有效利用涉及安全及国家利益。对各类攻击的有效认知、防范及预警、研究突破空间各类攻击及安全防护技术及产品,形成对未来空间资源的和平利用。具有重要的军事意义及社会意义。

附录 A 相关政策法规清单（国际/国内）

A.1 国内概览

- (1) 《中华人民共和国网络安全法》
- (2) 《中华人民共和国密码法》
- (3) 《中华人民共和国数据安全法》
- (4) 《中华人民共和国个人信息保护法》
- (5) 《关键信息基础设施安全保护条例》
- (6) 《信息安全等级保护管理办法》（公通字[2007]43号）
- (7) 《商用密码应用安全性评估管理办法》（国家密码管理局令第3号）
- (8) 相关政策文件
 - a. 2015年，国家发展改革委、财政部、国防科工局发布《国家民用空间基础设施中长期发展规划（2015—2025年）》
 - b. 2020年4月，国家发展改革委将卫星互联网纳入新型基础设施建设范畴
 - c. 2021年11月，《工业和信息化部关于印发“十四五”信息通信行业发展规划的通知》（工信部规〔2021〕164号）
 - d. 2022年2月，国务院《“十四五”国家应急体系规划》中提出：针对地震、滑坡、泥石流、堰塞湖、溃堤溃坝、森林火灾等重大险情，加强太阳能长航时和高原型大载荷无人机、机器人以及轻量化、智能化、高机动性装备研发及使用，加大5G、高

通量卫星、船载和机载通信无人机通信等先进技术应急通信装备的配备和应用力度

- e. 2025 年 3 月，工业和信息化部发布《卫星网络国内协调管理办法（暂行）》
- f. 2025 年 4 月，国家互联网信息办公室等七部门联合发布《终端设备直连卫星服务管理规定》（国信办发文〔2025〕1 号）
- g. 2025 年 7 月，国家航天局发布《关于加强商业航天项目质量监督 ze 管理 ze 工作的通知》
- h. 2025 年 8 月 25 日，工业和信息化部发布《工业和信息化部关于优化业务准入促进卫星通信产业发展的指导意见》（工信部信管〔2025〕180 号）
- i. 2025 年 10 月 10 日，工业和信息化部发布“公开征求对《工业和信息化部关于组织开展卫星物联网业务商用试验的通知（征求意见稿）》的意见”的通知。
- j. 2025 年 11 月 25 日，工业和信息化部发布《工业和信息化部关于组织开展卫星物联网业务商用试验的通知》（工信部信管函〔2025〕307 号）
- k. 2025 年 11 月 25 日，国家航天局官网发布《国家航天局推进商业航天高质量发展安全发展行动计划（2025—2027 年）》

A.2 国际概览

- (1) 2006 年，美国发布《2005~2030 年 NASA 空间通信与导航体系结构建议》

- (2) 2018 年 6 月，美国总统特朗普签署 3 号航天政策令《国家太空交通管理政策》。美国国家航天委员会成立于 2017 年 6 月，成立以来共举行了三次公开会议，“1 号航天政策令”重返月球；“2 号航天政策令”简化对太空商业化利用的监管。本次发布的“3 号航天政策令”推动跨部门的职能整合，力图通过制度创新适应新兴商业模式的需求
- (3) 2022 年 4 月，美国国会通过《卫星网络安全法》。根据法案要求，网络安全和基础设施安全局（CISA）将起草旨在协助商业卫星系统的开发、维护和运营的自愿型网络安全建议，包括风险监控、系统复原及防止未经授权访问等指南
- (4) 2022 年 5 月，美国网络安全和基础设施安全局（CISA）宣布成立“太空系统关键基础设施工作组”
- (5) 2024 年 4 月，美国国防部、天军联合发布《商业航天整合战略》。该战略描绘了商业航天整合过程中的基本原则、优先事项以及强化各类冲突中航天任务保障的方法，确保其能通过整合商业航天进一步增强国家太空安全体系的弹性与威慑力。确立了四项原则：平衡性、互操作性、弹性和负责任的行为。弹性原则指出：美国国防部优先考虑国家安全体系的弹性。商业航天的整合将通过增加供应商数量、促进供应链多样化、扩大国防部可采用解决方案的种类与规模等方式，进一步增强国家安全体系的弹性。国防部采用的商业解决方案本身也必须具备弹性，特别是在应对网络威胁方面^[24]

- (6) 2017 年英国发布《卫星和空间科学领域空间频谱战略报告》，目的是对卫星宽带的使用和普遍服务义务的进展进行监督。该计划进一步放宽非同步轨道卫星的频谱使用，适时引入新业务，以提高卫星通信频谱的利用率
- (7) 2025 年 6 月 25 日，欧盟委员会公布了欧盟《空间法案》提案
- (8) 移动卫星服务协会（MSSA）与全球移动通信协会（GSMA）开展战略合作，共同探索通过卫星移动业务（MSS）基于 3GPP 标准的手机直连卫星（D2D）和物联网（IoT）服务的前沿技术。发展开放、可互操作的生态系统，无缝连接地面（TN）和非地面网络（NTN）

附录 B 相关标准列表（国际/国内）

B.1 国际标准

ISO/IEC 与空间安全相关的标准包括且不限于：

- (1) BS ISO 20214-2015 Space data and information transfer systems. Security architecture for space data systems(空间数据和信息传输系统 空间数据系统的安全体系结构)
- (2) ISO 20214-2015 Space data and information transfer systems-Security architecture for space data systems (空间数据和信息传输系统-空间数据系统的安全架构)
- (3) ISO 21324：2016 Space data and information transfer systems — Space data link security protocol(空间数据和信息传输系统-空间数

据链路安全协议) 该协议可与 CCSDS 遥测、遥控和先进轨道系统空间数据链路协议一起使用, 以提供在数据链路层应用数据认证和/或数据机密性的结构化方法。

CCSDS 安全相关系列标准包括且不限于:

- (1) CCSDS Application & Support Architecture (应用与支撑架构)
- (2) CCSDS Global Spacecraft Identifier Field: Code Assignment Control Procedures (全球航天器识别符字段: 编码分配控制程序)
- (3) Reference Architecture for Space Data Systems (RASDS) (空间数据系统参考体系结构)
- (4) Registry Management Policy (注册管理策略)
- (5) Space Communication Cross Support Architecture Requirements Document (空间通信交叉支持体系架构需求文档)
- (6) CCSDS Authentication Credentials (认证)
- (7) CCSDS Key Management Guide (密钥管理指南)
- (8) CCSDS Security Guide for Mission Planners (任务规划人员安全指南)
- (9) CCSDS Symmetric Key Management Recommendations (对称密钥管理建议)
- (10) Intergovernmental Cloud-based Certification Authority 政府间基于云的认证机构
- (11) Network Layer Security Adaptation Profile (网络层安全适配轮

廓)

- (12) Reference Architecture for Space Data Systems. Recommendation for Space Data System Practices, CCSDS 311.0-M-1. Magenta Book. (空间数据系统参考体系结构.空间数据系统建议实践. CCSDS 311.0-M-1 洋红皮书) Issue 1. Washington, D.C.:CCSDS, September 2008.
- (13) Security Architecture for Space Data Systems. Issue 1.Recommendation for Space Data System Practices (Magenta Book), CCSDS 351.0-M-1 (空间数据系统安全体系结构.发布 1.空间数据系统建议实践(洋红皮书)), CCSDS 311.0-M-1. Washington, D.C.:CCSDS, November 2012.
- (14) The Application of CCSDS Protocols to Secure Systems. Report Concerning Space Data System Standards, CCSDS 350.0-G-2.Green Book (CCSDS 协议在安全系统中的应用.关于空间数据系统标准的报告. CCSDS 350.0-G-2 绿皮书) . Issue 2. Washington,D.C.:CCSDS, January 2006.
- (15) Space Missions Key Management Concept. Issue 1.Report Concerning Space Data System Standards, CCSDS 350.6-G-1. Green Book (空间任务密钥管理概念.空间数据系统标准报.发布 1.CCSDS 350.6-G-1 绿皮书) . Issue 1.Washington,D.C.: CCSDS,November 2011.
- (16) CCSDS Crptographic Algorithms.Recommendation for Space

Data System Standards, CCSDS 352.0-B-0.Blue Book(CCSDS 密码算法。空间数据系统标准建议.CCSDS 352.0-B-0 蓝皮书)。Issue 0. Washington, D.C: CCSDS forthcoming.

(17) Security Threats against Space Missions. Report Concerning Space Data System Standards, CCSDS 350.1-G-1. Green Book (空间任务的安全威胁.空间数据系统标准报告 CCSDS 350.1-G-1 绿皮书)。Issue 1. Washington, D.C: CCSDS October 2006.

(18) CCSDS Guide for Secure System Interconnection.Report Concerning Space Data System Standards, CCSDS 350.4-G-1. Green Book(CCSDS 安全系统互连指南.空间数据系统标准报告.CCSDS 350.4-G-1 绿皮书)。Issue 1. Washington, D.C.:CCSDS, November 2007.

(19) Information Security Glossary of Terms. Draft Report Concerning Space Data System Standards,CCSDS 350.8-G-0.Draft Green Book (信息安全术语.空间数据系统标准草案报告,CCSDS 350.8-G-0 绿皮书草案) , Issue 0.Washington.D.C.:CCSDS, forthcoming.

(20) Overview of Space Communications Protocols. Issue 3. Report Concerning , SpaceData System Standards (Green Book) (空间通信协议概述。发布 3, 空间数据系统标准报告, 绿皮书) , CCSDS 130.0-G-3. Washington,D.C.:CCSDS, July 2014.

(21) Space Data Link Security Protocol Extended Procedures. Recommendation for Space Data System Standards(空间数据链路安

全协议扩展过程.空间数据系统标准建议), CCSDS 355.1-B.
Washington, D.C: CCSDS,forthcoming

NIST 卫星领域安全相关系列标准:

- (1) NIST IR 8441 September 2023 Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN) (混合卫星网络 (HSN) 网络安全框架轮廓)
- (2) NIST IR 8270 July 2023 interagency Report Introduction to Cybersecurity for Commercial Satellite Operations (NIST 跨机构报告商业卫星运行网络安全导论)
- (3) NIST IR 8401 December 2022 Satellite Ground Segment Applying the Cybersecurity Framework to Satellite Command and Control (卫星地面段 网络安全框架在卫星命令和控制中的应用)

3GPP与卫星通信安全有关的标准或标准研究包括且不限于:

- (1) 3GPP Rel-19 TR 22.865 V19.2.0 (2023-12) Study on satellite access Phase 3 卫星接入研究第三阶段
- (2) 3GPP Rel-19 SP-241780 Security Aspects of 5G Satellite Access Phase 3 (5G 卫星接入的安全目标)
- (3) 3GPP Rel-19 TR 33.700-29 V19.1.0 (2025-07) Study on security aspects of 5G satellite access in the 5G architecture phase 3 (Release 19) (5G 架构阶段 3 中 5G 卫星接入安全研究)

- (4) 3GPP Rel-20 SP-250654 3GPP New Study on Transitioning to Post Quantum Cryptography in 3GPP (向后量子密码学过渡的新研究)
- (5) 3GPP Rel-19 SP-241771 New Study on 3GPP Cryptographic Inventory (关于 3GPP 加密清单的新研究)
- (6) 3GPP Rel-20 SP-250653 New WID on mission critical security enhancements for release 20 (Rel-20 中新 WID 关键任务安全增强功能)
- (7) 3GPP Rel-20 SP- 250876 New WID on Security related Events Handling (新 WID 与安全相关的事件处理)
- (8) 3GPP Rel-20 SP-250877 New WID on Security Assurance Specification for 5G-Advanced (新 WID 5G-Advanced 安全保证规范)

ETSI 已发布卫星相关标准包括且不限于：

- (1) ETSI TR 101 984 V1.2.1 Satellite Earth Stations and Systems (SES) Broadband Satellite Multimedia (BSM), Services and architectures (卫星地球站和系统 (SES) 宽带卫星多媒体 (BSM) , 服务和架构)
- (2) ETSI TR 102 287 V1.1.1 (2004-05) Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM) ; IP Interworking over satellite; Security aspects (卫星地球站和系统 (SES) ; 宽带卫星多媒体 (BSM)
- (3) ETSI TS 103 275 V1.1.1 (2015-05)Satellite Earth Stations and

Systems (SES); Broadband Satellite Multimedia (BSM); Common air interface specification; Satellite Independent Service Access Point (SI-SAP) interface: Services (卫星地球站和系统 (SES) ; 宽带卫星多媒体 (BSM) ; 通用空中接口规范; 卫星独立业务接入点 (SI-SAP) 接口: 服务)

B.2 国内标准

卫星通信相关国家标准包括且不限于:

- (1) GB/T 43670-2024 空间数据与信息传输系统 航天器 SpaceFibre 总线通信协议
- (2) GB/T 43671-2024 空间数据与信息传输系统 航天器 CAN 总线通信协议
- (3) GB/T 43669-2024 空间数据与信息传输系统 航天器 1553B 总线通信协议
- (4) GB/T 43374-2023 空间数据与信息传输系统 航天器信息系统软件体系结构
- (5) GB/T 43372-2023 空间数据与信息传输系统 深空光通信物理层
- (6) GB/T 43375-2023 空间数据与信息传输系统 封装包协议
- (7) GB/T 43373-2023 空间数据与信息传输系统 深空测控伪码测距技术要求
- (8) GB/T 43379-2023 空间数据与信息传输系统 基于 XML 的遥测遥控信息交换规范

- (9) GB/T 43423-2023 空间数据与信息传输系统 深空光通信编码与同步
- (10) GB/T 43424-2023 空间数据与信息传输系统 运载火箭航天器图像通信要求
- (11) GB/T 42636-2023 空间数据与信息传输系统 无损数据压缩
- (12) GB/T 42651-2023 空间数据与信息传输系统 图像数据压缩
- (13) GB/T 42650-2023 空间数据与信息传输系统 多光谱和高光谱图像无损及近无损压缩
- (14) GB/T 42644-2023 空间数据与信息传输系统 束协议
- (15) GB/T 42634-2023 空间数据与信息传输系统 星载数据管理监控设计要求
- (16) GB/T 42649-2023 空间数据与信息传输系统 利克莱德传输协议(LTP)
- (17) GB/T 42041-2022 航天术语 空间数据与信息传输
- (18) GB/T 42037-2022 空间数据与信息传输系统 参考体系架构
- (19) GB/T 42040-2022 空间数据与信息传输系统 统一空间数据链路协议
- (20) GB/T 42039-2022 空间数据与信息传输系统 空间包协议
- (21) GB/T 42038-2022 空间数据与信息传输系统 文件传输协议
- (22) GB/T 39354-2020 空间数据与信息传输系统 邻近空间链路协议
- (23) GB/T 39351-2020 物理层空间数据与信息传输系统 遥测空间

数据链路协议

- (24) GB/T 39352-2020 空间数据与信息传输系统 邻近空间链路协议 数据链路层
- (25) GB/T 39344-2020 空间数据与信息传输系统 通信操作规程-1
- (26) GB/T 39350-2020 空间数据与信息传输系统 遥控空间数据链路协议
- (27) GB/T 39345-2020 空间数据与信息传输系统 高级在轨系统空间数据链路协议
- (28) GB/T 39348-2020 空间数据与信息传输系统 遥测同步与信道编码
- (29) GB/T 39349-2020 空间数据与信息传输系统 遥控同步与信道编码
- (30) GB/T 39353-2020 空间数据与信息传输系统 邻近空间链路协议 同步和编码子层
- (31) GB/T 39355-2020 空间数据与信息传输系统 时间码格式
- (32) GB/T 37833-2019 航天器安全防护通用要求
- (33) GB/T 12364-2007 国内卫星通信系统进网技术要求

与通信安全有关的国家标准包括且不限于：

- (1) GB/T 15843.2-2024 网络安全技术 实体鉴别 第2部分：采用鉴别式加密的机制
- (2) GB/T 15843.3-2023 信息技术 安全技术 实体鉴别 第3部分：采

用数字签名技术的机制

(3) GB/T 15843.4-2024 网络安全技术 实体鉴别 第 4 部分:采用密码
校验函数的机制

(4) GB/T 15852.1-2020 信息技术 安全技术 消息鉴别码 第 1 部分:
采用分组密码的机制

(5) GB/T 15852.2-2024 网络安全技术 消息鉴别码 第 2 部分:采用专
门设计的杂凑函数的机制

(6) GB/T 15852.3-2019 信息技术 安全技术 消息鉴别码 第 3 部分:
采用泛杂凑函数的机制

(7) GB/T 18336-2001 信息安全技术 信息技术安全性评估准则

(8) GB/T 20269-2006 信息安全技术 信息系统安全管理要求

(9) GB/T 20984-2007 信息安全技术 信息安全风险评估规范

(10) GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

(11) GB/T 24364-2009 信息安全技术 信息安全风险管理指南

(12) GB/T 25058-2019 信息安全技术 网络安全等级保护实施指南

(13) GB/T 25069 信息安全技术 术语

(14) GB/T 25070-2019 信息安全技术 信息系统等级保护安全设计
技术要求

(15) GB/T 28453-2012 信息安全技术 信息系统安全管理评估要求

(16) GB/T 28448-2012 信息安全技术 信息系统安全等级保护测评
要求

(17) GB/T 32915 信息安全技术 二元序列随机性检测方法

- (18) GB/T 36624 信息技术 安全技术 可鉴别的加密机制
- (19) GB/T 36635-2018 信息安全技术 网络安全监测基本要求与实施指南
- (20) GB/T 37092 信息安全技术 密码模块安全要求
- (21) GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求

相关的行业标准包括且不限于：

- (1) GM/Z 4001-2013 密码术语
- (2) GM/T 0054-2018 信息系统密码应用基本要求
- (3) YD/T 5028-2018 国内卫星通信小型地球站（VSAT）通信系统工程设计规范
- (4) YD/T 3908-2021 卫星移动通信终端通用技术要求和测试方法
- (5) YD/T 3934-2021 Ka 频段移动中使用的车载卫星通信地球站通用技术要求

CCSA标准制定及研究还包括且不限于：

- (1) 《面向 5G 网络及 5G 增强的天地一体化网络安全需求与安全能力研究》
- (2) 《IMT 地面网络与未来 NTN 卫星网络邻频共存兼容性研究》
- (3) 行标制定《基于非地面网络（NTN）的物联网窄带接入（NB-IoT）接入网总体技术要求》
- (4) 行标制定《基于非地面网络（NTN）的物联网窄带接入（NB-IoT）卫星接入节点技术要求》

- (5) 行标制定《基于非地面网络（NTN）的物联网窄带接入（NB-IoT）
卫星接入节点测试方法》
- (6) 行标制定《基于非地面网络（NTN）的物联网窄带接入（NB-IoT）
终端设备技术要求》
- (7) 行标制定《基于非地面网络（NTN）的物联网窄带接入（NB-IoT）
终端设备测试方法》
- (8) 行标制定《基于非地面网络（NTN）的 5G 卫星接入节点设备技
术要求(第一阶段)》
- (9) 行标制定《基于非地面网络无线工作组（NTN）的 5G 终端技术
要求(第一阶段)》
- (10) 行标制定《基于非地面网络（NTN）的 5G 卫星接入节点设备
测试方法(第一阶段)》
- (11) 行标制定《基于非地面网络（NTN）的 5G 终端测试方法(第一
阶段)》
- (12) 行标制定《基于非地面网络（NR NTN）的宽带接入网总体技
术要求(第一阶段)》
- (13) 行标制定《基于 5G 的卫星互联网 第 1 部分：总体要求》
- (14) 行标制定《IMT-2020 卫星无线电接口的愿景、要求和评估方
法》
- (15) 《面向多种应用场景的星地融合终端技术研究》
- (16) 《面向电力行业的星地融合无线通信技术研究》
- (17) 《星地网络协同无线组网技术研究》

- (18) 《终端直连卫星应用场景和能力需求研究》
- (19) 《星地融合网络实时通信技术研究》
- (20) 《天地一体融合通信中的语音增强需求及技术研究》
- (21) 《天地一体网联无人机业务连续性研究》



全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

参考文献

- [1] ISO 20214:2015 Space data and information transfersystems —
Security architecture forspace data systems
- [2] 《2023年国外通信卫星发展综述》，国际太空
- [3] 《空间信息网络体系架构与发展构想》，中国工程院2017年第五届全国空间数据系统学术交流会报告，于全
- [4] 《卫星通信系统安全技术综述》，电信科学，2013年第7期
- [5] 《军用卫星通信新技术及应用》，电子科技大学，朱立东，2015
- [6] 《浅谈信息战中通信卫星系统安全性》，空间电子技术，2016
- [7] 《我国空间互联网网络架构和标准体系研究》，白卫岗、周笛，西安电子科技大学ISN国家重点实验室，2019年
- [8] 《2019中国商业航天通信应用发展研究报告》，艾瑞咨询研究院
- [9] 《低轨通信卫星：开启6G 通信时代，带动千亿规模市场》，中国银河证券研究院，2020年
- [10] 《中国宽带发展白皮书》，中国信息通信研究院宽带发展联盟，2019年10月
- [11] 《高通量卫星有效载荷新技术研究与展望》，中国空间技术研究院西安分院，李立
- [12] 《卫星互联网行业发展趋势》，中国卫通，2023年10月
- [13] 《我国卫星移动通信技术发展与应用》，中国空间技术研究院通信与导航卫星总体部，2023年10月

- [14] 《手机直连卫星技术发展及思考》，中国电信卫星公司，李屹寰
- [15] 《“天通一号”卫星移动通信系统发展与物联网应用》，中国电科54，王艳君，2020年10月
- [16] 《卫星互联网行业发展情况研究》，中国信通院博鼎实华，郑艺，2024
- [17] 《低轨卫星与 5G-R 融合网络架构设计》，太赫兹科学与电子信息学报，2024年5月，韩紫杰等
- [18] 《IoT NTN技术发展观察与产业化实践》，中国电信，2024年卫星应用大会
- [19] 《国外通信卫星产业发展动向与趋势思考》，北京空间信息科技研究所，朱贵伟，2024年10月卫星应用大会
- [20] 《筑生态 促发展——中信卫星的转型之路》，中信卫星，边力军，2024年卫星应用大会
- [21] 《5G时代的卫星通信》，国防工业出版社，2023年
- [22] 《SaT5G联盟公布“卫星上的5G”解决方案，6大亮点引人注目》，航天长城
- [23] 《空间数据系统标准化概览》，中国科学院国家空间科学中心，黄永辉
- [24] 《国外通信卫星产业发展动向与趋势思考》，北京空间信息科技研究所，2024年10月

- [25] 《中国商业航天的前景趋势与促进举措》，西北工业大学军民融合发展战略研究中心，田庆锋
- [26] <https://www.nist.gov/news-events/news/2023/06/draft-nist-ir-844-1-hybrid-satellite-network-hsn-cybersecurity-framework>
- [27] Satellite Ground Segment: Applying the Cybersecurity Framework to Satellite Command and Control (nist.gov)
- [28] 《国外重点国家巨型星座监管制度比较研究》，国际太空，2025年7月，北京空间科技信息研究所、中国空间技术研究院
- [29] 《量子信息技术国内外标准化进展（2024）》，量子科技产学研创新联盟，2025年1月
- [30] IETF RFC 2401: "Security Architecture for the Internet Protocol"
- [31] Journey to the NIST CSF 2.0, Cheri Pascoe, Director, NIST NCCoE
- [32] CSF 2.0: www.nist.gov/cyberframework
- [33] Hughes Network Systems, LLC HT Satellite Terminals Hardware Version: HT2300,HT2500,HT2550,HT2650 Firmware Version: 7.4.1.19
- [34] 《美国“坚定太空2025”全领域太空战演习调研》，北京航天情报与信息研究所，张梓阳
- [35] 《手机直连卫星发展探讨》，中国电科网络通信研究院 2023年10月

- [36] Ubiquitous 6G Service through Non-Terrestrial Networks, IEEE wireless communications2023
- [37] 5G from Space: An Overview of 3GPP Non-Terrestrial Networks, IEEE Commun. Standards Mag., vol. 5, no. 4, 2021
- [38] .Management and Orchestration in Rel-19 (3gpp.org)
- [39] 《高通量卫星通信技术与应用创新发展思考》，航天恒星科技有限公司，503所
- [40] 2024年中国应用卫星大会会议文件
- [41] Kurose J F. Computer networking: A top-down approach featuring the internet, 3/E[M]. Pearson Education India, 2005
- [42] 《计算机网络教程[M]》，谢希仁，谢钧，人民邮电出版社, 2002
- [43] Clark D D. Designing an internet[M]. MIT Press, 2018
- [44] 《星地融合移动通信卫星发展趋势》，中国信科，陈山枝，2025.10
- [45] 《“柯伊柏”星座介绍及与其他星座对比分析》，纪凡策，北京空间科技信息研究所，国际太空，2020.12
- [46] 《中华人民共和国无线电频率划分规定》
- [47] 《官方定义的43种无线电业务》 (miit.gov.cn)