卫星互联网发展趋势及网络安全治理研究综述*

白　江，赵高华，贾朔维，王　普
（中国网络空间研究院，北京　100048）

摘　要：卫星互联网技术正从传统通信技术演变为支撑全球战略竞争的关键基础设施和核心技术力量，但同时也面临着“卫星—地面—终端—云平台”全链路的安全威胁，亟需站在国家安全的角度构建更加完善的网络安全治理体系。系统梳理了低轨星座主导、6G 与 AI 融合、手机直连卫星等卫星互联网发展趋势，剖析了多维度安全威胁、网络主权冲击、数据跨境传输及国际规则滞后等风险挑战。通过比较美国国家安全驱动、欧盟数字主权规则、中国兼顾发展和安全及俄英印日等国家的差异化实践，总结卫星互联网网络安全治理的经验做法。面向全球卫星互联网建设的共同挑战，提出构建多边协同的国际规则体系、强化全链条安全与供应链韧性、推动全球卫星互联网基础设施普惠化建设等发展建议。

关键词：卫星互联网；网络安全；卫星互联网安全；手机直连卫星
中图分类号：TP309；G203　　**文献标志码：**A　　DOI：10.19358/j.issn.2097-1788.2026.06.005

中文引用格式：白江，赵高华，贾朔维，等. 卫星互联网发展趋势及网络安全治理研究综述[J]. 网络安全与数据治理，2026，45(6)：31-39.
英文引用格式：Bai Jiang，Zhao Gaohua，Jia Shuowei，et al. A review of development trends and cybersecurity governance of satellite internet[J]. Cyber Security and Data Governance，2026，45(6)：31-39.

A review of development trends and cybersecurity governance of satellite internet

Bai Jiang，Zhao Gaohua，Jia Shuowei，Wang Pu
（Chinese Academy of Cyberspace Studies，Beijing 100048，China）

Abstract：Satellite internet technology is evolving from a communications technology into a critical infrastructure and a core technological force in global strategic competition. However，it faces security threats across the entire chain—from satellites and ground systems to user terminals and cloud platforms. This underscores the urgent need to establish a more comprehensive cybersecurity governance framework from the perspective of national security. This paper systematically reviews major development trends in satellite internet，including the dominance of low Earth orbit（LEO）constellations，the integration of 6G and artificial intelligence（AI），and direct-to-device（D2D）satellite communications. It further analyzes main risks such as multidimensional security threats，impacts on cyber sovereignty，cross-border data transmission risks，and the lag of international regulatory frameworks. Through a comparative study of governance practices in the United States，the European Union，China，Russia，the United Kingdom，India，and Japan，the paper summarizes the major experiences and approaches in satellite internet cybersecurity governance. In response to the shared challenges of global satellite internet development，the paper proposes several policy recommendations，including establishing a multilateral and coordinated international regulatory framework，strengthening full-chain security and supply chain resilience，and promoting inclusive global satellite internet infrastructure development.

Key words：satellite internet；cybersecurity；satellite internet security；direct-to-device satellite communication（D2D）

0　引言

卫星互联网技术正从传统通信技术，演变为支撑全球战略竞争的关键基础设施和核心技术力量。通过大规模低轨（Low Earth Orbit，LEO）卫星组网，卫星互联网不仅为偏远地区和地面网络盲区提供了前所未有的连接可能，更在全球科技竞争、国家安全和数字主权博弈中占据核心位置。美国 Starlink、欧洲 IRIS²（Infrastructure for Resilience，Interconnectivity and Secur-

* 基金项目：国家社科基金重大项目（22&ZD147）

ity by Satellite）计划、中国星网星座等战略级项目的推进，标志着各国已将其视为未来数字基础设施和战略竞争能力的重要组成部分。

然而，卫星互联网的开放架构和全球覆盖特性也使其面临严峻的安全挑战。从信号干扰、链路劫持到网络入侵和物理破坏，安全威胁贯穿“卫星—地面站—终端—云平台”全链路，特别是手机直连卫星的快速发展，给各国网络空间管理带来了新的挑战。这一现实促使各国的治理重心从“如何促进产业发展”转向“如何管控安全风险”。未来，为保障卫星互联网的可持续发展，需要继续构建系统性的治理方案，防范应对日益复杂的网络安全挑战。这不仅是单一技术或市场问题，更是全球网络空间治理的共同命题。

1　卫星互联网发展现状与未来趋势

当前，卫星互联网已经从传统高轨卫星通信阶段，进入以低轨星座为核心的新一轮产业发展周期。美国的“Starlink”、欧洲的“OneWeb”以及中国的“国网星座”“千帆星座”等大型低轨星座计划，正在推动全球通信网络由“地面中心”向“天地一体化”模式演进。与此同时，手机直连卫星、物联网直连卫星成为近年备受关注的新兴方向，卫星互联网也逐步从专用行业市场进入大众消费市场。

（1）卫星互联网全球市场规模迅猛增长。当前，在低轨卫星规模化部署、火箭复用技术成熟以及相控阵天线成本骤降的推动下，全球卫星互联网市场正在迅速增长。根据 Global Market Insights 发布的最新报告，卫星通信市场从 2022 年的 200 亿美元增加至 2025 年的 252 亿美元，并将在 2035 年增加至 830 亿美元，如图 1 所示。另外，根据赛迪智库预测，从全球范围来看，手机直连终端用户数将上升至约 1.3 亿户，物联网潜在终端数量达 106 亿台。随着 Starlink、OneWeb、国网星座等不断部署，以及手机直连卫星等新业态不断成熟，卫星互联网已经从航空航海、应急通信等专业场景全面渗透进入大众消费市场，成为构建天地一体化网络的核心部分。

（2）低轨卫星星座逐渐占据市场主导地位。凭借低传输时延、高通量带宽和可规模化部署的显著优势，低轨卫星星座已成为全球卫星互联网市场的主导力量。目前，低轨星座由一些领先科技企业主导推动。其中，SpaceX 的 Starlink 是目前全球规模最大的低轨卫星互联网项目。根据公开数据统计，截至 2026 年 4 月，Starlink 的在轨卫星数量已经超过 10 300 颗。欧洲通信卫星公司（Eutelsat）的 OneWeb 星座也拥有较大规模的运营能力，第一代星座计划部署 648 颗卫星。根据国信证券报告，美国科技企业亚马逊的 Kuiper 项目目前已发射超 200 颗卫星，并计划部署 3 200 余颗卫星。与此同时，由中国卫星网络集团有限公司（以下简称“中国星网”）负责的国网星座也在快速发展和部署，计划最终部署约 13 000 颗卫星。根据公开信息，由上海垣信（SSST）牵头运营的千帆星座项目也已部署超过 160 颗卫星。

（3）6G+AI+卫星互联网一体融合成为核心技术趋势。在第六代移动通信网络（6G）“全域覆盖、万物智联”的愿景牵引下，卫星互联网、人工智能（AI）与地面移动通信正从独立演进走向一体深度融合，成为下一代信息基础设施的核心技术趋势。6G 网络将空天地一体化作为原生设计，低轨卫星星座不再是地面网络的补充，而是通过星间激光链路、多轨道协同与地面网络深度集成。另外，AI 将作为内生能力深度渗

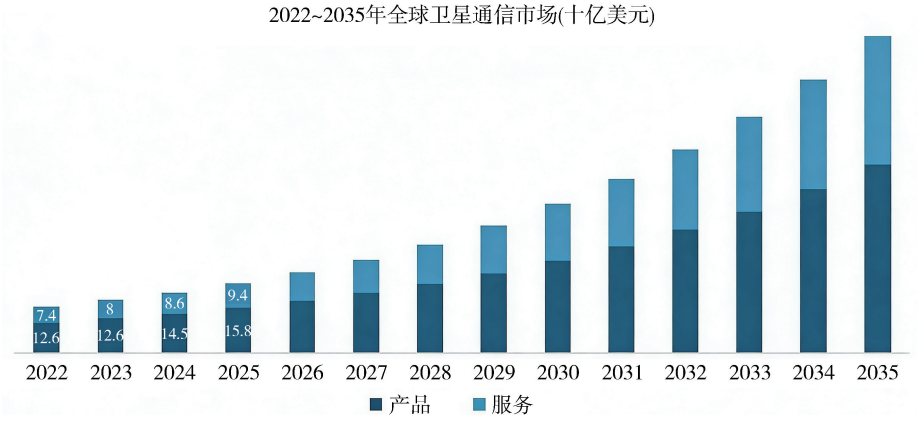

图 1　2022～2035 年全球卫星通信市场

透到空天地一体化信息网络架构的每一层，驱动跨域资源智能调度、星间路由自主优化、干扰协同抑制与网络故障自愈等核心功能。当前，国际电信联盟（ITU）和第三代合作伙伴计划（3rd Generation Partnership Project，3GPP）将“空天地一体化”和“内生 AI”列为 6G 关键场景，全球主要经济体围绕这一融合方向加速技术攻关。

（4）直连卫星终端能力与服务快速增长。随着低轨卫星互联网、5G NTN（Non-Terrestrial Network，非地面网络）以及天地一体化通信网络的快速发展，手机直连卫星已成为全球泛在连接的重要发展方向，未来将融合地面蜂窝通信与卫星通信能力，实现真正意义上的“空天地一体化连接”[1]。而且，随着 5G NTN 标准持续演进，未来手机用户无需更换终端即可直接接入卫星互联网服务，并从“双模接入”向“融合直连”模式逐步演进，实现卫星网络与地面网络的无缝切换[2]。当前，全球主流运营商、卫星企业以及终端厂商均在加速布局卫星直连能力，将进一步推动该技术服务进入大众市场[3]，成为下一代通信产业的重要增长方向[4]。

（5）卫星互联网逐渐从链接服务走向数据与平台。过去，卫星互联网主要聚焦通信覆盖能力，核心价值在于为偏远地区、海洋、航空等场景提供网络接入。但如今遥感数据、位置数据和环境监测数据的商业价值快速提升，特别是农业、气象、能源等领域，市场对“数据服务”和“智能决策”的需求越来越大。未来，卫星网络将不仅提供通信链路连接，还将逐步发展为具备星上处理、边缘计算和通导遥融合能力的智慧空间平台，为物联网、自动驾驶、应急救灾等领域提供算力与感知服务。如即时智能遥感已成为未来卫星互联网的重要方向，星载 AI 能够在轨完成数据识别、目标检测和智能分析，直接向地面提供最终计算结果和服务[5]。

2 卫星互联网潜在网络安全风险与治理挑战

由于“全球覆盖、高度开放、跨境运行、天地融合”的特点，卫星互联网也带来了前所未有的安全风险与治理挑战，并从传统通信安全，扩展至网络安全、数据安全、网络主权以及国际治理等多个层面。

卫星互联网面临多维度攻击威胁。卫星互联网的开放信道、动态拓扑及星地异构等特性使其面临从物理层到用户层的系统性网络安全威胁[6]。卫星互联网技术架构可以分为空间段、地面段和用户段三个主要部分，其安全问题涉及通信链路安全、载荷系统安全、供应链安全等方面。在通信链路安全方面，由于卫星信号覆盖广，不法分子易利用高灵敏度接收设备进行窃听，获取敏感信息，从而威胁用户隐私和通信安全。另外，恶意实体还可以通过地面设备发送高功率干扰信号导致通信中断，或者发送伪造信号欺骗卫星及地面站，诱导系统接收错误信息，导致系统误操作。在载荷系统安全方面，卫星系统本质上是一个计算机系统，卫星互联网中的设备和应用系统也同样存在各种软件漏洞，攻击者可以通过各类漏洞，入侵系统并控制卫星或者基站主机，甚至通过启动自毁程序或耗尽推进剂的方式直接毁灭卫星。另外，如果卫星载荷存储介质中敏感数据没有经过适当的加密和权限管理，可能被非法访问、窃取或篡改。在供应链安全方面，卫星硬件及软件的设计和生产涉及诸多环节，许多国家依赖进口设备建设卫星互联网。这些设备可能包含隐蔽的网络安全风险，一旦关键部件或系统由外国供应商控制，便可能被敌对势力恶意利用，如植入恶意组件，从而导致严重的系统安全和间谍活动风险。

太空基础设施成为新的军事冲突战场。当前，通信卫星、遥感卫星、导航卫星以及商业卫星互联网星座已逐步嵌入现代战争体系，在情报侦察、精确打击、通信保障和战场感知等领域发挥核心作用。特别是低轨卫星互联网凭借星间链路和低时延宽带传输等优势，已成为战场态势感知、精确打击的关键支撑。在俄乌冲突期间，Starlink 被广泛应用于乌克兰军事通信保障、无人机协同和战场信息传输[7]。美国、中国、俄罗斯等主要航天国家均在加强空间军事能力建设。如美国正在推动“弹性太空架构”建设，通过分布式低轨卫星星座提升战时生存能力。与此同时，为对抗彼此的卫星互联网服务能力，围绕太空资产端的“软杀伤”能力也在加速发展，国家行为体纷纷将网络入侵、电子干扰等反卫星网络武器纳入作战体系，并将对手的卫星地面站和天基节点列入打击清单。一旦卫星互联网等关键空间基础设施遭到破坏，将对国家通信、金融、电力以及军事体系造成系统性冲击。

跨境直连卫星影响国家网络空间主权。由于卫星互联网天然具备“跨境覆盖、全球接入、绕过地面网络”等特点，其运行服务对以国界为基础建立的网络空间主权概念带来了新的挑战。网络空间主权的重要基础在于国家对网络基础设施、数据流动以及信息传播的有效管辖[8]。在地面移动通信体系中，移动网络运营商通过基站、核心网和互联网关构建了一个与物理领土高度耦合的网络边界，国家可以通过频谱许可、

设备准入、合法拦截和实名制管理等手段实现有效管辖。但是，卫星互联网的全球覆盖能力削弱了传统地理边界在网络空间治理中的作用，特别是在手机直连卫星场景下，用户终端无需依赖本地运营商，即可直接接入境外卫星互联网。另外，天地一体化网络将导致跨境数据流动更加频繁，部分数据可能在未经本国批准的情况下直接传输至境外平台，从而带来更加复杂的数据主权和国家安全问题[9]。

敏感数据和个人隐私泄露的风险上升。卫星链路天然具有开放广播属性，当用户通过卫星网络传输敏感数据时，更容易受到窃听、链路劫持和恶意攻击。特别是直接接入卫星互联网的消费级终端设备在身份认证、终端安全和数据加密等方面存在不足，可能导致用户位置信息、通信内容以及个人身份数据泄露[10]。例如，在手机直连低轨卫星场景下，用户的身份由移动网络运营商管理，而位置信息也可以被卫星网络运营商访问和存储，该架构导致身份与位置信息被分离在不同运营实体之间[11]。其次，AI、大数据与卫星互联网融合也将加速数据的流动与跨主体处理，从而进一步放大数据安全风险。例如，未来空间信息网络将广泛应用于智能交通、无人系统和智慧城市等场景，卫星系统会持续采集位置轨迹、行为模式和环境感知数据[12]。这些数据经过 AI 聚合分析后，可能推断出用户活动规律、关键基础设施分布，从而形成新的数据泄露及国家安全隐患。

全球治理体系难以应对技术的快速发展。低轨巨型星座、手机直连卫星、星上边缘计算与 AI 融合等前沿技术已从概念逐步走向大规模商用，但从频谱资源分配、跨境数据流动、网络安全保障，到国际法律适用，全球治理体系明显面临“制度滞后”现象。首先，传统太空空间治理规则主要形成于冷战时期，核心对象是少量国家主导的航天活动，而当前商业航天和卫星互联网呈现“高密度、全球化、平台化”特点，导致现有全球治理体系存在失效的挑战[13]。其次，不同国家和企业围绕轨道优先权、频谱资源等方面展开激烈竞争，现有协调机制难以满足产业快速发展需求[14]。再次，现有国际网络治理规则主要面向传统地面互联网，传统通信监管、数据主权以及内容治理机制难以应对手机直连卫星场景的风险冲击[13]。最后，卫星互联网融合了通信网络与空间基础设施双重属性，一旦遭受网络攻击、电子干扰或反卫星打击，可能引发全球通信安全风险。目前，国际社会尚未形成针对卫星互联网网络安全、跨境数据治理、频谱资源共享以及商业卫星军事化使用的国际规则体系[15]。

3 全球主要国家卫星互联网安全治理实践与经验

3.1 美国：以国家安全和政府参与为特点的治理模式

美国是当前全球卫星互联网发展最领先的国家，其治理体系呈现出国家安全驱动、商业资本推动、技术标准主导等特征。

3.1.1 国家安全优先的治理逻辑

美国卫星互联网治理首先服务于国家安全目标，特朗普签署第 14369 号行政令，明确指出“太空优势是衡量国家愿景和意志力的尺度”。特别是近年来，美国战争部、太空军和国家安全局不断强化卫星互联网建设，推动商业卫星星座与军事体系深度融合，提升美国的战略竞争能力。其中，Starlink 不仅是商业互联网项目，更是美国强化全球战略通信优势的重要工具，其军民融合属性非常突出。另外，由于传统大型卫星容易成为反卫星武器攻击目标，美国逐步推动“分布式低轨星座”架构，以提升空间系统抗毁能力，包括持续推进“弹性太空架构（Proliferated Space Architecture）”，即通过大规模部署低轨道卫星星座，利用大量低轨卫星增加抵抗太空攻击的能力，确保自身卫星通信系统的韧性和战略优势。

3.1.2 同步推进网络安全防护与供应链安全审查

美国正在将卫星互联网安全纳入国家网络安全体系，逐步构建覆盖“卫星—地面站—终端—云平台”的全链路安全防护体系[15]，重点防范星间链路攻击、地面站网络入侵、卫星控制链路劫持、GNSS 欺骗和电子干扰、AI 驱动的网络攻击等威胁挑战。另一方面，美国高度重视供应链安全，限制高风险芯片、通信设备进入其卫星互联网体系，并强化卫星制造本土化能力。

卫星互联网安全防护方面，2025 年 12 月，美国议员联合提出《卫星网络安全法案》（Satellite Cybersecurity Act of 2025），并于 2026 年 4 月进入参议院审议阶段。该法案要求商务部协同其他联邦机构，一是为商业卫星系统制定针对性的网络安全建议指南，涵盖基于风险的和网络安全导向的工程设计、网络安全事件发生时恢复或保持对商业卫星系统有效控制的预案等内容。二是建立商业卫星系统网络安全公共信息交换中心，汇集当前能够用于商业卫星系统的网络安全资源，帮助中小企业实现商业卫星系统的安全开发、运营和维护。另外，美国国家标准与技术研究院（NIST）针对商业卫星系统空间段、地面段、用户段及混合卫星网络等对象的网络安全风险，相继发布了

4 个网络安全风险管理指导框架，帮助商业卫星运营服务相关主体识别网络安全风险。

供应链安全方面，2025 年 2 月，美国国会议员推动《太空基础设施法案》（Space Infrastructure Act）立法，推动国土安全部将太空系统、服务和技术认定为“关键基础设施”，让其享有与电网、通信网络和金融系统同等的国家安全保护级别。2025 年 6 月，美国参议院提出《2025 安全太空法案》（Secure Space Act of 2025），并于 2026 年 4 月经参议院商业、科学与交通委员会审议推进。该法案禁止美国联邦通信委员会（FCC）向“被认定为对美国国家安全构成不可接受风险的通信设备或服务”的实体及其关联企业授予卫星执照、美国市场准入或地球站授权。

卫星通信频谱管理方面，Part 25 是 FCC 监管卫星通信频谱的核心规则框架，包括卫星通信频谱分配、许可审批、技术标准和干扰协调等环节。FCC 于 2025 年 10 月启动制度改革，提出将 Part 25 规则体系整体重构为全新的 Part 100，具体包括：一是制定频谱共享框架，通过《卫星宽带频谱共享现代化》的最终规则，用新的基于传输性能的协调框架取代以前等效功率通量密度的协调模式，有效释放频谱资源的潜在容量；二是大规模释放新的频谱资源，FCC 正在评估释放超过 20 000 MHz 的频段资源，以支持低轨卫星和下一代卫星宽带服务的发展；三是探索手机直连卫星频谱监管，包括允许卫星运营商在获得移动网络运营商授权的前提下共享特定的频谱频段、保证利用专用移动卫星服务（MSS）频谱的专有使用权。

3.2 欧盟：以数字主权和规则治理为核心的治理模式

欧盟卫星互联网治理模式更加重视“数字主权”和“规则治理”，其核心目标是减少对美国商业卫星体系的依赖，建立欧洲自主可控的空间数字基础设施，并以法律规则提升网络安全保障能力。

3.2.1 IRIS² 计划与欧洲数字主权

近年来，欧盟推动 IRIS² 低轨卫星互联网计划，旨在建立欧洲自主卫星通信体系。该计划定位于“公共服务+关键行业保障”双重体系，打造支持欧盟战略自主、韧性和竞争力的战略资产。该计划准备部署一个由约 290 颗低轨及中轨（MEO）卫星组成的多轨道星座，为欧盟及其成员国提供安全、自主、韧性的卫星通信服务。在欧盟的战略叙事中，IRIS² 早已超出一项通信工程的技术范畴，而是被定位为欧洲数字主权的核心基础设施，承载着降低对外依赖、保障关键通信安全、巩固战略自主的多重使命。特别是面对 SpaceX Starlink 星座的垄断地位，欧盟决策层面存在“非欧盟实体控制欧洲关键通信链路”的巨大担忧。这种担忧不仅限于商业竞争，更涉及国家安全。为此，欧盟加快推进 IRIS² 的建设，在系统定位上希望为欧洲政府机构和关键行业企业提供安全、低延迟、韧性的卫星通信服务。在技术和产业层面希望减少欧盟境外地面站的依赖。

3.2.2 以太空安全立法提升网络安全与韧性水平

一方面，由于欧盟各成员国在卫星设计、网络安全风险管理和环境约束方面存在规则不统一情况，给卫星互联网跨境运营与管理造成了较大的障碍。另一方面，欧盟日益意识到本土卫星产业对其连通性、防御和主权目标至关重要。欧盟 2025 年 6 月 25 日公布《欧盟太空法案》提案，旨在为全欧盟提供统一的太空活动监管框架，降低跨境运营的合规成本和市场准入障碍，希望解决太空网络建设资金投入不足、市场碎片化和对外依赖等问题。

《欧盟太空法案》构建了覆盖太空活动全生命周期的统一授权和监管框架。在适用主体上，法案适用于在欧盟境内提供太空服务的所有运营商，包括满足“充分关联”条件的非欧盟实体，即在欧盟境内提供卫星互联网数据或服务的第三国运营商。该做法直接借鉴了欧盟《通用数据保护条例》（GDPR）的“长臂管辖”逻辑，试图以市场准入的手段，将欧盟的安全标准外溢至全球其他国家。在监管授权方面，该法案创设了“欧盟空间授权”制度，即空间运营商须在“联盟空间活动存储库”注册并获得认证后方可在欧盟境内提供相关服务。

网络安全要求是该法案最核心的内容。2023 年 1 月生效的欧盟《网络和信息安全指令》（Network and Information Security Directive，NIS2）已将空间行业纳入监管范围，强化了对地面基础设施的韧性要求，但未能覆盖太空基础设施的全部环节。《欧盟太空法案》衔接 NIS2 指令，将相关网络安全要求延伸至太空网络，要求运营商从卫星设计、制造、发射、运营和退役等全生命周期实施持续的风险管理。一是卫星端的安全测试。运营商必须在首次发射前（对于星座，在首批次发射前）完成实施“威胁导向的渗透测试”，此后至少每三年重复一次。二是数据加密与身份认证要求。运营商应定义加密方案，实施加密策略，并确保控制中心与卫星终端设备之间的端到端身份认证，对远程指令实施基于风险的加密保护措施。三是供应链风险管理。运营商须在合同中规定安全要求，建立

关键非欧盟来源资产的清单，以确保对技术控制链条的有效掌握。四是安全事件报告与运营维护。运营商必须在 12~72 小时内完成重大安全事件的上报，并建立网络安全事件实时检测和响应能力。

3.3 中国：以顶层设计和体系化安全为核心的治理模式

3.3.1 强调顶层设计和协同推动

2026 年中国《政府工作报告》提出“加快发展卫星互联网”，“十五五”规划纲要进一步将其纳入国家重大工程项目体系，统筹推进卫星、导航、遥感三大系统协同建设，构建一个由我国主导、安全可控的天地一体化信息基础设施体系。针对低轨巨型星座的建设任务，中国采用国家队主导和民营企业相结合的双轨并行模式。其中，中国星网主导推进首个空天一体 6G 互联网计划——国网星座建设，并计划发射近 1.3 万颗卫星。民营企业上海垣信正在建设运营中国第二大卫星星座——千帆星座，计划到 2030 年底完成超过 1 万颗低轨宽带卫星的部署，以提供全球卫星互联网服务。

3.3.2 体系化构建卫星互联网安全保障要求

《终端设备直连卫星服务管理规定》是中国首部专门针对手机直连卫星等新兴服务的法规文件。该规定由国家网信办等七部门联合发布，自 2025 年 6 月 1 日起施行。在准入许可和安全监管方面，该规定构建了严格的合规框架和底线要求。例如相关主体提供直连卫星服务，必须依法取得电信业务、无线电频率使用等许可；仅可连接在我国境内合法运营的卫星互联网服务。在网络和数据安全方面，该规定要求卫星互联网服务提供者等相关主体落实现有网络安全的法律法规要求。例如，服务提供者须严格遵守《网络安全法》《数据安全法》《个人信息保护法》，落实网络安全等级保护和通信网络安全防护制度，对所处理的数据实行分类分级保护，并采取必要措施保障个人信息安全等。

另外，2025 年 8 月，工信部印发《关于优化业务准入促进卫星通信产业发展的指导意见》，要求企业依法履行主体责任，在系统设计、建设、运行中需同步落实网络安全防护、数据分类分级保护、关键信息基础设施保护等相关要求，并加强用户实名制管理。国家标准《空间数据与信息传输系统网络安全总体技术要求》于 2025 年 3 月对外征求意见，该标准构建了覆盖空间数据和信息系统全链条的网络安全防护体系，并从通用安全、通信安全、节点安全、安全运维四个方面定义空间数据和信息系统的安全技术要求。

3.3.3 推动卫星互联网国际治理与合作

中国近年来不断将“网络空间命运共同体”理念扩展至空间互联网与天地一体化网络治理领域，强调网络空间应共同遵循和平、安全、开放、合作的原则，特别是反对少数国家或大型商业企业垄断频谱资源和国际技术标准。在卫星频谱协调方面，中国积极参与 ITU 相关规则制定。其中，《无线电规则》（Radio Regulations）是 ITU 框架下具有普遍法律约束力的国际条约，它规范了全球无线电频谱的使用。在该框架下，中国已经与俄罗斯、韩国、越南等举行多轮高级别卫星网络协调会谈，就无线电频率兼容共用达成共识，为全球各国建设卫星星座解决频谱协调问题。另外，中国正通过商业合作与技术赋能，积极将自主低轨卫星互联网服务扩展至全球，为全球其他国家提供便捷、可靠的卫星互联网接入。例如，上海垣信的卫星互联网系统已在哈萨克斯坦完成测试，能够为乡村学校、医疗机构等关键基础设施提供高质量通信服务，并计划于 2026 年正式启动运营。

3.4 其他国家：多元化路径和差异化实践

3.4.1 俄罗斯呈现以本地化强监管的防御性模式

俄罗斯的卫星互联网治理实践呈现出鲜明的以“主权防御”和“本地化强监管”为核心的特征。面对 Starlink 等外国低轨星座在未经授权情况下进入俄边境地区的潜在风险，俄罗斯数字发展部发布的《外国低轨卫星通信监管条例》自 2026 年 3 月 1 日起生效。该条例的核心要求包括：一是频率许可，外国低轨星座须事先取得频谱分配许可；二是地面落地，必须在俄境内建设地面接口站，所有用户流量强制走“手机—卫星—接口站”路径，禁止未经批准的直连卫星模式；三是监控接入，接口站内须安装俄联邦安全局认证的 SORM（作战搜索措施系统）和 TSPU（技术威胁应对系统），实现对信令、话务和数据的实时镜像与回溯。

3.4.2 英国推动直连卫星服务授权监管和频谱管理

英国在卫星互联网安全治理领域，选择了以频谱授权监管为核心的实践路径。2026 年 2 月，《无线电（直连设备卫星通信）（豁免）条例 2026》正式生效，首次授权在已经许可的移动频谱频段内，手机和 SIM 卡设备可以直接连接卫星。该条例在频谱管理方面重点确定两方面要求：一是手持终端的许可豁免，免除其获得无线电许可的要求；二是建立移动网络运营商（MNO）的牌照变更机制——MNO 须向英国通信管理局申请变更其现有无线电牌照后方可提供手机直连卫

星服务。这使英国通信管理局获得了更加精细的频谱控制权。虽然英国通信管理局并未为卫星服务分配新的频谱，但它允许 MNO 将其已获许可的 34 GHz 以下频段扩展到轨道频率，使得相同的频率能够同时服务于地面网络和卫星网络，扩大现有移动频谱资源的利用效率。

3.4.3 印度建立首个政府主导的空间网络安全框架

2026 年 2 月，印度计算机应急响应小组（CERT-In）与印度航天协会（SIA-India）联合发布了空间网络安全框架和指南，旨在保护空间通信资产并增强印度空间生态系统的韧性。这是在印度卫星互联网政策出台、卫星通信市场向私营部门开放之后，首次由政府主导出台的面向空间领域的系统性网络安全框架。该框架涵盖政府机构、卫星服务提供商、地面站运营商、设备供应商和私营航天企业等利益相关方，明确阐述了空间网络安全的基本原则、推荐控制措施和责任分配。此外，框架还要求卫星运营商执行年度审计，并遵守数据本地化、合法拦截和通过本地网关路由流量等安全规定。

3.4.4 日本强化卫星通信网络战略地位和安全防护

日本的卫星互联网安全治理体现出军事安全导向的显著特征，且将安全防护机制逐步融入新兴空间活动的法律框架之中。2025 年 7 月，日本防卫省发布《太空防卫战略纲要》（Space Defense Guidelines），认为太空利用在通信和地面观测方面是国民生活不可或缺的基础，提出要确保卫星通信、构筑卫星安全防护能力。该纲要提出构筑能够承受通信干扰的卫星通信网络，推进盟友间的卫星通信相互运用，以及从物理和网络共同强化卫星安全防护能力。同时，日本计划优先资助先进信号处理和频率跳变系统等干扰技术的开发，提升国家卫星通信基础设施的韧性。

3.5 特点分析

综合美国、欧盟、中国以及俄罗斯、英国、印度、日本等国家和地区的治理实践可以看出，当前全球卫星互联网治理已经从早期的通信业务管理逐渐演变为涵盖国家安全、网络主权、网络安全、产业竞争以及国际规则博弈的综合治理体系。

3.5.1 国家安全与战略安全已成为核心目标

当前，各国普遍将卫星互联网视为国家关键基础设施，其治理逻辑已从传统商业通信监管转向国家安全考虑。其中美国最具代表性，将低轨卫星互联网直接纳入国防通信、联合作战、太空态势感知等战略内容。日本强调“太空防卫”，俄罗斯强调“主权防御”，欧盟强调“战略自主”，本质上都体现出卫星互联网已成为国家安全能力的重要组成部分。未来，国家安全导向将持续深刻影响全球卫星互联网的发展和应用，商业卫星互联网可能越来越多地承担军事功能，与军事通信体系之间的边界将越来越模糊。因此，围绕频谱资源、空间网络控制权、国际技术标准等领域的卫星互联网竞争将更加激烈，并将持续是全球科技竞争和地缘政治博弈的前沿。

3.5.2 卫星互联网安全与韧性是各国关切的重点

随着卫星互联网与云计算、AI、6G 等技术深度融合，其网络安全风险也快速上升。各国越来越关注卫星控制链路劫持、地面站入侵、星间链接共建、跨境接入等安全威胁及其解决方案。如，美国强调全过程风险管理，NIST 建立卫星网络安全框架；欧盟则强调对卫星从设计、制造、发射到退役全过程进行监管，并强制要求开展卫星系统的渗透测试。未来，卫星互联网的安全防护将不再局限于单个卫星，而是面向整个星座体系的整体防御，在国家层面逐渐形成类似国家关键基础设施保护的安全模式。而且，各国将更加关注“遭受攻击后能否持续运行”的卫星互联网韧性能力，重点推动分布式星座、智能流量切换、弹性路由等关键技术突破和应用。

3.5.3 供应链安全和自主可控将进一步强化

随着卫星互联网逐渐演变为覆盖全球的信息基础设施，各国将更加重视该领域“网络主权”“数字主权”和“技术主权”，并推动建立自主可控的产业链和供应链体系，以避免核心基础设施受制于外部技术和商业平台。如美国通过《安全太空法案》《太空基础设施法案》等政策工具，限制高风险外国设备、芯片和通信系统进入其卫星互联网体系。《欧盟太空法案》还要求运营商建立关键非欧盟来源资产清单，加强供应链风险管理，防止外部技术依赖带来的系统性安全风险。从发展趋势来看，未来全球卫星互联网产业链可能不再是完全开放的全球化体系，而是逐渐形成美国、欧洲、中国等各自主导的产业生态，围绕芯片、操作系统、通信协议等核心领域的“技术脱钩”和“规则分化”趋势也可能进一步加剧。

3.5.4 各国对频谱资源的竞争与利用创新日益加剧

不同于传统地面通信网络，卫星互联网需要同时协调无线电频率资源以及跨境覆盖问题，而低轨巨型星座的快速扩张进一步加剧了全球频谱资源竞争。当前，美国、中国、欧盟、英国等国家和地区都在积极推动频谱制度改革和利用模式创新，围绕频谱分配、

共享机制、动态协调、手机直连卫星以及星地融合等领域展开新一轮竞争。其中，美国推动传统地面移动频谱与卫星频谱融合使用，并建立基于“性能导向”的动态频谱协调机制。欧盟高度重视对关键频谱资源的自主控制，并试图通过统一规则减少成员国之间的协调障碍。未来，随着 AI 技术的发展，通过 AI 算法动态识别频谱空闲状态，将实现不同卫星系统之间的智能避让，结合认知无线电等频谱技术，卫星频谱利用将逐渐从“固定频谱模式”向“智能频谱模式”演进。

3.5.5 国际规则与全球治理体系建设将加速推进

当前，全球卫星互联网治理体系仍处于“规则快速形成但尚未成熟”的阶段。一方面，ITU 等传统国际组织仍然是频谱协调和空间活动规则制定的重要平台；另一方面，随着 Starlink、Kuiper、国网星座、千帆星座等大型低轨星座快速部署，现有国际规则体系已经面临越来越大的治理压力，轨道资源占用、频率干扰、跨境数据流动以及商业卫星军事化等问题日益突出。未来，国际规则与全球治理体系建设将从“技术协调”走向“战略治理”，并逐步扩展至网络安全、商业卫星军事化、安全责任等更加复杂的战略议题。

4 推动全球卫星互联网共同发展的建议

面对卫星互联网快速发展带来的网络安全、网络主权以及国际治理风险，未来全球治理需要在“安全、发展、合作”之间建立更加平衡的治理体系。

4.1 建立多边协同的国际治理机制，完善全球规则体系

当前全球卫星互联网治理仍存在规则碎片化、国际协调不足以及治理主体失衡等问题。特别是在频谱资源、跨境数据流动以及商业卫星军事化等领域，现有国际规则已经难以适应低轨巨型星座快速发展的现实需求。因此，需要进一步强化联合国、ITU 等多边机制作用，加快建立覆盖“空间—网络—数据”一体化的国际治理框架。一是推动完善国际频谱资源协调机制。针对部分大型商业星座快速占用频率资源的问题，研究建立更加公平、透明和动态的资源分配规则，避免形成“先占先得”的资源垄断格局。同时，推动建立低轨卫星频谱共享机制，提高全球有限频谱资源的利用效率。二是推动形成卫星互联网安全国际规则。围绕商业卫星军事使用、网络攻击、卫星干扰、反卫星网络武器使用等敏感问题，加强国际行为规范建设，明确商业卫星的责任边界和安全义务，避免商业系统过度卷入地缘政治和军事对抗。

4.2 强化网络安全与供应链安全体系建设，提升系统韧性能力

卫星互联网的安全风险已经从传统通信安全扩展至供应链安全以及人工智能驱动的新型攻击风险。未来应重点构建覆盖“卫星—链路—地面站—终端—云平台”的全链条安全防护体系。一是加强卫星互联网网络安全能力建设。针对星间链路攻击、GNSS 欺骗、电磁干扰以及地面站入侵等风险，推动建立统一的安全技术标准和风险评估机制，加强卫星身份认证、端到端加密、星间链路保护等关键技术研发和能力建设。二是强化供应链安全与自主可控能力。卫星互联网关键环节高度依赖芯片、操作系统、通信协议和云平台等核心技术，需要推动星载芯片、卫星操作系统自主研发，核心通信设备本土化等建设，降低对单一外部供应链的依赖。三是提升卫星互联网系统韧性能力。推动构建“分布式、冗余化、弹性化”的低轨卫星架构，通过多轨道协同、动态重构和快速恢复机制提升系统抗毁能力。同时，应建立覆盖空间段与地面段的安全实时监测和应急响应体系，提升对网络攻击、极端事件的快速恢复能力。

4.3 坚持发展和普惠原则，加强国际合作与能力共享

未来全球卫星互联网治理不仅要关注安全风险防控，也应更加重视数字包容和能力建设，推动卫星互联网成为促进全球共同发展的公共数字基础设施。一是推动全球卫星互联网基础设施普惠化建设。国际社会应通过国际合作、融资支持、联合建设等方式，帮助欠发达地区提升卫星互联网接入能力。例如，可通过国际开发银行、多边合作基金为偏远地区建设地面站、配套通信设施，降低卫星互联网接入成本。二是推动形成开放共享的国际技术合作体系。目前全球卫星互联网技术、核心标准和关键设备仍主要掌握在少数国家和企业手中，容易形成新的“数字技术壁垒”。未来应鼓励国际社会加强在卫星通信、网络安全、频谱共享、卫星终端等领域的开放共享，推动技术共享和标准互认。三是推动卫星互联网在公共服务领域的全球应用。未来卫星互联网不仅能够提升全球通信能力，还可广泛应用于远程教育、灾害应急、海洋通信、农业监测等公共服务领域。特别是在自然灾害、战争冲突和基础设施受损情况下，卫星互联网往往能够成为恢复通信和保障公共服务的重要手段。因此，国际社会应推动建立全球公共服务合作机制，提高卫星互联网在全球公共治理中的应用能力。

5 结论

卫星互联网的发展已进入“安全定义边界、治

理决定未来”的新阶段。频轨资源争夺、供应链武器化、商业星座军事化等趋势表明，技术演进与地缘博弈已经深度交织。各国在治理路径上虽有分歧，但在安全优先、全生命周期管控、强化网络主权管辖等核心议题上，正呈现出高度趋同的态势。应对这一全局性挑战，仅靠单边立法或碎片化协调已难以为继，亟需在多边框架下构建安全与发展的再平衡机制，既要守住网络安全与供应链自主的底线，也要防止“技术脱钩”与“规则阵营化”侵蚀全球数字公平。唯有通过国际社会的共同努力，将卫星互联网从竞争工具转化为合作平台，才能真正实现弥合数字鸿沟、增进人类共同福祉。

参考文献

[1] 何元智,肖永伟,张世杰,等. 全球泛在连接新模式:手机直连卫星关键技术及挑战[J]. 电子与信息学报,2024,46(5):1591-1603.
[2] 李思栋,李侠宇,孙建成,等. 手机直连卫星应用发展与挑战[J]. 电信科学,2024,40(4):43-55.
[3] 宋艳军,肖永伟,孙晨华. 手机直连卫星关键技术分析与发展展望[J]. 电信科学,2024,40(4):1-9.
[4] 沈学民,承楠,周海波,等. 空天地一体化网络技术:探索与展望[J]. 物联网学报,2020,4(3):3-19.
[5] 孙莉,仇翔,孙军帅. 空天地一体化卫星互联网及其即时智能遥感应用展望[J]. 电讯技术,2025,65(7):1179-1186.
[6] Wang Buhong, Xiao Jin, Dong Ruochen, et al. A comprehensive literature review of cybersecurity in satellite networks[J]. Aerospace,2026,13(3):249.
[7] 徐悦,陈奇东,郭艺,等. 卫星导航系统安全威胁与防御策略概述[J]. 全球定位系统,2025,50(5):89-96.
[8] 张新宝,许可. 网络空间主权的治理模式及其制度构建[J]. 中国社会科学,2016(8):139-158.
[9] 赵洁洁,王海泉. 天地一体化算网融合数据安全风险及防范机制[J]. 网络空间安全科学学报,2024,2(4):36-52.
[10] 谷欣,单超,孙才俊,等. 卫星互联网安全风险及应对措施分析[J]. 天地一体化信息网络,2024,5(1):95-101.
[11] Shi Quan, Wang Liying, Gope P, et al. LPG: raise your location privacy game in direct-to-cell LEO satellite networks[J]. Cryptology ePrint Archive,2025.
[12] 王超,安建平,邢成文,等. 面向空间信息网络的隐蔽通信技术综述[J]. 中国科学:信息科学,2024,54(6):1319-1349.
[13] 王贵国. 网络空间国际治理的规则及适用[J]. 中国法律评论,2015(2):15-29.
[14] 龚自正,陈川,张晶亮. 外空安全与环境治理:进展,挑战与机遇[J]. 空间科学与试验学报,2024,1(1):120-131.
[15] 张元玉,赵双睿,何吉,等. 卫星互联网安全:需求,现状与趋势[J]. 网络空间安全科学学报,2024,2(4):2-17.

（收稿日期：2026-05-20）

作者简介：

白江（1980-），男，硕士，工程师，主要研究方向：网络安全、数据安全、卫星互联网治理。

赵高华（1990-），女，硕士，副研究员，主要研究方向：网络安全和数据安全。

王普（1992-），通信作者，男，博士，助理研究员，主要研究方向：网络安全、数据安全、卫星互联网安全等。E-mail：wangpu@cac.gov.cn。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部