2024 年卫星互联网安全年报：驾驭一个充满竞争和不断演变的领域

I. 执行摘要

2024 年，卫星互联网安全领域经历了复杂性的急剧升级，其主要特征表现为持续的国家级网络威胁、低地球轨道（LEO）星座的迅速扩张所带来的新型漏洞，以及各方为加强监管框架和发展先进防御技术所付出的协同努力。卫星互联网固有的军民两用特性，进一步巩固了其作为关键基础设施和地缘政治博弈中首要目标的地位。

综合分析显示，2024 年卫星互联网安全的核心态势包括：国家背景的行为者持续发起针对卫星系统的高级网络威胁，旨在获取情报、实施干扰并谋求战略优势 [1]。LEO 星座及其地面基础设施的激增，显著扩大了攻击面，并暴露出新的安全薄弱环节 [3]。年内发生了多起值得关注的安全事件，包括大范围的 GPS 干扰/欺骗以及针对商业卫星服务的定向攻击 [2]。与此同时，防御策略也取得了显著进展，例如人工智能驱动的威胁检测技术和后量子密码标准的制定 [6]。各国政府和国际组织亦加强了建立安全标准和法规的努力，例如美国的《卫星网络安全法案》和欧盟的 NIS2 指令 [9]。

这些发展态势表明，卫星互联网的安全已不再是小众议题，而是关乎国家安全、经济稳定和全球通信韧性的基础组成部分。因此，采取主动、协作和适应性的安全防护姿态，对于应对当前及未来的挑战至关重要。

II. 2024 年不断演变的威胁态势

A. 主流网络威胁概述

2024 年的整体网络安全环境依然严峻，高级持续性威胁（APT）攻击、勒索软件活动以及漏洞利用事件频发，为卫星互联网面临的特定威胁构成了复杂背景 [1]。由盛邦安全等机构联合发布的《2024 卫星互联网安全年度报告》明确指出，卫星互联网的安全防御是一个涉及通信链路、卫星设备、网络架构及地面终端等多个层面的复杂系统工程 [6]。

在此背景下，针对卫星互联网的特定威胁在 2024 年表现尤为突出：

- **干扰与欺骗攻击**：这类攻击持续且广泛存在，特别是针对全球定位系统（GPS）信号的干扰和欺骗，严重影响了导航精度和通信完整性。俄罗斯在此类活动中表现得尤为活跃和广泛 [2]。欧洲网络与信息安全局（ENISA）在其报告中也将干扰列为主要威胁之一 [10]。
- **非法节点接入与“伪卫星”攻击**：攻击者通过利用卫星网络的身份认证漏洞，或模拟合法卫星信号，实现对卫星网络的非法接入。这种攻击方式不仅破坏了网络的可信度

和安全性[3]，还可能形成“伪卫星”，类似于移动通信领域的伪基站，用于截获、监控或篡改通信数据。例如，铱星系统目前采用的类 GSM 单向认证协议，使其面临严峻的“伪卫星”攻击风险[3]。

- **链路与路由攻击**：这些攻击主要针对卫星与地面站之间的通信路径，或卫星网络内部的路由机制，旨在中断通信或重定向数据流[3]。
- **计算机网络利用（CNE）**：攻击者试图通过网络渗透手段，获取对卫星系统或地面控制网络的未授权访问权限，以进行间谍活动或实施破坏[10]。
- **劫持攻击**：指攻击者非法夺取卫星有效载荷或整个卫星平台的控制权，是极具破坏性的威胁类型[4]。
- **拒绝服务（DoS）攻击**：此类攻击旨在通过消耗目标资源，使卫星服务不可用，其攻击目标可涵盖地面设施或在轨卫星段[4]。

B. 卫星系统及基础设施的脆弱性

卫星系统及其基础设施的固有脆弱性是威胁得以滋生的土壤。2024 年的研究与事件揭示了以下关键薄弱环节：

- **卫星调制解调器（Modem）的漏洞**：由 Yu 等人发表在 CCS '24 会议的论文《卫星调制解调器安全漏洞与攻击的综合分析》中，通过对商用卫星调制解调器的拆解分析，揭示了分布在卫星通信接口（SCI）、地面网络接口（GNI）和硬件（HW）三个攻击面的 16 个安全漏洞，并演示了 18 种新型攻击方法[13]。这些漏洞包括时间与位置同步机制的脆弱性、身份认证薄弱、默认配置下流量未加密、加密算法本身存在缺陷、缺乏对命令的有效验证以及操作系统内核存在已知漏洞等[13]。调制解调器作为关键的接口设备，其安全性直接关系到整个系统的安危。
- **未加密流量的普遍存在**：尽管许多卫星系统具备加密能力，但在默认配置下，敏感数据往往以未加密方式传输，这使得数据极易在传输过程中被截获和窃听[13]。
- **身份认证机制的薄弱环节**：卫星与地面用户身份验证机制中存在的缺陷，为攻击者冒充合法用户或设备、进行未授权访问提供了可乘之机[3]。
- **地面段基础设施的脆弱性**：地面站和控制系统作为卫星网络的神经中枢，依然是攻击者青睐的目标。这些系统往往依赖传统的 IT 基础设施，因此也继承了传统 IT 系统易受已知漏洞利用的风险[6]。
- **软件定义卫星与商用现货（COTS）组件的引入**：软件定义架构和 COTS 组件的日益广泛应用，在为卫星系统带来灵活性的同时，如果未能得到妥善的安全加固，也可能引入新的安全漏洞和风险[10]。

C. 主要威胁行为者及其动机

识别威胁行为者及其动机对于理解和预测攻击趋势至关重要。2024 年，以下几类行为者

在卫星互联网安全领域表现活跃：

- **国家背景行为者**：中国、俄罗斯、伊朗和朝鲜等国家被频繁指出针对航空航天、国防和关键基础设施（包括卫星系统）实施了复杂的网络行动。其动机主要包括情报搜集、获取军事优势以及实施干扰破坏 [1]。CSIS 在其《2025 年空间威胁评估》报告中详细描述了对俄罗斯和中国反太空能力及网络行动的具体关切 [2]。
- **网络犯罪团伙和雇佣黑客组织**：这类行为者主要受经济利益驱动，可能通过对商业卫星运营商或其客户发起勒索软件攻击或窃取敏感数据来牟利 [1]。
- **私营部门攻击性行为者（PSOA）**：指那些开发并销售网络攻击工具和服务的实体，其产品可能被各类行为者获取并用于恶意目的 [10]。
- **黑客行动主义者（Hacktivists）**：出于意识形态动机的团体，旨在通过攻击行动干扰服务或表达政治诉求 [10]。

卫星互联网面临的攻击手段日益多样化，不再局限于针对空间段的专业攻击，而是越来越多地融合了针对其地面系统和用户终端的常见网络威胁，如恶意软件、网络钓鱼和网络入侵。这种攻击向量的融合，一方面是因为卫星地面基础设施常采用标准 IT 组件和操作系统 [13]，使其易受传统网络攻击；另一方面，用户终端本身也如同其他物联网或计算设备一样，可能成为攻击的切入点 [5]。因此，卫星互联网的攻击面已从单纯的空间段扩展至整个端到端系统，使得传统 IT 安全挑战与独特的空间环境风险交织在一起，这对防御策略提出了更为全面的要求。

尽管拥有最尖端工具的仍是国家级行为者，但商业调制解调器中漏洞的暴露 [13]，以及利用相对简单设备即可尝试“伪卫星”攻击的可能性 [3]，暗示着能力稍逊的行为者也可能对卫星网络构成日益增长的威胁，尤其是在干扰和局部破坏方面。商用现货组件在卫星系统中的应用 [10]，相较于高度定制化的保密系统，可能在一定程度上降低了逆向工程或漏洞发现的门槛。这意味着，即使是简单的破坏性攻击，如拒绝服务、局部干扰或利用已知的调制解调器缺陷，也可能变得更加普遍。

安全与信任之间存在着密不可分的联系。身份认证机制的薄弱 [3] 以及因未加密传输导致数据被截获的风险 [13]，直接削弱了用户和政府对卫星服务的信任度。正如非法节点接入被明确指出“大大削弱了卫星互联网的可信性和安全性” [3]。对于政府、军事、金融等关键应用而言，数据完整性和保密性的保障是其信赖服务的前提。信任的缺失不仅会阻碍卫星互联网在关键领域的应用推广，还会进一步催生各国加强对本国卫星基础设施控制权的需求，以确保信息安全和国家主权。

表 1: 2024 年卫星互联网主要安全威胁总结

威胁类型	描述	主要目标/影响	关键参考资料
干扰与欺骗 (Jamming & Spoofing)	故意发送干扰信号以中断正常通信，或发送虚假信号误导接收设备，如 GPS 欺骗。	通信中断、导航失效、数据完整性受损；影响军事、民航、关键基础设施等。	2
非法节点接入/“伪卫星”攻击	利用认证漏洞或模拟合法卫星信号接入网络，或设立虚假基站截获/篡改通信。	网络信任度下降、数据泄露、服务中断、网络被用于恶意活动跳板；铱星系统特定风险。	3
链路与路由攻击	针对卫星与地面站之间或卫星网络内部的通信链路和数据路由协议发起的攻击。	通信中断、数据包丢失或被窃听、网络拓扑被恶意修改。	3
计算机网络利用 (CNE)	通过网络渗透手段，获取对卫星系统、地面控制网络或相关 IT 基础设施的未授权访问。	情报窃取、系统控制权丧失、恶意软件植入、关键数据篡改或删除。	10
劫持 (Hijacking)	非法夺取对卫星有效载荷（如传感器、转发器）或整个卫星平台的控制权。	卫星功能丧失或被滥用、服务中断、可能造成物理损坏或轨道偏离。	4
拒绝服务 (DoS/DDoS)	通过大量无效请求或恶意流量淹没目标系统（卫星、地面站、网络链路），使其无法提供正常服务。	服务中断、业务瘫痪、经济损失。	4
调制解调器漏洞利用	针对卫星用户终端	用户数据泄露、终端	13

	（调制解调器）的硬件、固件或软件漏洞进行攻击，如利用弱认证、未加密流量、命令注入等。	被控、网络接入被滥用、服务中断。	

III. 2024 年重大安全事件与活动

A. 记录在案的针对空间领域的攻击

根据 CSIS《2025 年空间威胁评估》中引用的欧洲网络事件知识库（ERCI）数据，2024 年约有**五起攻击事件明确针对空间领域**[2]。这一数字与 2023 年大致相当，表明针对空间领域的直接攻击持续存在，尽管报告数量上未显示急剧增长。CSIS 的报告同时指出，准确追踪此类攻击的年度数量和攻击动机仍然是一项挑战[2]。

B. 与卫星网络相关的重大事件及活动分析

2024 年，多个国家背景的行为者被指与针对卫星网络及其相关基础设施的活动有关，凸显了地缘政治因素对卫星互联网安全的深刻影响。

- **俄罗斯相关活动：**
  - **针对星链（Starlink）的持续行动：**据报道，在 2022 年至 2024 年间，俄罗斯国家支持的黑客持续尝试突破星链系统的安全性，利用硬件和软件漏洞以获取情报并干扰通信。其采用的策略包括 GPS 欺骗、信号干扰、网络间谍活动（如 Sandworm 组织参与）以及针对星链终端和指挥控制（C2）基础设施部署恶意软件（如 Amadey、Tavdig）[5]。这些攻击旨在拦截通信、扰乱乌克兰军事行动并绘制星链网络架构图[5]。
  - **大范围 GPS 干扰与欺骗：**俄罗斯在从波罗的海到黑海的广大区域内广泛干扰 GPS 信号，该活动在 2024 年中期显著加剧。部分分析认为，这在一定程度上是对乌克兰使用 GPS 制导武器攻击俄境内目标的回应[2]。
  - **反卫星武器引发关切：**2024 年 5 月，美国指责俄罗斯发射了一枚被认为是反卫星武器的“宇宙-2576”（Cosmos 2576）卫星，该卫星随后进入一颗美国政府卫星的共面轨道[2]。此外，俄罗斯其他军事卫星（如宇宙-2558、2581、2582、2583）持续进行的在轨机动也展示了其先进的太空能力[2]。
- **中国相关活动：**
  - 尽管公开信息中较少有直接针对空间系统的具体网络攻击案例，但中国持续进行着积极的网络活动。其在轨卫星展现出先进的机动能力，并且发射能力不断增强，这些都被视为其太空战能力建设的一部分[2]。
  - 值得注意的是，“咸 Typhoon”（Salt Typhoon）网络攻击活动虽然主要目标是电

信巨头（如 AT&T、Verizon）和美国财政部，但其展现了中国国家背景行为者针对关键基础设施的复杂攻击能力，这对于卫星网络安全具有高度的警示意义[14]。该攻击利用已知漏洞的事实也突显了补丁管理的重要性[14]。

- **伊朗相关活动：**
  - “桃色沙尘暴”（Peach Sandstorm）网络攻击活动被认为由伊朗伊斯兰革命卫队（IRGC）指导，目标针对航空航天、卫星和通信等行业，以进行情报收集和社会工程攻击[2]。Mandiant 在 2024 年 2 月报告称，与伊朗伊斯兰革命卫队有关联的间谍活动针对中东地区（可能还包括土耳其、印度和阿尔巴尼亚）的航空航天和国防部门[2]。
- **朝鲜相关活动：**
  - 2024 年 7 月，美国联邦调查局（FBI）发布联合预警，指出朝鲜的网络间谍活动针对全球范围内的国防、航空航天和核工程实体，旨在提升其军事和核能力[2]。Mandiant 在 2024 年 6 月识别出一个与朝鲜有关联的组织，该组织针对能源和航空航天实体进行了网络钓鱼攻击[2]。

C. 从入侵事件和网络活动中汲取的教训

2024 年的安全事件为卫星互联网的防御者提供了宝贵的经验教训：

- **已知漏洞的利用仍是主要途径：**许多攻击事件，如“咸 Typhoon”攻击，是通过利用已公开记录且已有补丁的漏洞得逞的。这暴露出即使是大型组织在补丁管理和网络卫生方面也存在严重缺陷[14]。
- **第三方风险不容忽视：**“咸 Typhoon”对美国财政部的攻击利用了 BeyondTrust 远程支持软件的漏洞，这凸显了第三方解决方案可能带来的风险[14]。对于依赖各类供应商提供地面系统和软件的卫星运营商而言，这一点尤为重要。
- **国家背景行为者的持久性和适应性：**相关网络活动显示，国家背景的攻击者具有长期投入、拥有复杂工具集，并能根据特定目标（如星链）调整其战术策略的能力[5]。
- **军民两用基础设施成为首要目标：**一些国家（如俄罗斯）已明确将用于政府或军事目的的商业卫星系统视为合法打击目标[2]。

2024 年的安全事件，如 GPS 干扰/欺骗[2] 和针对星链的干扰尝试[5]，清晰地展示了一个趋势：网络攻击正对卫星服务的可用性和完整性产生直接的物理世界影响。这模糊了纯粹网络空间行动与空间领域动能效应之间的界限。GPS 干扰直接影响物理导航和授时；星链服务中断则影响地面用户（包括军事单位）的实时通信[5]。CSIS 的报告[2] 指出，未来的战争将在太空、通过太空和从太空进行，这意味着轨道上的干扰和破坏将成为关键考量。因此，卫星安全不仅要考虑数据泄露风险，更要确保其所赋能的物理服务的运行连续性。

在空间领域，明确攻击归属和理解攻击者真实意图的难度[2]，造成了一种“网络战迷雾”。

虚假声明或夸大的攻击成果可能被用于宣传目的，使得准确的威胁评估变得异常困难。CSIS 报告[2]明确提到了在统计和描述网络攻击（包括动机和目标）方面面临的挑战，并指出黑客可能虚报战果。许多空间技术的军民两用特性[2]意味着某些行为（如卫星机动）即使是良性的，也可能被误解为敌对行为，反之亦然。这种模糊性，尤其是在紧张的地缘政治环境下，可能导致误判和局势升级。

商业卫星系统（如星链）成为攻击目标[5]，以及俄罗斯明确声明将美国军方使用的商业资产视为合法打击对象[2]，这些都凸显了商业卫星基础设施正日益被卷入地缘政治冲突的漩涡，无论其主要的商业用途为何。星链在乌克兰冲突中的作用使其成为直接目标[5]。俄罗斯外交部的声明[2]则从官方层面确认了这种威胁。而“数字主权”概念的兴起[15]，也反映出各国因担心在地缘政治危机中关键功能受制于人，而对依赖外国商业系统持谨慎态度。这意味着商业卫星运营商除了应对技术安全挑战外，还必须驾驭复杂的地缘政治风险。

表 2: 2024 年重大卫星互联网安全事件/活动概述

事件/活动	日期 (大约)	归属行为者 (若已知)	目标	主要策略/利用漏洞	影响	参考资料
俄罗斯针对星链的持续网络活动	2022-2024 年	俄罗斯国家支持黑客	星链系统（硬件、软件、用户终端、C2 基础设施）	GPS 欺骗、信号干扰、网络间谍（Sandworm）、恶意软件（Amadey, Tavdig）、固件漏洞利用、弱认证利用	拦截通信、干扰乌克兰军事行动、绘制网络架构、部分用户服务中断	5
俄罗斯广泛的 GPS 干扰与欺	2024 年 (中期加剧)	俄罗斯	GPS 信号用户（波罗的海至黑海区	信号干扰、信号欺骗	导航失效、授时错误、影响民航及	2

骗活动			域）		关键基础设施运营	
俄罗斯“宇宙-2576”反卫星武器疑虑	2024 年 5 月	俄罗斯	潜在目标：美国政府卫星 (USA 314)	在轨机动至目标卫星共面轨道	引发对在轨反卫星武器部署的担忧，加剧太空军事化风险	2
中国“咸 Typhoon”网络攻击活动 (背景)	2024 年 (持续)	中国国家支持黑客	美国电信巨头、美国财政部	利用已知漏洞 (如 CVE-2023-46805, CVE-2024-21887)、第三方软件漏洞 (BeyondTrust)	(对电信/金融业) 数据泄露、系统入侵；警示卫星关键基础设施面临类似复杂威胁的风险	14
伊朗“桃色沙尘暴”网络攻击活动	2024 年 (持续)	伊朗伊斯兰革命卫队	航空航天、卫星、通信等行业	情报收集、社会工程攻击	数据泄露、潜在的系统渗透风险	2
朝鲜针对航空航天等领域的网络间谍活动	2024 年 (持续)	朝鲜关联组织	国防、航空航天、核工程实体	网络钓鱼、间谍软件	敏感技术信息泄露、助力朝鲜军事及核能力发展	2

IV. 卫星互联网安全技术与防御进展

面对日益严峻的安全挑战，2024 年卫星互联网领域在防御技术和策略方面也取得了显著进展。

A. 防御策略与框架

- **盛邦安全等提出的“三维度构建安全屏障”：**《2024 卫星互联网安全年度报告》由盛邦安全、南京航空航天大学及南京天际易达通信技术有限公司联合发布，报告强调需从通信链路、卫星设备、网络架构以及地面终端等多个层面构建卫星互联网安全屏障[6]。虽然公开摘要中细节有限，但这表明业界正朝着一个整体化、多层次的安全理念发展。
- **ENISA 的网络安全控制框架：**ENISA 在其《从网络到外层空间：商业卫星运营安全指南》（2025 年 3 月发布，涵盖持续需求）中，为商业卫星运营商提供了一个扩展的网络安全控制框架，包含 35 个子类别下的 125 项控制措施[10]。该框架的发布，为规范行业安全实践做出了重要贡献。
- **主动威胁狩猎与零信任模型：**2024 年整体网络安全趋势强调从被动事件响应转向主动威胁狩猎（在威胁被利用前识别并清除）和零信任模型（对每个访问请求进行严格验证）[9]。这些理念对于结构复杂、节点分散的卫星网络而言，具有极高的应用价值和必要性。
- **“设计安全”与“默认安全”原则：**ENISA 建议引入基于“设计安全”和“默认安全”的最低行业标准[10]。这意味着在卫星系统开发的最早阶段就将安全因素融入其中，而非后期弥补。

B. 人工智能与机器学习（AI/ML）的角色

AI/ML 技术在提升卫星互联网安全防御能力方面展现出巨大潜力：

- **异常检测与威胁预测：**
  - **Slingshot Aerospace 的 Agatha AI：**作为 2024 年的一项瞩目技术进展，Agatha AI 由 Slingshot Aerospace 与美国国防高级研究计划局（DARPA）合作开发。它采用“逆向强化学习（IRL）”技术，通过评估卫星行为模式来识别异常并预测潜在威胁，而无需依赖特定的威胁特征库。据报道，Agatha AI 在 2024 年识别出中国和俄罗斯等国卫星的诸多异常活动[7]。这标志着 AI 在提升空间态势感知和安全预警能力方面迈出了重要一步。
  - **通用 AI 应用：**AI/ML 被日益视为增强电信网络（包括卫星网络）功能、提高效率、实现预测性维护以及进行安全/异常检测的关键技术[17]。
- **网络韧性与自动化：**AI 技术能够实现跨多个网络资产的自动化智能路由和通信重路由[20]，从而增强网络在遭受攻击或干扰时的韧性。计划于 2024 年 6 月发布的 3GPP Release 18（5.5G 标准）也强调利用 AI/ML 进行网络优化和自动化[18]。

C. 量子密码学与后量子密码学（PQC）进展

量子计算的出现对现有密码体系构成了颠覆性威胁，同时也催生了量子密码和后量子密码

的快速发展：

- **量子威胁的紧迫性**：据预测，量子计算机可能在 2030 年左右破解当前广泛使用的加密算法，这将对包括卫星通信在内的所有数字通信安全构成严重威胁 [8]。
- **NIST PQC 标准化进程**：2024 年 8 月，美国国家标准与技术研究院（NIST）正式发布了三项后量子密码标准：FIPS 203（基于 ML-KEM/CRYSTALS-Kyber，用于通用加密）、FIPS 204（基于 ML-DSA/CRYSTALS-Dilithium，用于数字签名）和 FIPS 205（基于 SLH-DSA/SPHINCS+，用于数字签名）。第四项标准（FN-DSA/FALCON）预计于 2024 年底完成标准化 [8]。这为全球向抗量子密码体制迁移提供了清晰的技术路线图。
- **卫星量子加密探索**：
  - 中国研究团队在通过微小卫星进行量子密钥分发方面取得进展，实现了远距离安全密钥共享 [21]。这种技术基于硬件，利用单光子特性提供高级别的安全性。
  - 将量子能力集成到卫星星座中（如中国 LEO 星座计划中提及 [22]），有望进一步增强数据安全性和韧性。
  - Arquit 等公司正在开发抗量子攻击的加密解决方案，Sparkle 已于 2024 年采用 Arquit 技术推出其网络即服务（NaaS）产品 [21]。量子加密市场预计将迎来显著增长 [21]。

D. 安全通信协议与加密技术发展

- **区块链技术的应用探索**：区块链技术因其去中心化账本、智能合约和先进加密方法的特性，被探索用于增强卫星通信安全。其优势包括提供强大的加密保护、防篡改记录、去中心化控制以及安全的身份验证和数据交换机制 [23]。中国和美国在该领域的研究处于领先地位 [23]。
- **5G/6G 中的增强加密**：相较于 4G，5G 引入了更强的安全措施，包括增强的加密算法和身份管理机制 [18]。而未来的 6G 网络则旨在原生集成 AI，并为泛在连接提供更为强大的安全保障 [18]。
- **Link 16 在太空的应用**：York Space Systems 公司在 2023/2024 年成功演示了从美国太空发展局（SDA）“增殖型作战人员太空架构”（Proliferated Warfighter Space Architecture）Tranche 0 卫星向军事资产进行安全、实时的 Link 16 战术数据链通信，显著增强了军事通信的安全性和互操作性 [7]。

尽管人工智能（如 Agatha AI）为监控和威胁检测提供了强大的新型防御能力 [7]，但一个不言而喻的现实是，攻击方同样会利用 AI 来开发更复杂的攻击手段。这预示着太空网络安全领域将上演一场由 AI 驱动的、持续升级的攻防竞赛。Agatha AI 所采用的“逆向强化学习”技术 [7]，其核心在于理解行为意图，理论上攻击者也可能借鉴类似方法来更好地建模和规避防御系统。

NIST 在 2024 年完成 PQC 标准的制定是一个关键里程碑[8]，但向这些新算法的迁移将是一项极其庞大而复杂的工程，对于像卫星这样生命周期长的资产尤其如此。如果不能及时完成迁移，一旦强大的量子计算机出现，“先窃取后解密”的威胁将使大量当前通过卫星传输的数据面临回顾性泄露的风险。卫星系统升级密码体制通常非常困难，甚至不可能在轨完成。考虑到卫星系统的复杂性（涉及空间段、地面段和用户终端），整个生态系统需要协同进行 PQC 迁移。而 2030 年量子计算机破解现有加密的预测[8]，为这场全球性的复杂迁移设定了一个相对紧迫的时间窗口。

量子加密[21]和全面的区块链集成[23]等技术虽然能提供极高水平的安全性，但在成本、灵活性、可扩展性和部署便捷性方面，与传统方法相比仍面临挑战。量子加密被指“高度依赖硬件且不灵活”，短期内因技术复杂性和成本因素“不太可能被大多数互联网用户采用”[21]。尽管区块链具有诸多优势[23]，但在复杂、实时的卫星操作中广泛采用，仍需克服重大的工程和标准化障碍。因此，近期更有可能出现混合方案，即新的安全技术与现有技术“多层叠加”[20]，逐步演进，而非一蹴而就的全面替代。

V. 2024 年法规、政策与标准化进展

2024 年，各国政府和行业组织在为卫星互联网建立更健全的安全治理框架方面做出了显著努力。

A. 关键政府政策与立法

- **美国：**
  - **《卫星网络安全法案》（S. 1425）：**该法案于 2023 年提出，要求就联邦政府对商业卫星系统网络安全的支持情况提交报告，并整合针对商业卫星系统开发、维护和运营的自愿性网络安全建议。这些建议涵盖基于风险的网络安全工程、网络安全事件后的恢复能力、对关键系统功能的未授权访问防护、指挥控制与遥测接收系统的物理防护措施，以及针对干扰、窃听、劫持、计算机网络利用、欺骗、光通信威胁和电磁脉冲等多种威胁的防护[11]。这标志着美国政府对商业卫星基础设施安全的关注度日益提升。
  - **《国家网络安全战略》及实施计划（NCSIP）：**《2024 年美国网络安全态势报告》（涵盖 2023 年及 2024 年初）概述了国家网络安全战略的进展，强调从被动应对转向主动防御。其中包括通过制定监管要求来保护关键基础设施，以及推动构建尊重权利的数字生态系统[9]。卫星网络作为关键基础设施，也包含在这一战略框架之内。
  - **空间相关出口管制的现代化：**2024 年，美国国务院和商务部宣布了一系列新规，旨在实现空间相关出口管制的现代化，以期在保障国家安全的同时，增强美国在该领域的竞争力和国际空间伙伴关系。相关意见征询已于 2024 年 12 月结

束[24]。
    - **修订卫星频谱共享规则**：新规则旨在促进市场准入、提高监管确定性并提升频谱利用效率，尤其关注非对地静止轨道（NGSO）卫星系统[24]。
- **欧盟：**
    - **NIS2 指令**：该指令将空间领域列为高度关键行业，因其网络攻击可能产生跨行业、跨境的连锁效应。卫星运营商必须遵守高级别的网络安全义务[10]。
    - **欧盟空间信息共享与分析中心（EU Space ISAC）**：于 2024 年成立，旨在加强空间威胁相关信息的合作与共享。ENISA 在该中心拥有观察员席位[10]。这是迈向集体防御的关键一步。
    - **《数字运营韧性法案》（DORA）**：自 2024 年起对欧盟所有金融实体具有约束力。鉴于金融交易日益依赖卫星通信，该法案与卫星安全间接相关[10]。
    - **《网络韧性法案》（CRA）**：预计将对空间系统的开发、运营和退役产生影响，因为它强制要求所有投放欧盟市场的含数字元素的产品在其整个生命周期内都必须符合具有约束力的网络安全标准[10]。
    - **拟议的《欧盟空间法》**：原计划于 2024 年发布，现已推迟至 2025 年。预计将涵盖空间交通管理和关键空间基础设施安全等规则[24]。

B. 新增及更新的行业标准与指南

- **欧洲空间标准化合作组织（ECSS）**：于 2024 年 7 月发布了一系列技术标准和指南[10]。这些标准对于统一欧洲航天工业的安全实践至关重要。
- **ENISA 商业卫星运营商网络安全控制框架**：（如第四部分 A 节所述）提供了详细且可操作的指导[10]。
- **移动卫星服务协会（MSSA）推动的 D2D 生态系统标准**：MSSA 旨在促进建立一个设备直连（D2D）解决方案提供商生态系统，包括地面移动和卫星运营商、OEM 厂商、基础设施和芯片供应商等，并为多轨道卫星系统、地面基础设施和终端用户设备构建可互操作的架构和标准[24]。

C. 国际合作与信息共享

- **欧盟空间信息共享与分析中心（EU Space ISAC）**：是区域信息共享合作的典范[10]。
- **《阿尔忒弥斯协定》（Artemis Accords）**：由美国主导的一系列旨在指导太空探索与合作的原则，2024 年有更多国家签署加入[24]。虽然不完全聚焦于安全，但合作本身有助于增进透明度。
- **《零碎片宪章》（Zero Debris Charter）**：为解决日益严重的空间碎片问题而发起，通过倡导负责任的空间操作，间接促进了空间安全[24]。

各国政府在制定卫星互联网安全法规时，似乎在寻求一种平衡：既要对关键的卫星基础设施实施严格的安全监管，又要避免扼杀快速增长的商业航天市场的创新活力。美国的《卫星网络安全法案》中提出的“自愿性建议”[11]，以及在出口管制等领域更为直接的监管举措[24]，都体现了这种权衡。卫星互联网巨大的经济潜力[25]和其在军事、灾害响应等关键领域的极端重要性[20]，以及其固有的脆弱性[2]，共同塑造了这种复杂的监管环境。欧盟通过 NIS2 指令[10]对关键行业采取了更具指导性的监管方式，而美国则往往在初期倾向于公私合作和自愿性标准，尽管这种做法未来也可能演变。

除了正式的条约和国家法律之外，“软法”（如《阿尔忒弥斯协定》这类不具约束力的原则和指南[24]）、行业主导的标准（如 ECSS 标准[10]）以及多利益相关方机构（如 EU Space ISAC[10]）在塑造空间安全规范和实践方面的作用日益凸显。国际条约的制定过程通常缓慢且复杂，而空间领域涉及政府、商业公司、学术界等多元行为体。“软法”机制更为灵活，更能适应技术的快速变革。像 ISAC 这样的信息共享机构对于及时的威胁响应至关重要，这是仅靠正式法规难以实现的。

频谱共享规则的修订[24]和星座的 ITU 备案[22]等频谱管理措施，其首要目标是资源分配和防止干扰，但也间接影响着安全。更清晰的频谱规则可以减少模糊性以及可能升级或被利用的潜在争端，而频谱分配过程本身也为监管机构进行国家安全审查提供了一个窗口。射频干扰本身就是一种攻击形式（如干扰），频谱权利的争端也可能成为地缘政治的摩擦点。此外，高效的频谱利用也有助于实现更具韧性的网络设计。

表 3: 2024 年卫星互联网安全关键法规政策进展

政策/法规/标准	发布机构/地区	卫星安全关键条款	状态/日期	参考资料
《卫星网络安全法案》(S. 1425)	美国	要求报告联邦对商业卫星系统网络安全的支持；整合自愿性网络安全建议（风险工程、事件恢复、访问控制、物理防护、威胁防御等）。	2023 年提出	[11]

《国家网络安全战略》及实施计划 (NCSIP)	美国	强调从被动应对转向主动防御；保护关键基础设施；推动尊重权利的数字生态系统。	2024 年报告发布	9
空间相关出口管制现代化	美国	更新出口管制规则，平衡国家安全与产业竞争力及国际合作。	2024 年宣布/征询意见	24
修订卫星频谱共享规则	美国	促进市场准入、监管确定性和频谱效率，特别针对 NGSO 系统。	2024 年	24
NIS2 指令	欧盟	将空间领域列为高度关键行业；卫星运营商须遵守高级别网络安全义务。	已生效	10
欧盟空间信息共享与分析中心 (EU Space ISAC)	欧盟	改善空间威胁相关信息的合作与共享。	2024 年成立	10
《数字运营韧性法案》(DORA)	欧盟	对金融实体具有约束力，间接关联卫星通信安全。	2024 年生效	10
《网络韧性法案》(CRA)	欧盟	预计将强制要求含数字元素的产品（包括空间系统）在其生命周期内符合网络安	预期影响	10

		全标准。		
拟议的《欧盟空间法》	欧盟	预计涵盖空间交通管理和关键空间基础设施安全。	原定 2024 年，推迟至 2025 年	24
欧洲空间标准化合作组织 (ECSS) 标准	ECSS (欧洲)	发布一系列技术标准和指南，促进欧洲航天工业安全实践的统一。	2024 年 7 月发布	10
移动卫星服务协会 (MSSA) D2D 标准	MSSA (国际)	推动建立 D2D 生态系统，为多轨道卫星系统、地面基础设施和终端用户设备构建可互操作的架构和标准。	2024 年目标	24

VI. 地缘政治与商业因素对安全的影响

A. 地缘政治紧张局势的影响

地缘政治的紧张态势深刻地塑造着卫星互联网的安全格局：

- **军民两用性与战略资产地位**：LEO 卫星日益被视为国家安全和地缘政治利益的战略资产，而不仅仅是商业服务 [15]。空间本身就是一个战略领域，而 LEO 网络具有军民两用的特性 [16]，这使其天然地处于地缘政治博弈的中心。
- **冲突中的目标化**：一些国家（如俄罗斯）已明确将用于军事或政府目的的商业卫星资产视为合法打击目标 [2]。星链在乌克兰冲突中的广泛应用，生动地展示了商业卫星系统如何被卷入武装冲突并成为攻击对象 [5]。
- **数字主权与技术依赖**：对外国控制关键通信基础设施的担忧日益加剧 [15]。例如，印度等国家对依赖星链等外国系统持谨慎态度，担心失去对数据和网络的控制权，这反过来推动了发展本土能力或寻求有明确安全保障的战略合作 [16]。
- **太空成为大国竞争的新舞台**：卫星星座的开发和部署正成为国家软实力和全球影响力的体现。各国在技术基础设施方面也开始与特定政治集团结盟，例如印度选择与美国体系（星链、OneWeb）合作，而非中国的“国网”星座，反映了印太地区民主技术联

盟的趋势[16]。

B. LEO 星座扩散与竞争的安全影响

LEO 星座的迅速发展和激烈的市场竞争，为卫星互联网安全带来了新的维度和挑战：

- **攻击面的显著扩大**：LEO 巨型星座（如星链、柯伊伯计划、OneWeb 以及中国的国网和千帆等）中卫星数量的激增，极大地扩展了潜在的攻击面[4]。每一个在轨卫星、每一个地面站、每一个用户终端都可能成为潜在的攻击入口。
- **新型漏洞的出现**：LEO 系统不仅面临针对用户段和控制段的传统网络威胁，还面临针对空间段本身的攻击，例如有效载荷或整个卫星平台的劫持风险[4]。其全球化的资产分布和更高的金融风险，要求采取量身定制的网络安全策略[4]。
- **商业竞争的动态影响**：
  - **创新与韧性**：竞争（例如亚马逊的柯伊伯计划对星链的挑战）能够推动技术创新、降低服务价格并提升服务质量。一个多元化的产业格局可以减少对单一供应商的依赖，从而增强整体安全性和可靠性[26]。卫星互联网市场预计将持续显著增长[25]。
  - **垄断风险**：如果单一供应商（如目前星链的领先地位）形成市场主导，可能会抑制创新、抬高价格，并因过度依赖而造成经济和安全上的脆弱性[26]。
  - **供应链与制造挑战**：快速部署 LEO 星座（如中国的 LEO 计划[22]和柯伊伯计划的卫星制造[27]）对发射能力和卫星制造能力提出了巨大挑战。如果在追求速度和规模的过程中，对供应链安全和组件审查有所松懈，则可能引入安全隐患。

C. 保护大规模商业星座的挑战与策略

确保大规模商业 LEO 星座的安全，需要综合性的策略和持续的努力：

- **协调与标准化**：欧洲航天局（ESA）的 SPACE-SHIELD 等倡议，承认需要通过标准、建议和信息共享来协调 LEO 卫星通信系统的安全防护工作[4]。
- **量身定制的网络安全方法**：鉴于 LEO 卫星通信系统面临的威胁暴露程度和潜在影响的严重性，其网络风险可能高于地面网络，因此需要采取特定的、有针对性的安全措施[4]。
- **整合网络安全与航天工程技能**：为了在 LEO 系统中正确有效地实施安全措施，必须确保网络安全专业知识与航天工程技能的紧密结合[4]。
- **资源约束与安全需求的平衡**：对于新兴或规模较小的 LEO 运营商而言，在星座部署的巨大成本与强大的网络安全投入之间取得平衡，可能是一个严峻的挑战。

地缘政治的紧张局势正在加速商业航天领域的“安全化”进程，即商业决策（如选择供应商、数据路由等）越来越多地从国家安全的视角进行审视。俄罗斯的表态[2]和对数字主权

的担忧[15]表明，各国政府对其关键通信由谁控制高度敏感。军民两用特性[16]意味着商业系统本身就具有军事价值。各国正努力发展本土能力[16]，以减少依赖。这可能导致市场碎片化和“技术民族主义”，对全球互操作性和开放市场构成潜在影响。

LEO 领域的竞争对安全而言是一把双刃剑。一方面，竞争可以推动创新并提供替代方案，从而降低单点故障风险[26]。另一方面，激烈的商业压力，尤其对于试图追赶市场领导者的新进入者而言，如果将上市速度或成本控制置于强大的安全工程之上，则可能导致安全妥协。部署数千颗卫星的竞赛[22]资本密集且时间敏感。如果未能从一开始就贯彻“设计安全”的原则[10]，后续弥补安全缺陷将非常困难且成本高昂。快速实现运营能力和市场份额的压力，可能会诱使一些运营商在不太显眼的安全投入上做出让步。

中国大力发展自己的 LEO 巨型星座（如国网、千帆）[22]，其驱动力不仅来自商业利益，更源于战略需要（如国家实力、主权和国家安全）。正如报告所指出的，对于中国的 LEO 计划而言，“战略需要优先于财务考量”[22]。这与更广泛的“数字主权”关切[15]相呼应。拥有独立的 LEO 能力，可以使其在面临外国势力潜在的服务拒止时保持韧性，并为其自身的国家和军事需求提供安全通信保障。这是成为全面航天强国的关键组成部分。

VII. 2024 年主要安全报告与研究的核心发现

2024 年发布的多份报告和研究成果，为理解卫星互联网安全态势提供了重要视角。

A. 盛邦安全等 - 《2024 卫星互联网安全年度报告》

- 该报告被誉为“行业首份”，由盛邦安全联合南京航空航天大学、南京天际易达通信技术有限公司共同发布[6]。
- 报告的核心观点是卫星互联网安全的复杂性，指出其安全防御涉及通信链路、卫星设备、网络架构以及地面终端等多个层面[6]。
- 报告提出了构建“三维度安全屏障”的理念[6]，尽管公开摘要未提供具体细节，但这暗示了一种多方面、深层次的防御战略。
- （注：现有公开信息对这份报告的具体内容揭示有限，主要集中在其发布背景和总体目标。获取完整报告才能深入了解其详细发现。）

B. ENISA - 《从网络到外层空间》及《LEO 卫星通信网络安全评估》

- **《从网络到外层空间：商业卫星运营安全指南》**（2025 年 3 月发布，内容与 2024 年背景相关）：该指南概述了卫星生命周期模型、参与者、资产分类和空间威胁，并使用四种风险情景进行了风险评估分析。它为商业卫星运营商提供了一个包含 125 个项目（分为 35 个子类别）的扩展网络安全控制框架[10]。报告强调了干扰、劫持、计算机网络利用（CNE）等主要威胁，以及国家背景行为者、网络犯罪团伙、私营部

门攻击性行为者（PSOA）和黑客行动主义者等威胁行为者[10]。同时，报告还指出了由软件定义卫星、商用现货组件（COTS）使用和量子技术发展带来的演进性威胁[10]。

- **《LEO 卫星通信网络安全评估》**（2024 年 2 月）：这份报告聚焦于 LEO 系统，指出它们除了面临针对用户段和控制段的传统攻击外，还面临针对空间段的威胁（如有效载荷/平台劫持）。报告建议，鉴于 LEO 系统资产的全球性和较高的金融风险，应采取量身定制的网络安全方法。报告还强调了协调安全措施以及网络安全与空间工程技能融合的必要性[4]。
- **《ENISA 2024 年威胁态势报告》**（2024 年 9 月）：这份通用性报告识别了 2024 年七大主要网络威胁，其中针对可用性的攻击和勒索软件位列前茅[10]。该报告为理解卫星互联网所处的整体威胁环境提供了背景。

C. CSIS - 《2025 年空间威胁评估》（涵盖 2024 年事件）

- 报告作者指出，追踪针对空间系统的网络攻击的年度数量变得越来越困难[2]。
- 根据 ERCI 数据，2024 年所有行业共报告约 720 起网络事件，其中 57%针对关键基础设施，有 5 起明确针对空间领域[2]。
- 报告重点强调了 GPS 信号的广泛干扰和欺骗（尤其是在俄罗斯和中东地区）、中国和俄罗斯卫星先进的在轨机动能力，以及对俄罗斯潜在核反卫星武器的持续担忧[2]。
- 报告还讨论了军民两用技术、作为反太空武器的网络行动，以及特定国家（中国、俄罗斯、伊朗、朝鲜）的相关活动[2]。

D. 学术研究成果

- **Yu 等人 - 《卫星调制解调器安全漏洞与攻击的综合分析 CCS '24》**：这是首个通过物理拆解商用调制解调器进行的全面研究。研究识别出 16 个漏洞（分布于卫星通信接口 SCI、地面网络接口 GNI 和硬件 HW）并演示了 18 种新型攻击。关键问题包括：脆弱的时间同步机制、薄弱的身份认证、默认未加密流量、命令注入、跨站脚本（XSS）、SQL 注入以及固件提取等[13]。这篇论文对于理解地面终端脆弱性至关重要。
- **张远宇等人 - 《卫星互联网安全：需求、现状与趋势》（《网络空间安全科学学报》，2024 年）**：该文聚焦于卫星互联网的关键安全需求、当前状况和发展趋势。其中部分内容[3]详细描述了非法节点接入、链路与路由攻击以及“伪卫星”攻击等威胁，并特别指出了铱星系统认证机制的脆弱性。（注：公开的元数据信息[3]较多，需获取原文以了解全部内容）。

尽管盛邦安全的报告[6]和 ENISA 的报告[10]提供了框架并识别了威胁，但 CSIS 报告中承认追踪攻击的困难性[2]，以及关于“五起空间攻击”的公开细节有限，这暗示着在情报获取

或信息公开方面可能存在显著的“已知未知”缺口。许多事件的真实程度和性质可能未被充分报道。CSIS 报告明确指出作者发现“越来越难以追踪……针对空间系统的网络攻击” [2]。商业运营商和政府可能出于国家安全或声誉考虑而不愿披露事件。空间相关事件归属的技术复杂性也加剧了这一挑战。这意味着公开报告虽然有价值，但可能只揭示了冰山一角。

当前的研究格局展现出学术界、产业界和政府之间日益增强的合作与协同趋势。学术研究（如 Yu 等人关于调制解调器的研究 [13]，以及张远宇等人关于一般性威胁的研究 [3]）揭示了深层次的技术漏洞。产业界报告（如盛邦安全的报告 [6]）则致力于提供实用的框架。而与政府关联的机构（如 ENISA、CSIS）则提供更广泛的威胁评估和政策指导。这种协同对于应对复杂的安全挑战至关重要。盛邦安全的报告 [6] 有高校和科技公司参与；ENISA [10] 与产业界和国家当局合作；CSIS [2] 利用开源信息但为决策者提供参考；而学术论文则为行业最佳实践和政府标准提供了基础研究支撑。

VIII. 2025 年展望与建议

A. 预期安全挑战与趋势

展望 2025 年，卫星互联网安全领域预计将面临以下主要挑战和趋势：

- **攻击复杂性持续升级**：预计将出现更多由人工智能驱动的攻击，针对 LEO 星座复杂性的漏洞利用，以及国家背景行为者对卫星关键网络基础设施（CNI）的持续关注。
- **供应链脆弱性凸显**：随着 LEO 星座的快速扩张，确保全球组件和软件供应链的安全将成为一个更大的挑战，并可能成为新的攻击热点区域。
- **后量子密码（PQC）迁移启动**：在新的卫星系统和地面基础设施中规划和实施 PQC 的初步工作将会展开，但广泛采用仍需数年时间。
- **竞争环境下的对抗升级**：在地缘政治热点地区，针对卫星服务的干扰、欺骗和网络攻击可能会持续或加剧。
- **监管差异与协调的博弈**：各国/地区针对卫星互联网的安全标准可能出现差异，给全球运营商带来合规性挑战；与此同时，国际间寻求标准协调的努力也将继续。

B. 战略建议

为应对上述挑战，建议各相关方采取以下战略措施：

- **对卫星运营商：**
  - 在整个卫星生命周期中贯彻“设计安全”和“默认安全”原则。
  - 实施强健的漏洞管理和补丁部署流程，尤其针对地面系统和用户终端（汲取 [13] 的教训）。
  - 投资于先进的威胁检测技术，包括 AI/ML 能力（如 [7] 所述），并积极参与信息共

享机制（如欧盟空间 ISAC [10]）。
    - 制定全面的事件响应和恢复计划，充分考虑空间资产的独特性。
    - 启动向 PQC 迁移的战略规划。
- **对政府与监管机构：**
    - 继续制定和协调清晰的卫星互联网网络安全标准与法规，在保障安全需求与鼓励创新之间取得平衡（借鉴 [9] 的经验）。
    - 促进在威胁情报共享、事件响应以及制定空间行为规范方面的国际合作。
    - 支持卫星安全技术（包括 PQC 和基于 AI 的防御技术）的研发。
    - 将频谱安全作为整体卫星安全的一部分加以解决。
- **对企业与用户：**
    - 对卫星互联网提供商的安全实践进行尽职调查。
    - 为用户终端实施强大的端点安全防护。
    - 了解通过卫星链路传输数据的风险，并在可能的情况下使用端到端加密。

C. 总结性强调

卫星互联网的安全是一项共同责任。主动协作、持续适应不断演变的威胁态势，以及致力于强大的安全工程，对于确保这个日益重要的全球基础设施的韧性和可信度至关重要。2024 年的经验教训进一步凸显了这些努力的紧迫性。

尽管大部分关注点在于防止数据泄露（机密性）和数据篡改（完整性），但广泛的干扰事件（如 GPS 干扰 [2]）和拒绝服务攻击 [4] 的影响表明，确保卫星服务的*可用性*和*韧性*可能是 2025 年最为关键的安全挑战，特别是考虑到其在关键基础设施和冲突中的作用。Viasat 事件（[10] 背景信息）和星链服务中断 [5] 都显示了当可用性丧失时，会立即产生广泛的运营影响。对于应急响应 [20] 或军事行动 [20] 等服务而言，可用性是首要的。LEO 星座以其分布式架构，部分设计目标就是为了提高韧性，但这需要针对不断演变的威胁进行持续测试。因此，未来的建议应高度强调架构韧性、冗余设计和快速恢复能力。

引用的著作

1. 网络安全威胁 2024 年度报告 - 奇安信, 访问时间为 五月 26, 2025，https://www.qianxin.com/threat/reportdetail?report_id=335
2. CSIS 2025 Space Threat Assessment: Cyberattacks on space ..., 访问时间为 五月 26, 2025， https://industrialcyber.co/reports/csis-2025-space-threat-assessment-cyberattacks-on-space-systems-persist-tracking-harder-amid-infrastructure-threats/
3. 卫星互联网安全：需求、现状与趋势 - 网络空间安全科学学报, 访问时间为 五月 26, 2025， https://www.journalofcybersec.com/CN/10.20172/j.issn.2097-3136.240401

4. Report: LEO Satcom Cybersecurity Assessment (EU 2024) - New Space Economy, 访问时间为 五月 26, 2025， https://newspaceeconomy.ca/2024/02/26/report-leo-satcom-cybersecurity-assessment-eu-2024/
5. Uncovering Potential Vulnerabilities in Starlink: Russian Hackers' Persistent Attempts, 访问时间为 五月 26, 2025， https://www.thesign.media/blog/uncovering-potential-vulnerabilities-in-starlink-russian-hackers-persistent-attempts
6. 卫星互联网加速“狂飙”背后如何筑牢信息安全防线？ - C114 通信网, 访问时间为 五月 26, 2025， https://m.c114.com.cn/w3542-1289881.html
7. Satellite Technology of the Year Nominees for 2024 | March 2025, 访问时间为 五月 26, 2025， https://interactive.satellitetoday.com/via/march-2025/satellite-technology-of-the-year-nominees-for-2024
8. NIST's Official 2024 Post-Quantum Algorithms - Sectigo, 访问时间为 五月 26, 2025， https://www.sectigo.com/resource-library/who-are-nists-post-quantum-algorithm-winners
9. 2024 REPORT ON THE CYBERSECURITY POSTURE OF THE UNITED STATES - Joe Biden for President, 访问时间为 五月 26, 2025， https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf
10. From Cyber to Outer Space: A Guide to Securing Commercial Satellite Operations - ENISA, 访问时间为 五月 26, 2025， https://www.enisa.europa.eu/news/from-cyber-to-outer-space-a-guide-to-securing-commercial-satellite-operations
11. Text - S.1425 - 118th Congress (2023-2024): Satellite Cybersecurity Act, 访问时间为 五月 26, 2025， https://www.congress.gov/bill/118th-congress/senate-bill/1425/text/is
12. 网络安全威胁 2024 年中报告 - 奇安信, 访问时间为 五月 26, 2025， https://www.qianxin.com/threat/reportdetail?report_id=317
13. ittc.ku.edu, 访问时间为 五月 26, 2025， http://ittc.ku.edu/~bluo/pubs/yu2024ccs.pdf
14. The Major Cyber Breaches and Attack Campaigns of 2024 - Picus Security, 访问时间为 五月 26, 2025， https://www.picussecurity.com/resource/blog/the-major-cyber-breaches-and-attack-campaigns-of-2024
15. The geopolitics of satellite connectivity and the Africa-Europe digital partnership - ECDPM, 访问时间为 五月 26, 2025， https://ecdpm.org/work/geopolitics-satellite-connectivity-and-africa-europe-digital-partnership
16. Satellite Internet: Geopolitics And Digital Divide - Only IAS, 访问时间为 五月 26, 2025， https://pwonlyias.com/current-affairs/about-satellite-internet/
17. 2024 Data Security Standards: A Peek into the Future of Cybersecurity, 访问时间为 五月 26, 2025， https://www.micromindercs.com/blog/2024-data-security-standards-a-peek-into-the-future-of-cybersecurity

18. 2024 Emerging Tech Trends Redefining the Future – Pt. 3 - IoT Marketing, 访问时间为 五月 26, 2025， https://iotmktg.com/2024-emerging-tech-trends-redefining-the-future-pt-3/
19. Satellite internet will fuel AI-powered systems and reshape global telecom with 24/7 coverage and smarter devices., 访问时间为 五月 26, 2025， https://wca.org/satellite-internet-will-fuel-ai-powered-systems-and-reshape-global-telecom-with-24-7-coverage-and-smarter-devices/
20. Satellite communications in 2024: The ins and outs - Viasat, 访问时间为 五月 26, 2025， https://www.viasat.com/perspectives/corporate/2024/satellite-communications-in-2024-the-ins-and-outs/
21. Record-Breaking Quantum Encryption Link Through Micro-Satellites Achieved - Securities.io, 访问时间为 五月 26, 2025， https://www.securities.io/record-breaking-quantum-encryption-link-through-micro-satellites-achieved/
22. China's LEO Megaconstellations: Closing the Gap in the Global Space Race - Frank Rayal, 访问时间为 五月 26, 2025， https://frankrayal.com/2025/05/19/chinas-leo-megaconstellations-closing-the-gap-in-the-global-space-race/
23. Emerging technology in detail: blockchain in satellite communications - WIPO, 访问时间为 五月 26, 2025， https://www.wipo.int/web-publications/wipo-technology-trends-technical-annex-future-of-transportation-in-space/en/emerging-technology-in-detail-blockchain-in-satellite-communications.html
24. Space and satellite wrap up – Legal and regulatory developments in 2024 - Bird & Bird, 访问时间为 五月 26, 2025， https://www.twobirds.com/en/insights/2025/global/space-and-satellite-wrap-up-legal-and-regulatory-developments-in-2024
25. Satellite Internet Market Size, Share | Global Report [2032] - Fortune Business Insights, 访问时间为 五月 26, 2025， https://www.fortunebusinessinsights.com/satellite-internet-market-109242
26. City Insider: Competition for Starlink will ensure a healthier, more dynamic and safer satellite connectivity market - Aviation Business News, 访问时间为 五月 26, 2025， https://www.aviationbusinessnews.com/in-depth/city-insider-competition-for-starlink-will-ensure-a-healthier-more-dynamic-and-safer-satellite-connectivity-market/
27. Project Kuiper - Wikipedia, 访问时间为 五月 26, 2025， https://en.wikipedia.org/wiki/Project_Kuiper
28. 直击北京军博会：eVTOL 以水滴机身+折叠机翼拓展应用场景，卫星 ..., 访问时间为 五月 26, 2025， https://finance.eastmoney.com/a/202505163406756790.html
29. Space Threat Assessment 2025 - CSIS, 访问时间为 五月 26, 2025， https://www.csis.org/analysis/space-threat-assessment-2025