

卫星互联网安全产业深度梳理

分析师：方闻千 SAC S0910523070001

2023年12月20日



华金证券客户中的专业投资者参考

更多免费行业报告

并购家

www.ipoipo.cn

并购家 免费行业报告网

IPOIPO.CN 每日更新 不用注册会员 无广告 永久免费

- ◆ 卫星通信技术的快速发展催生卫星互联网产业浪潮的到来，当前卫星互联网已经成为国家信息基础设施建设和大国在信息时代竞争的关键战略领域，其所面临的数字安全、网络安全问题正在逐渐凸显。随着卫星安全和网络安全的跨域融合，卫星互联网安全产业的发展机遇正在到来。
- ◆ 从安全域视角来看，卫星互联网面临的主要安全威胁涉及通信链路安全、地面系统安全、卫星及载荷安全、供应链安全以及用户终端安全等多个领域。其中通信链路、地面系统、供应链三大安全域是当前卫星互联网面临的最主要的攻击目标，攻击手段主要包括干扰、链路劫持、漏洞利用、窃听、恶意程序等，其中干扰、链路劫持和漏洞利用是最为常见的攻击手段。
- ◆ 从安全产品视角来看，卫星互联网安全产品主要包括通信加密认证、入侵检测与防御、网络攻击弹性测试、供应链风险管理和日志系统等。其中：1) 通信链路安全：涉及上行链路、下行链路和卫星间链路的安全，以加密与认证产品为主；2) 地面系统安全：产品种类较多，既包括防火墙、安全网关，又包括适用于卫星互联网的星载入侵检测与防御系统、星载日志系统等；3) 供应链安全：主要涵盖卫星系统开发的安全性、后续测试和验证以及供应商、第三方机构等的安全管理，产品包括太空靶场、多因素身份验证等。
- ◆ 卫星互联网安全的主要参与者既包括专业卫星安全厂商，同时也包括国防承包商及军工单位。其中，专业卫星安全厂商以加密类产品为主，而国防承包商及军工单位产品覆盖更广，并且可以将安全功能集成在卫星通信设备中，并以解决方案的形式交付客户。国内互联网安全厂商基于企业背景可分为两类：1) 以电科网安和航天江南为代表的国家队，其中，电科网安背靠中国电科，航天江南背靠航天五院，国家队在获取总包项目上具备一定优势，比如电科网安作为总包单位为星网提供密码安全产品，合同金额超过2000万元；2) 以佳缘科技为代表的民营卫星安全厂商，在产品技术和标杆客户等方面各具优势，同样是卫星安全市场的重要参与者。

- ◆ **国内卫星互联网安全厂商的竞争力主要体现在产品能力和标杆客户两方面。**1) 卫星安全产品需要具备在太空环境中的加密、认证与检测高可靠性：由于太空环境下具有高辐射、极低温或极高温等特点，相较于地面环境，容易引发半导体器件单粒子翻转等一系列问题，进而导致安全设备失效，因此卫星安全厂商需要具备卫星抗辐照软硬件平台开发、星际链路加密等相关技术，并能够满足部署在卫星上的一系列硬性要求；2) 标杆客户、标杆项目是未来快速拓展市场的基础，其中，电科网安、航天江南的产品已进入中国星网、中国卫通等大型卫星运营商供应链，且佳缘科技也成为了通信数传网安领域主要军工厂的供应商，在标杆客户方面已经建立一定的先发优势。
- ◆ **市场规模测算：2024-2027年中国卫星互联网安全市场有望新增七十亿元的规模。**1) 根据佳缘科技招股说明书，预计在“十四五”期间，卫星安全的总需求约为69-138亿元，即当前平均每年卫星安全市场规模约为14-28亿元；2) 据不完全统计，根据各家公司向国际电联（ITU）递交的申报计划，截止2027年预估我国小卫星数量将达到约1.4万颗；3) 结合NSR对单颗卫星网络安全支出的预测以及卫星制造成本情况，保守假设单颗卫星平均安全支出50万元，即24-27年有望新增70亿的卫星互联网安全相关需求。
- ◆ **投资逻辑：卫星互联网安全产业未来将迎来快速发展，看好具有国资背景、产品能力和标杆客户优势的公司，关注标的：佳缘科技、电科网安；相关标的：启明星辰、安恒信息、奇安信、盛邦安全、绿盟科技、吉大正元。**
- ◆ **风险提示：卫星建设进度不及预期；卫星发射进度不及预期；卫星互联网安全需求增长不及预期；市场竞争加剧；相关政策出台不及预期。**

01

卫星互联网安全的整体态势

02

卫星互联网安全域与安全威胁

03

卫星互联网安全技术及产品

04

卫星互联网安全产业链梳理

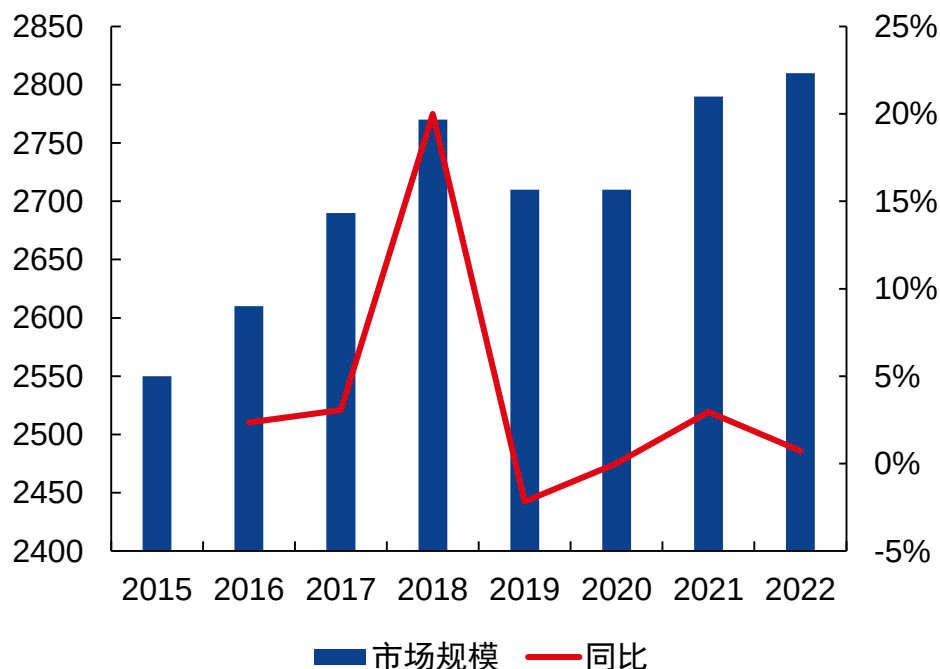
05

投资逻辑及风险提示

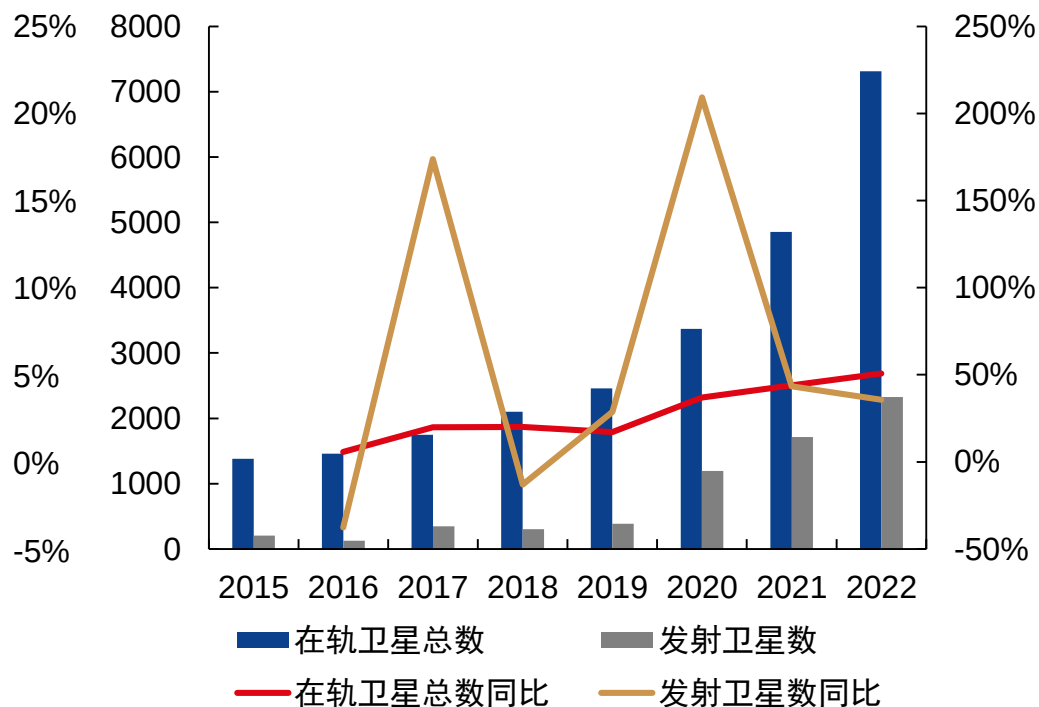
一、全球卫星互联网产业迎来发展热潮

卫星通信技术的快速发展催生卫星互联网产业浪潮的到来。近年来，各航天强国纷纷提出卫星星座计划，包括OneWeb、03b、Starlink等，其中SpaceX的Starlink星座计划已累计发射5581颗卫星。根据美国卫星产业协会SIA统计数据，2022年全球卫星产业规模达到2810亿美元，2022年全球卫星发射数量为2325颗，同比增长36%。同时自2017年以来，我国多个近地轨道卫星星座计划相继启动，包括鸿雁星座、行云工程、虹云工程、天象星座等。

图表：2015-2022年全球卫星产业规模（亿美元）



图表：2015-2022年全球在轨卫星总数和发射卫星数情况

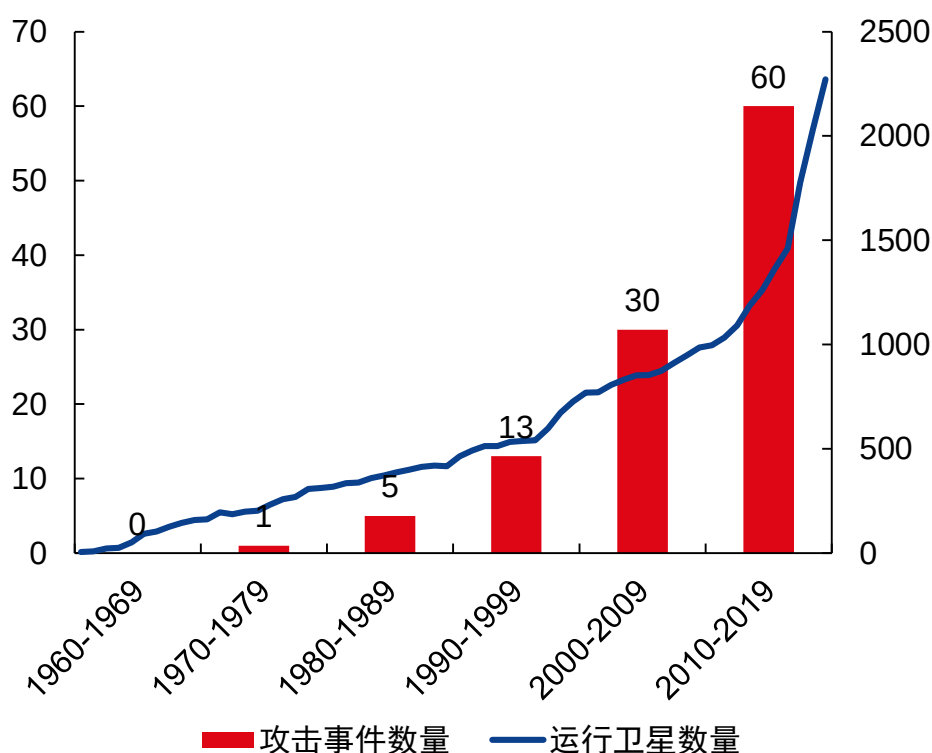


一、近年卫星网络安全攻击事件激增

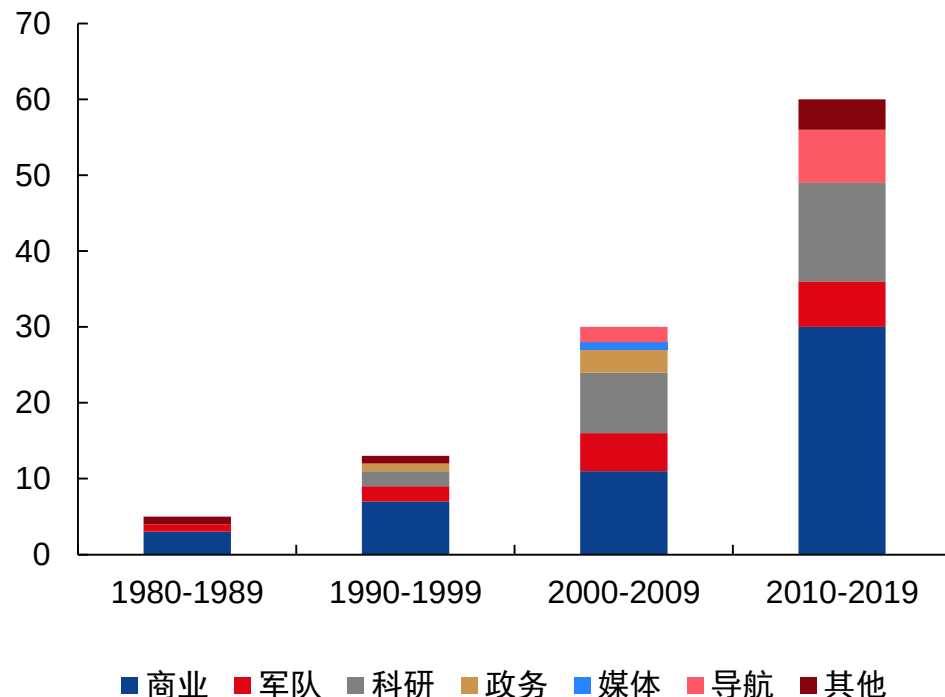
当前卫星互联网已经成为国家信息基础设施建设和大国在信息时代竞争的关键战略领域。卫星互联网当前面临的数字安全、网络安全问题正在逐渐凸显。随着卫星安全和网络安全的跨域融合，卫星互联网安全产业的发展机遇正在到来。

全球卫星网络安全攻击事件呈现两大趋势：1) 攻击高频化：随着卫星网络高速发展，卫星网络安全攻击事件激增，同时小卫星占比提升，降低了卫星行业进入门槛，导致系统安全性下降，又因其本身系统复杂度较低，使攻击者更易得手；2) 攻击面扩大：攻击目标从商业企业和军队向科研机构、政府等扩展，针对商业企业和军队以外的安全攻击占比从20%左右提升到40%。

图表：卫星互联网攻击事件激增

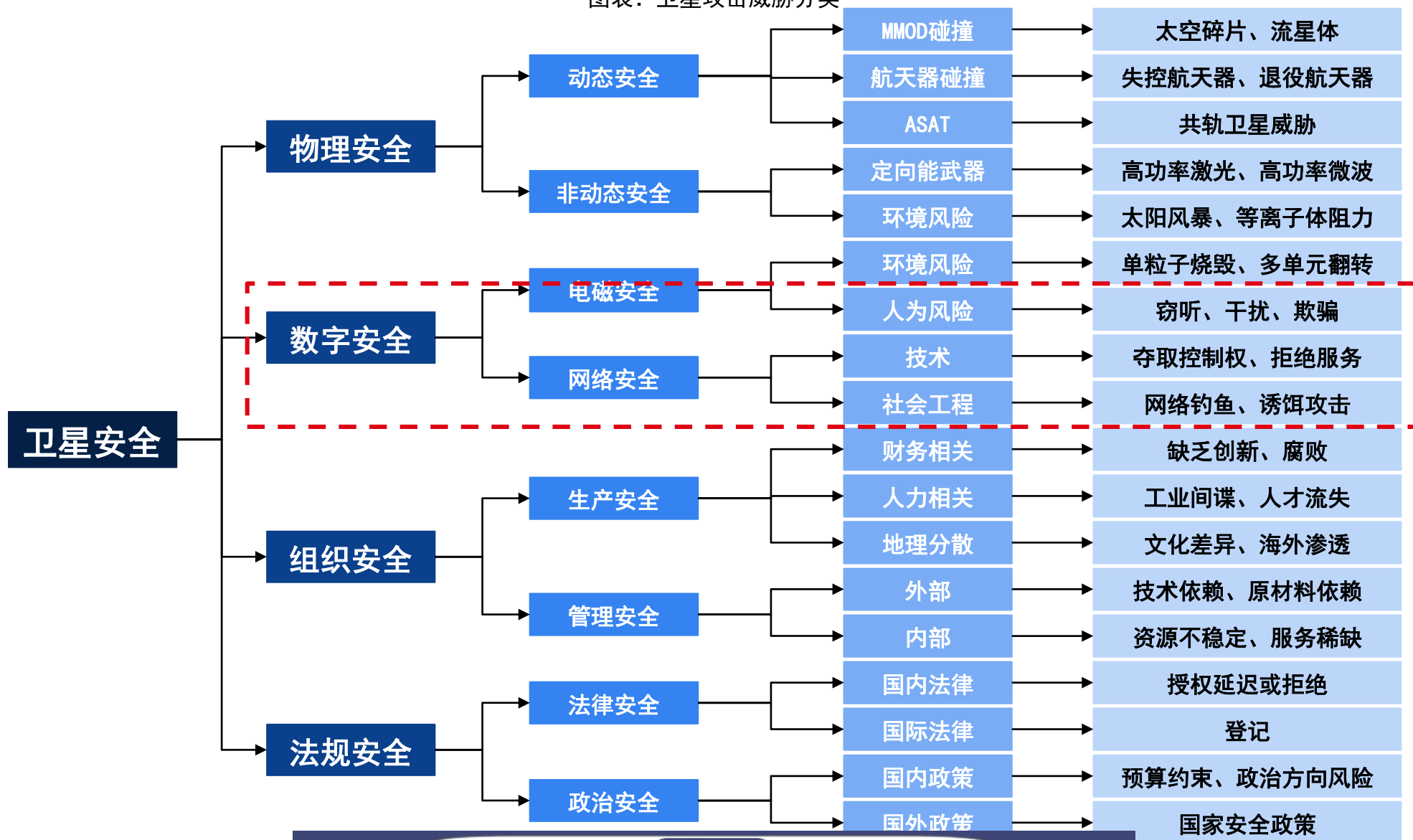


图表：攻击目标从商业和军队向其他领域扩展



二、整体框架：从卫星安全到卫星互联网安全

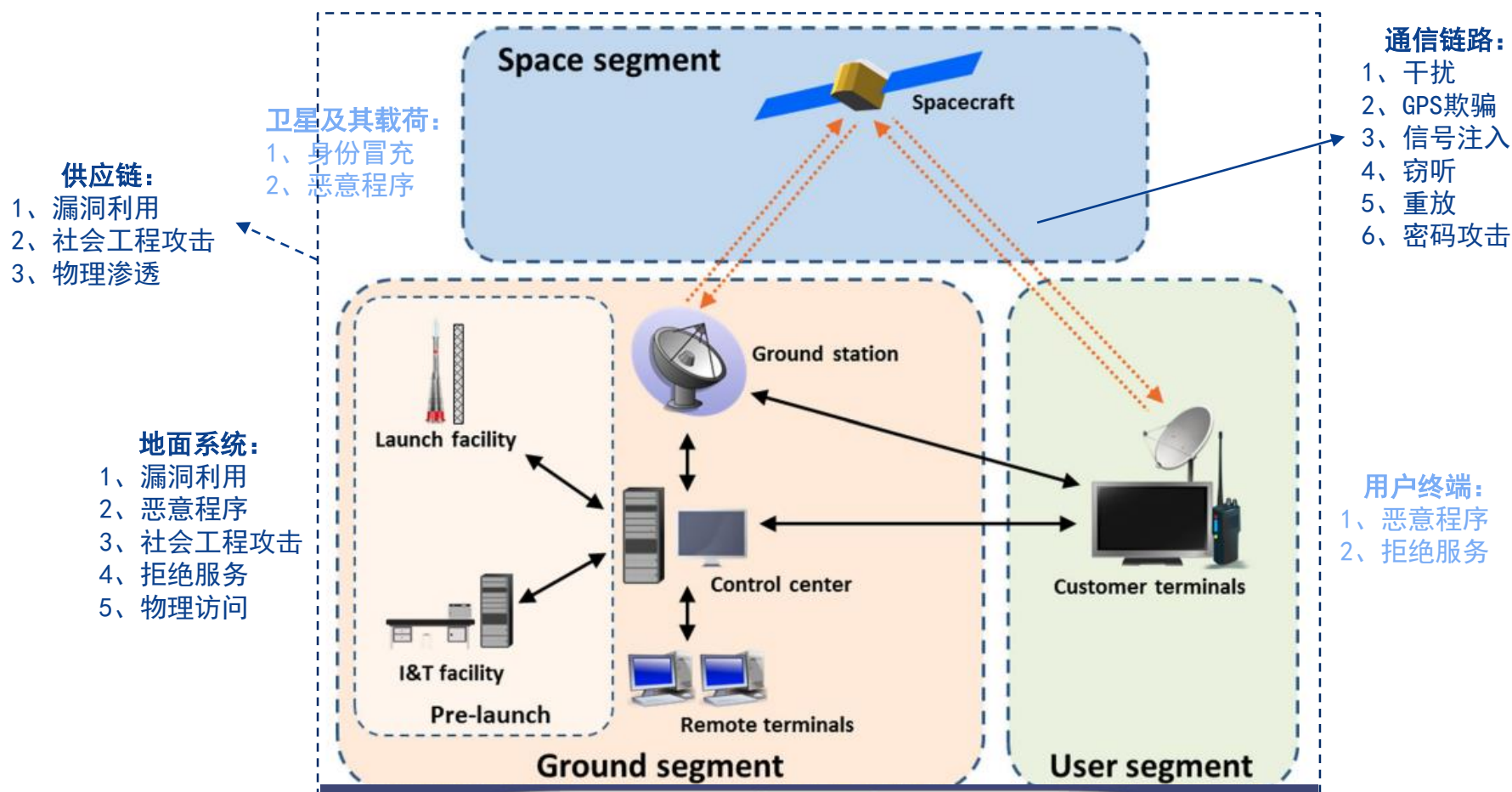
图表：卫星攻击威胁分类



二、安全域视角：卫星互联网的主要安全威胁

从安全域视角来看，卫星互联网的主要安全威胁涉及通信链路安全、地面系统安全、卫星及载荷安全、供应链安全以及用户终端安全，其中通信链路、地面系统、供应链三大安全域是当前卫星互联网面临的最主要的攻击目标。攻击者除了能够对地面站等地面基础设施、卫星通信链路、供应链发起直接攻击之外，还能间接攻击到卫星及其载荷和用户终端，比如GPS欺骗中黑客直接攻击链路，最终导致飞机、轮船等的导航系统失灵。

图表：卫星互联网面临的主要安全威胁



二、安全域1：通信链路安全

通信链路包括上行链路、下行链路和卫星间链路，攻击者通常利用卫星链路未经过加密的弱点，监听合法用户之间的对话，进行数据窃取、通信拦截等。目前攻击集中在上行和下行链路上，并以干扰技术为主。

图表：通信链路攻击梳理

攻击方式	攻击原理	主要案例
干扰	攻击者利用信号发生器来广播射频信号，压制卫星转发的信号（上行链路干扰）或者压制特定区域内卫星服务的地面用户所需的信号（下行链路干扰），导致信号阻断无法接收或者接收数据不完整甚至错误	2003年，美国指控伊朗通过在古巴放置卫星干扰器，使BBG的美国之音电视台节目无法正常播放 新泽西州一名豪华轿车司机在他的车上安装GPS干扰器，以防止其雇主跟踪车辆，但也对附近机场的导航系统造成干扰
GPS欺骗	攻击者利用射频信号发生器产生伪造的GPS报文信息，利用假信号干扰或替代真实的GPS信号，从而误导飞机、轮船等的导航系统，导致其偏离预定线路	2017年，美国海事管理局报告了针对20多艘黑海海域船只的GPS欺骗攻击，在攻击过程中船只导航工具失灵，期间某一时刻，其中一艘船只导航显示该船位于Gelendzhik机场附近，但实际位置与之相距25海里
链路劫持	用户向可信服务器发送文件下载请求时，请求信息同时被广播给ISP（Internet Service Provider）和攻击者，攻击者会伪装成ISP，给用户发送病毒软件或非预期数据作为应答	2015年，卡巴斯基报告了俄罗斯黑客组织Turla通过劫持卫星链路来盗取数据，Turla在接收到合法用户请求后伪装成ISP进行应答，盗取用户账号、密码等信息
窃听	由于卫星网络传输缺乏加密，攻击者只需要一个低成本的卫星信号接收装置，很容易就能截获卫星互联网传输的内容，并进行数据窃取	1986年，印度尼西亚政府被一家美国卫星成像公司指控在未订阅服务的情况下使用大型卫星接收器截获地球观测图像数据 2009年，伊拉克叛乱分子被指控使用名为SkyGrabber的商业软件产品通过卫星链路拦截美国无人机拍摄的未加密的视频流
重放	受限于卫星平台资源，多数测控链路都没有抗重放攻击的功能，攻击者可以将之前拦截并记录的指令向目标卫星重复发送。若重放指令未被识别并丢弃，则卫星将重复执行操作导致卫星天线指向错误或运行偏离预定轨道	-
密码攻击	卫星通信经过加密后，攻击者可以运用缓存碰撞时间攻击等技术破解出对应的明文，获取通信信息	1993年，一群黑客通过解码器卡共享方案在公寓大楼内分发BSkyB卫星频道

二、安全域2：地面系统安全

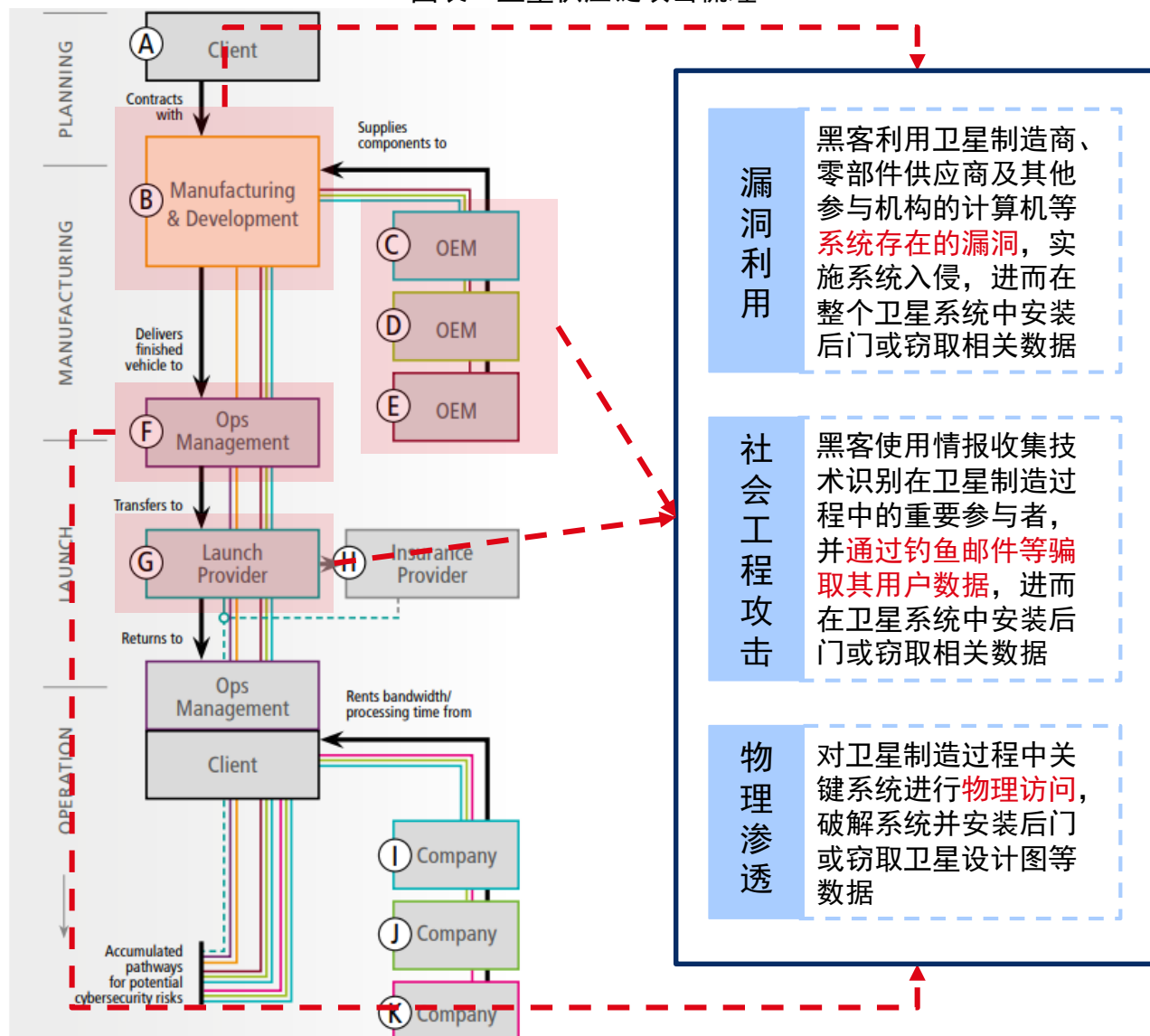
地面系统以地面站为主，地面站作为用户与卫星之间的桥梁，能够接收卫星的运行状态等数据以及转发的用户数据并向卫星发送数据，同时通过控制中心发送控制信号。攻击者通常利用地面计算机存在的漏洞或后门，实施入侵，进一步控制卫星运行，攻击方式包括漏洞利用、社会工程攻击、拒绝服务等。

图表：地面系统攻击梳理

攻击方式	攻击原理	主要案例
漏洞利用	黑客利用地面站使用的计算机系统或网络存在的漏洞，侵入地面站系统，并向卫星发送恶意命令来控制卫星	2007年，美国Landsat-7卫星遭到长达12分钟干扰，2008年美国Terra AM-1地球观测卫星也遭到2分钟的干扰，经调查可能是黑客利用挪威一家卫星地面站系统的漏洞实施入侵，控制卫星 今年3月，黑客Lockbit利用系统网络中的漏洞成功勒索了火箭零件制造商Maximum Industries，使其泄露3000张经SpaceX认证的工程图纸
恶意程序	以木马为例，它可以伪装成合法的应用程序，以诱骗用户下载并安装使用，进而渗透系统，攻击者借此能够窃取用户信息	1987年，德国计算机黑客在全球计算机网络Span中植入了特洛伊木马程序，进而在特权用户登录卫星控制系统时窃取其账号和密码等信息，造成数据泄露 赛门铁克于2017年报告了Thrip间谍组织试图通过恶意程序感染能够监视和控制卫星的计算机系统
社会工程攻击	黑客使用情报收集技术识别拥有地面站系统较高访问权限的关键人员，并通过钓鱼邮件等骗取其用户数据，进而控制卫星	-
拒绝服务	攻击者通过捕获卫星信号进行分析，并将篡改后的频谱信号不断发送给卫星，大量合法的虚假请求占用卫星带宽资源，使卫星无法对其他用户提供服务	俄乌冲突爆发时，美国卫星运营商Viasat遭到有针对性的DDoS攻击，攻击者控制大量设备集中访问网络，导致多家卫星互联网运营商中断服务，数万名卫星网络用户断网
物理访问	攻击者可以带走服务器慢慢破解密码，或者安装硬件键盘记录器窃取操作记录，或是使用外部存储器启动系统并读取硬盘上的未加密数据等	-

二、安全域3：供应链安全

图表：卫星供应链攻击梳理



卫星供应链是黑客的重要攻击入口点，目前针对卫星供应链的攻击包括漏洞利用、社会工程攻击和物理渗透，其中：

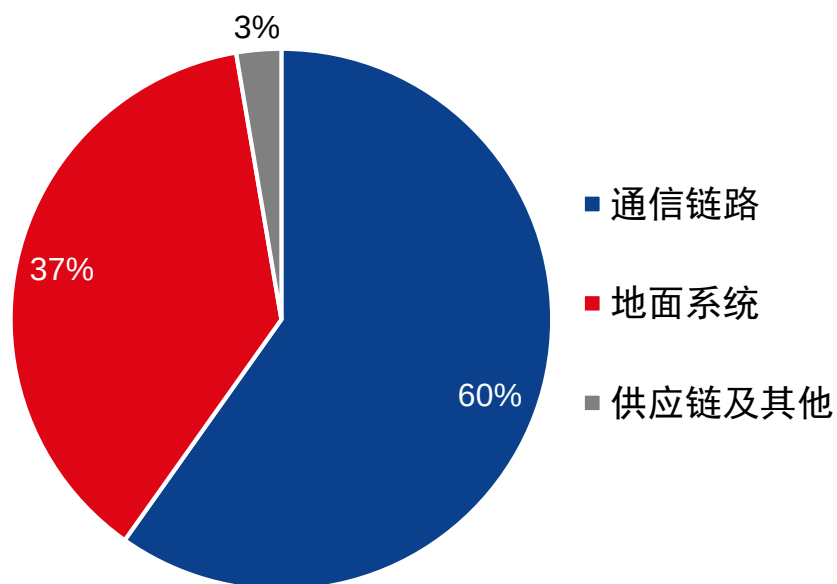
- 1) 卫星系统具有高复杂性和高集成度的特点，卫星系统由众多供应商的数千个软硬零部件组成，在零部件的任何阶段都有可能出现漏洞，导致卫星供应链成为了黑客关键的攻击入口点；
- 2) 更严重的是，许多供应商只重视经济效益，对产品安全性和可靠性的把控极为松散；
- 3) 此外，黑客组织也会针对供应商、卫星制造商、第三方机构实施安全攻击，在软硬件中留下后门。

二、攻击集中在链路侧和地面侧

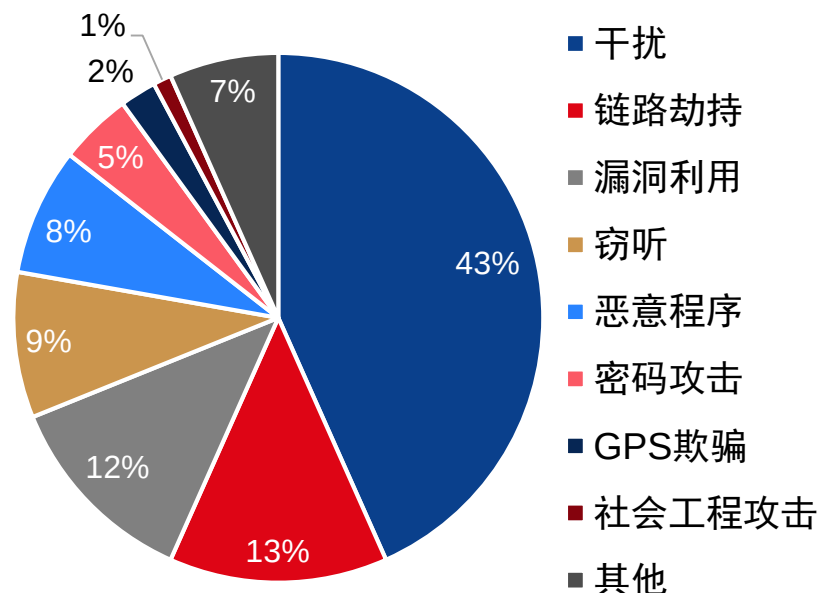
从安全域的角度，卫星互联网安全攻击集中在链路侧和地面侧，数量占比分别为60%和37%。卫星通信链路存在未加密或加密性弱的特点，易被攻击者利用。其次，地面系统包括地面站、数据中心等，覆盖面较广，且地面基础设施云化趋势下增加了新的攻击点，而各类地面设施中的计算机、网络等系统中存在漏洞，易被攻击者利用。

在攻击手段方面，干扰、链路劫持、漏洞利用最为常见。其中，干扰攻击占比超过四成，具有低门槛、低成本的特点，在攻击对象附近放置卫星干扰器即可发动攻击，目前多见于各国政府之间进行对抗时，在边境处放置干扰器以对电视广播、导航系统等造成干扰。

图表：安全攻击集中在链路侧和地面侧



图表：干扰、链路劫持、漏洞利用是常用手段

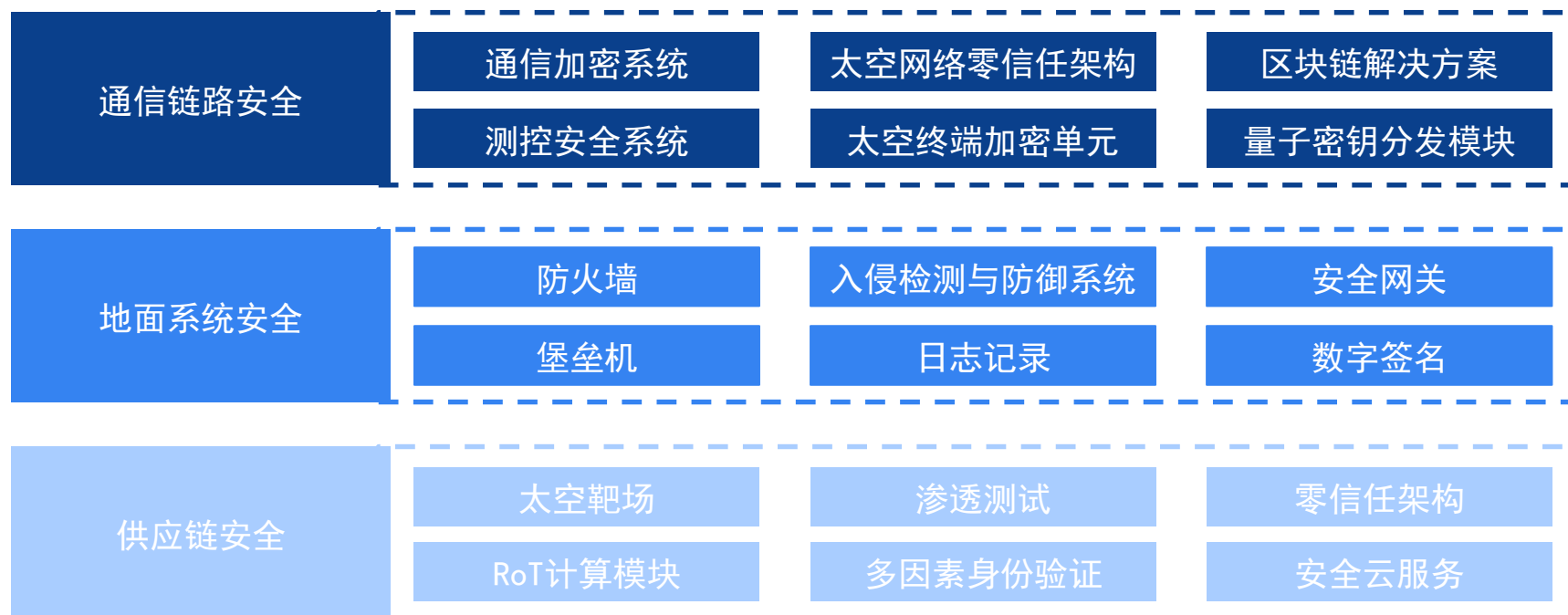


三、安全域视角：三大安全子领域

卫星互联网安全分为通信链路、地面系统、供应链安全三个子领域：

- 1) 通信链路安全：涉及上行链路、下行链路和卫星间链路的安全，以加密与认证产品为主；
- 2) 地面系统安全：产品种类较多，既包括防火墙、安全网关，又包括适用于卫星互联网的星载入侵检测与防御系统、星载日志系统等；
- 3) 供应链安全：主要涵盖卫星系统开发的安全性、后续测试和验证以及供应商、第三方机构等的安全管理，产品包括太空靶场、多因素身份验证等。

图表：卫星互联网安全概念范畴



三、技术视角：以加密为主

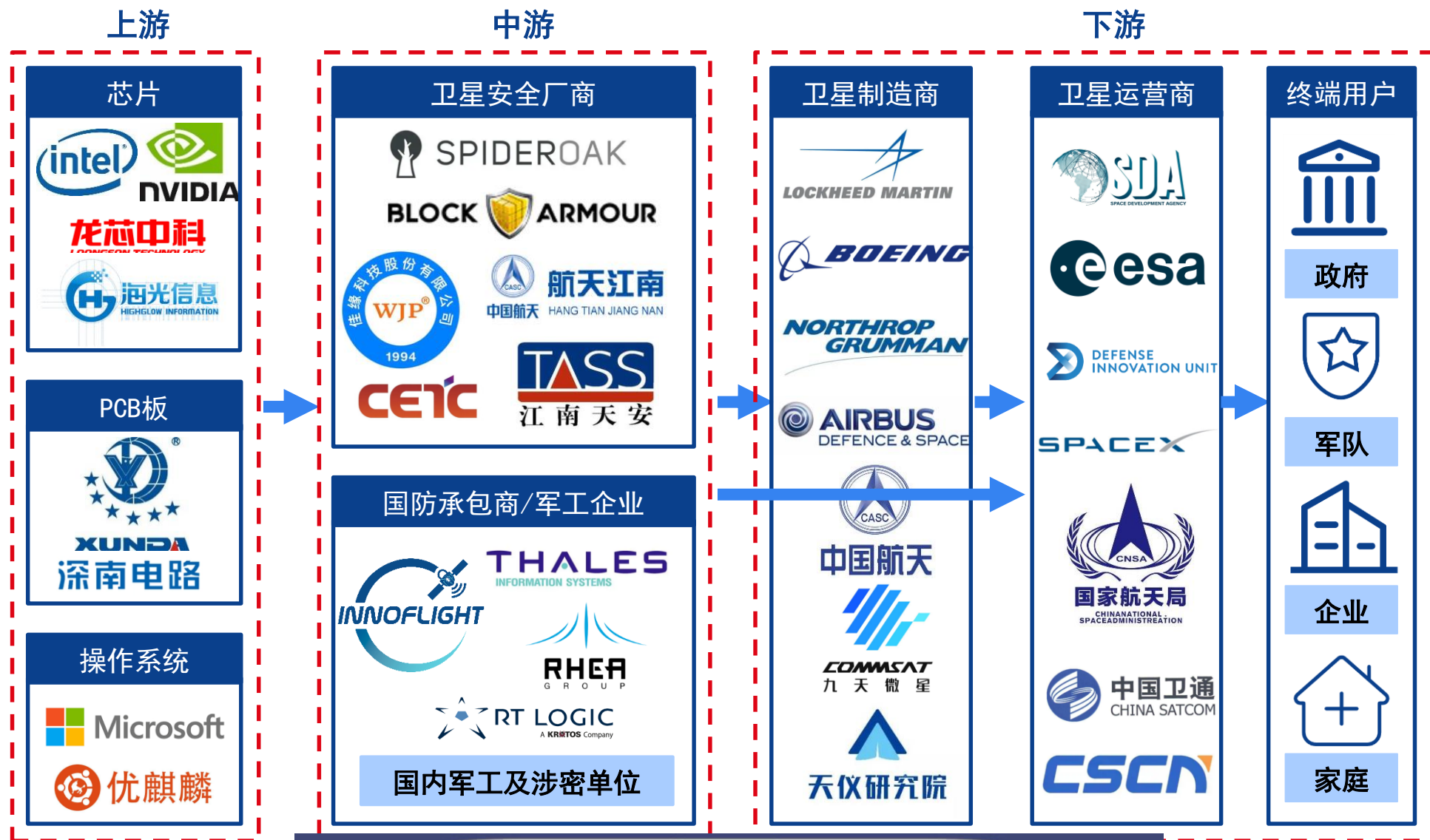
卫星互联网安全产品主要包括通信加密、入侵检测与防御系统、网络攻击弹性测试、供应链风险管理、日志记录等，其中加密是第一道防线，也是最重要的防御手段。

图表：卫星互联网安全概念范畴

防御手段	主要描述
通信加密	对卫星发送和接收的数据进行加密，是空间系统内部的第一道防线。加密以安全协议与密码算法为核心技术支撑，用以实现认证、密钥协商、机密性保护、完整性保护和抗重放攻击的功能，卫星数据加密系统一般包括密钥管理中心和终端加密设备
入侵检测与防御系统	入侵检测与防御系统包括入侵检测系统（IDS）和入侵防御系统（IPS）。其中，IDS同时部署在地面和卫星上，采用基于签名和基于机器学习的异常检测技术，负责对遥测、命令序列、命令接收状态、卫星运行状态等进行监控，如果检测到异常，则进行报警或通知IPS；IPS集成到星载航天器故障管理系统（FMS）中，一般采取简单的基于规则的检测技术，主要负责在出现异常时采取措施，包括切换到冗余侧、隔离命令序列停止可疑单元
网络攻击弹性测试	网络攻击弹性测试是在设计阶段就考虑空间系统对常见网络攻击的弹性，以提高卫星系统的安全性，属于预防措施。网络攻击弹性测试是指开发人员在现实环境中精确复制他们的航天器、地面站和通信网络，并模拟真实的网络攻击，最后由网络专家评估其脆弱性
供应链风险管理	针对供应商和提供软硬件产品或技术的第三方机构，设置严格评估和管理流程，确保每个软硬件的安全性和可靠性，具体措施包括：1）使用安全编码标准以减少意外的软件弱点，2）使用静态和动态源代码分析工具进行安全性评估
日志记录	日志记录主要用于收集和存储数据，为其他安全工具分析系统事件奠定基础。卫星和地面都应该独立记录命令执行数据以便交叉验证。日志应记录命令接收器的输入参数等指标，用于异常调查
信任跟/RoT（root of trust）	RoT概念应包含在卫星设计中，是指计算模块能够访问其信任的函数和命令。RoT计算模块能够验证设备自身的代码和配置，保证系统在安全的硬件中运行
数字签名	软件和硬件的更新应使用数字签名进行验证，保护其内容隐私并验证其完整性和真实性

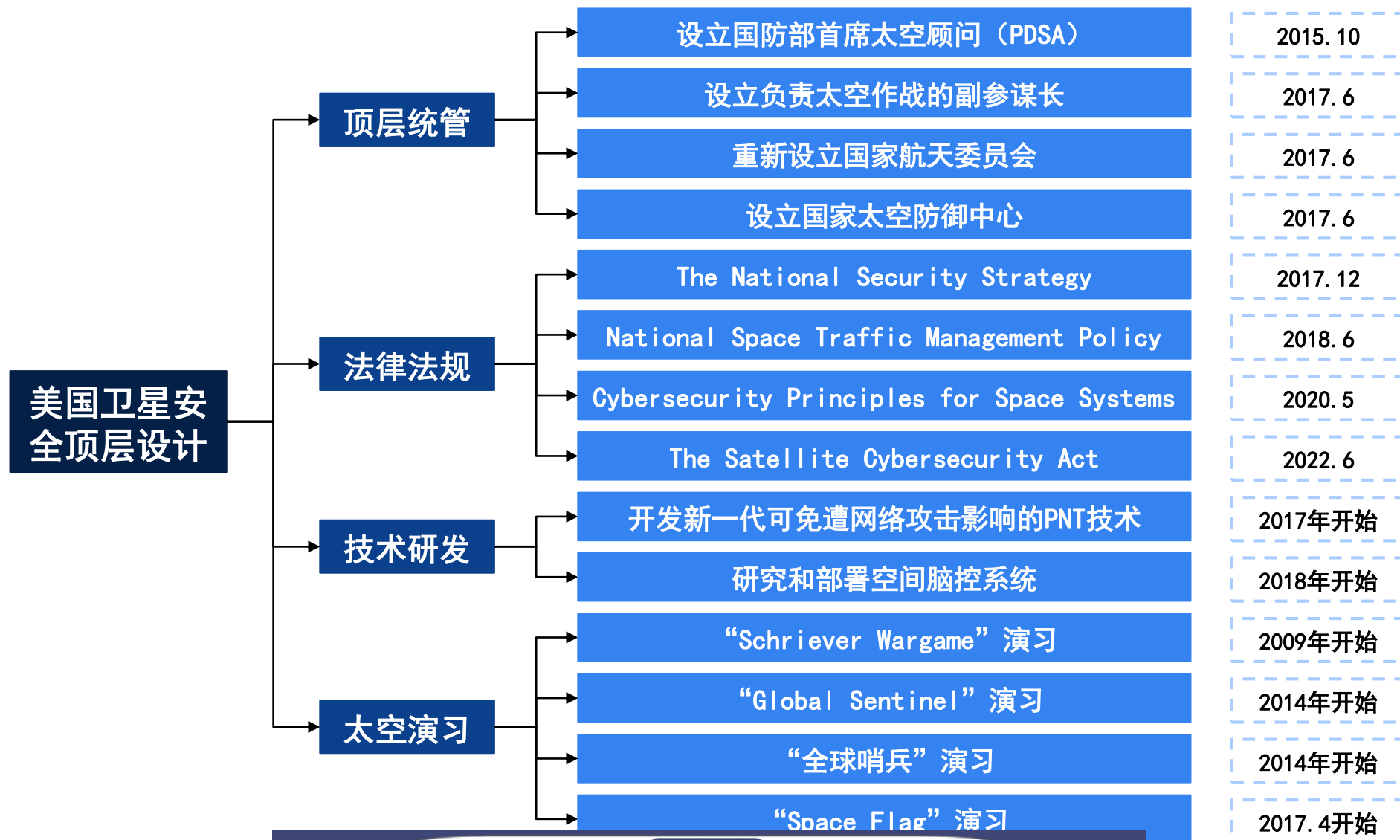
四、卫星互联网安全产业链

图表：卫星互联网安全产业链



四、海外借鉴：美国卫星安全的顶层设计

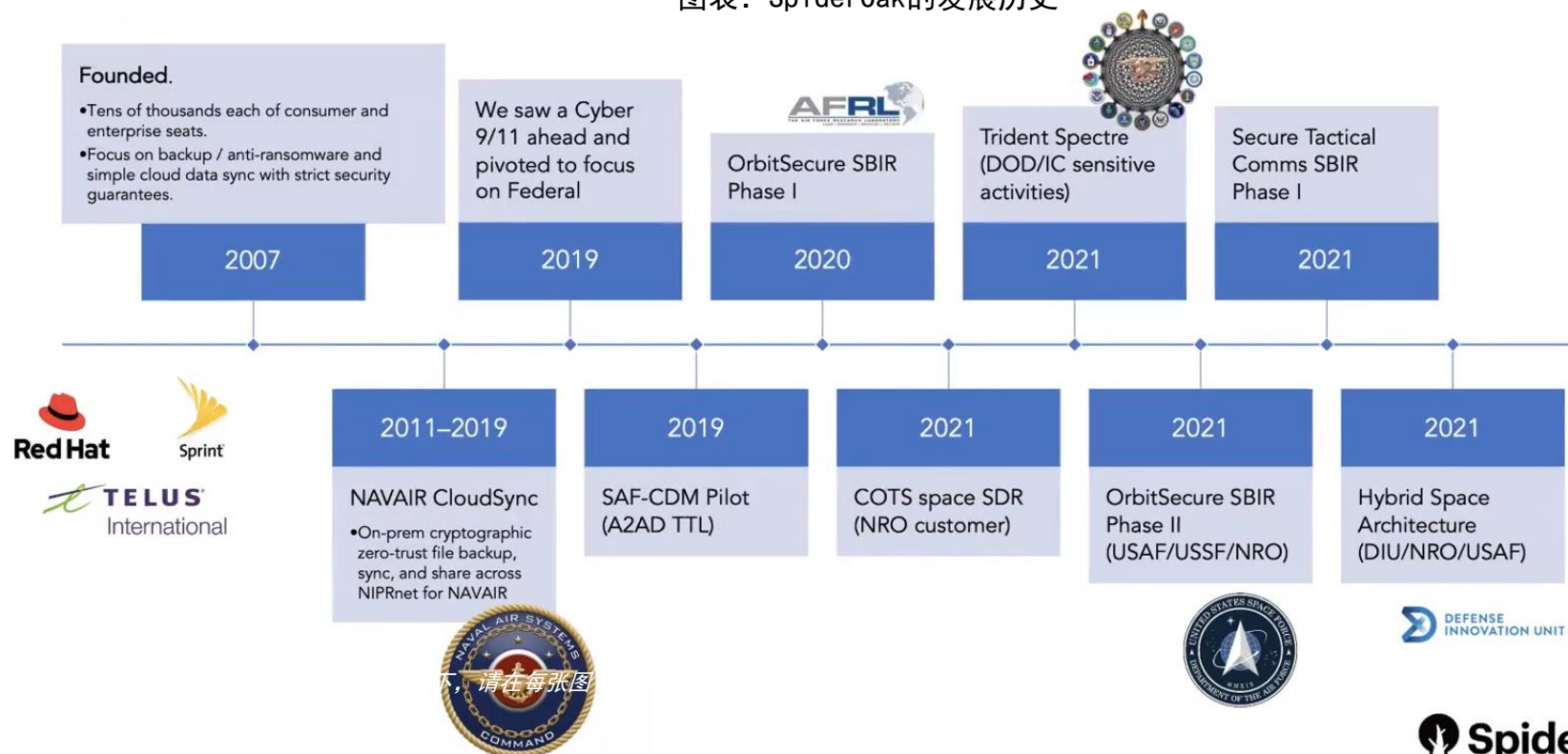
图表：美国卫星安全顶层设计



四、SpiderOak：太空网安先行者

SpiderOak是全球太空系统零信任网络安全领域的领导者和先行者，标杆客户优势显著。SpiderOak成立于2007年，总部位于美国，以加密的私人备份程序起家。公司已完成了1640万美元的C轮融资，截至目前，投资者包括雷神、埃森哲和Stellar Ventures。相较于其他卫星安全厂商，SpiderOak在标杆客户方面处于领先地位，目前已突破多家关键的美国军方机构和国防承包商客户，包括美国海军航空系统司令部（NAVAIR）、美国国家创新部门（DIU）、美国太空发展局（SDA）以及全球最大的军工企业洛克希德马丁，其中，公司于2022年3月与洛克希德马丁签署协议，允许其使用公司的OrbitSecure零信任架构软件并与公司合作将其集成到卫星网络中，公司又于2023年10月与SDA签署协议，SDA将把公司的OrbitSecure软件集成到正在开发的地面控制系统中。

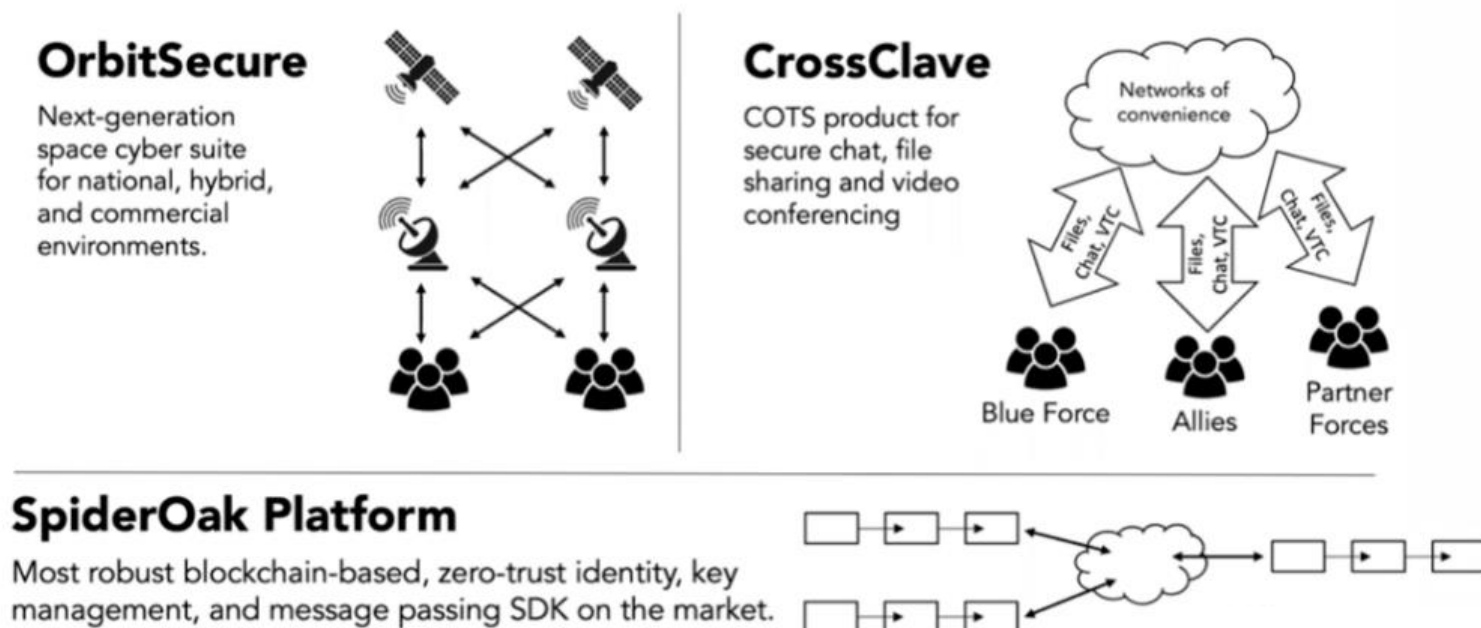
图表：SpiderOak的发展历史



四、SpiderOak：太空网安先行者

2011年SpiderOak便突破美国海军航空系统司令部客户，并在此之后专注于为美国航空领域的军方客户提供零信任安全解决方案。一方面，2011年开始公司持续进行产品迭代，围绕航空安全尤其是卫星网络安全逐渐形成了以OrbitSecure零信任架构软件为代表的丰富的产品组合，还包括CrossClave零信任通信和协作产品、SpiderOak Platform加密程序开发平台等。另一方面，公司基于美国海军航空系统司令部提供安全解决方案近十年的积累，2020年开始快速拓展SDA等统筹太空事务的国家机构以及洛克希德马丁等大型卫星制造商。SpiderOak也在2023年被Via Satellite评为当年卫星领域10家最热门的公司之一。

图表：SpiderOak的主要产品



四、泰雷兹：伽利略系统头部网安供应商

泰雷兹集团是全球十大军工巨头之一，是欧洲伽利略系统的头部网安产品供应商。泰雷兹成立于1968年，以电子元件、通信和半导体相关业务起家，80年代开始转向国防电子和国防航空领域，持续深耕近四十年，目前公司形成了国防与安全、航空航天、数字身份与安全三大业务板块，2022年总营收达到176亿欧元。2023年，公司与欧洲宇航局签订了两份总价值超过6000万欧元的合同，为伽利略二代系统提供安全解决方案，包括网络安全规范和设计、基础设施安全监控。

公司加密产品在众多国防承包商中保持领先，公司的太空安全产品包括加密设备和攻击检测系统两类，其中，公司具有强大的密钥管理能力，在Modor Intelligence发布的EKM市场调研报告中位列第一梯队，而得益于对数据加密龙头Gemalto和Vormetric的收购，公司Mistral等加密设备在加密性能、可靠性、灵活性等方面保持领先。

图表：泰雷兹集团的太空安全产品

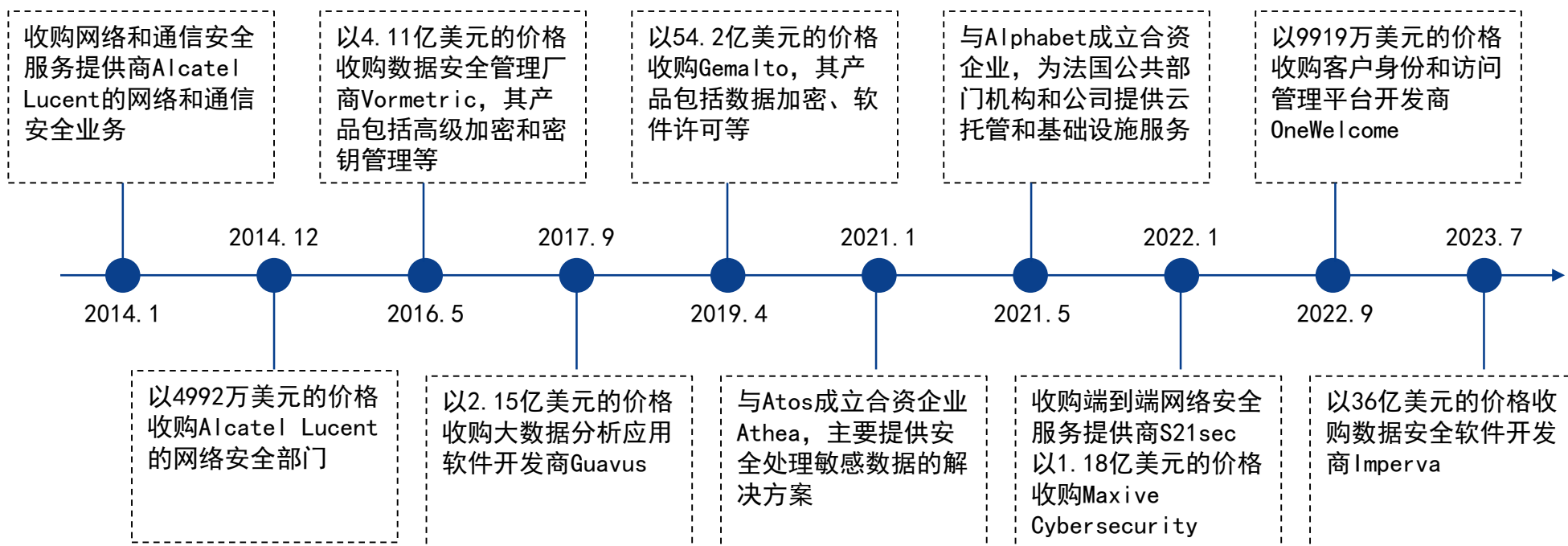
产品	简介
BBKME	一种黑匣子密钥管理设备，用于在GCC（地面控制中心）、GSS（伽利略传感器站）和卫星之间传输密钥材料，能够安全地存储和分发不同长度的黑色和红色密钥数据
Cybel's KMC Space	一种专门为保证Galileo PRS用户的通信安全而设计的加密密钥管理系统，允许用户1）生成、分发、准备和批量导入加密密钥，2）离线（通过外部存储设备）和在线（通过安全 TLS 网络）分发密钥，3）在易于使用的平台上管理密钥
Elips-SD	一种安全网关，该解决方案适用于任何类型的现有网络，利用了安全二极管的特性，可确保从一个网络到另一个网络的单向数据流，提供全面的保护，防止与流量传输相反的方向上的数据泄露
Mistral	一套独特的加密设备，旨在保护通过IP网络（例如互联网或运营商网络）传输的最敏感数据。该解决方案适用于任何规模的新网络和旧网络，非常适合关键国家IT基础设施内的小型 and 大规模部署
Cybel's Sensor	一种网络攻击检测系统，部署在信息系统的关键领域，根据泰雷兹研究实验室开发的检测规则和行为分析算法来识别攻击。CYBELS Sensor采用模块化架构，面对新的威胁和监管变化能够灵活调整
Cybel's Analytics	一个集成了多种攻击检测和取证方法的分析平台，用于实时检测和追踪最复杂的网络攻击，包括以前未知的威胁。该平台结合了基于现有威胁分析的实时威胁检测（网络威胁情报）和主动搜索前所未有的网络攻击（“冷”调查或狩猎），检测高级持续威胁的时间从平均二个月缩短到几天

四、泰雷兹：伽利略系统头部网安供应商

背靠法国政府，与欧洲宇航局近二十年保持紧密合作。公司第一大股东是法国政府，持股比例35.15%，第二大股东是法国的军工巨头达索，持股比例29.92%，两大股东均是欧洲本土机构，为公司进入伽利略供应链形成背书。此外，公司与欧洲宇航局多年的合作积累，是伽利略系统的重要供应商，也为业务拓展至安全产品奠定基础。

不断并购网安公司，持续丰富安全产品矩阵并强化安全能力。2014年开始，泰雷兹陆续收购Altecal Lucent、Vormetric、Guavus、Gemalto等知名网安厂商，快速布局网络安全领域，形成了通信防护、身份与访问控制、安全检测等多种安全能力。其中，头部安全厂商的收购强化了公司在细分安全领域的竞争优势，比如收购数据加密龙头Vormetric和Gemalto，增强了公司的加密能力。

图表：泰雷兹集团持续并购网络安全厂商



四、国内市场：主要卫星安全厂商

国内卫星安全厂商基于企业背景可分为两类：1) 以电科网安和航天江南为代表的国家队，其中，电科网安背靠中国电科，航天江南背靠航天五院，国家队在获取总包项目上具备一定优势，比如电科网安作为总包单位为星网提供密码安全产品，合同金额超过2000万元；2) 以佳缘科技为代表的民营卫星安全厂商，在产品技术和标杆客户等方面各具优势，同样是卫星安全市场的重要参与者。

图表：国内卫星互联网安全厂商情况

厂商	成立时间	背景	上市时间	营收（2022年）	员工人数	主营业务	下游市场
电科网安	1998	央企， 中国电科持股35.14%	2008	34.38亿元	2901	密码系统、网络安全、数据安全	政府、央企、金融、能源、交通、通信
航天江南	2017	央企 航天科技集团五院503所全资子公司	未上市	未披露	26	加密、身份认证、安全网关	政务、金融
佳缘科技	1994	民营企业 王进持股37.68%	2022	2.70亿元	233	信息安全、信息化	军工、医疗、政务
江南天安	2005	民营企业 邓冬柏持股54.55%	未上市	未披露	194	商密产品	政府、金融、电信、医疗、互联网
天御云安	2018	民营企业 郑重持股71.1%	未上市	未披露	27	密码产品	军工、公检法、能源、医疗、轨道交通
数盾科技	2002	民营企业 朱云持股31.22%	未上市	未披露	144	密码产品	能源、交通、政务、医疗、军工、金融
国领科技	2017	民营企业 张建国持股98%	未上市	未披露	9	密码产品、安全网关	政务、运营商、视频会议领域

四、厂商竞争力体现在产品能力和标杆客户上

国内卫星互联网安全厂商的竞争力主要体现在产品能力和标杆客户两方面。1) 卫星安全产品需要具备在太空环境中的加密、认证与检测高可靠性：由于太空环境下具有高辐射、极低温或极高温等特点，相较于地面环境，容易引发半导体器件单粒子翻转等一系列问题，进而导致安全设备失效，因此卫星安全厂商需要具备卫星抗辐照软硬件平台开发、星际链路加密等相关技术，并能够满足部署在卫星上的一系列硬性要求；2) 标杆客户是企业快速横向拓展市场的基础，其中，电科网安、航天江南的产品已进入中国星网、中国卫通等大型卫星运营商供应链，且佳缘科技也成为了通信数传网安领域主要军工厂的供应商，在标杆客户方面已经建立一定的先发优势。

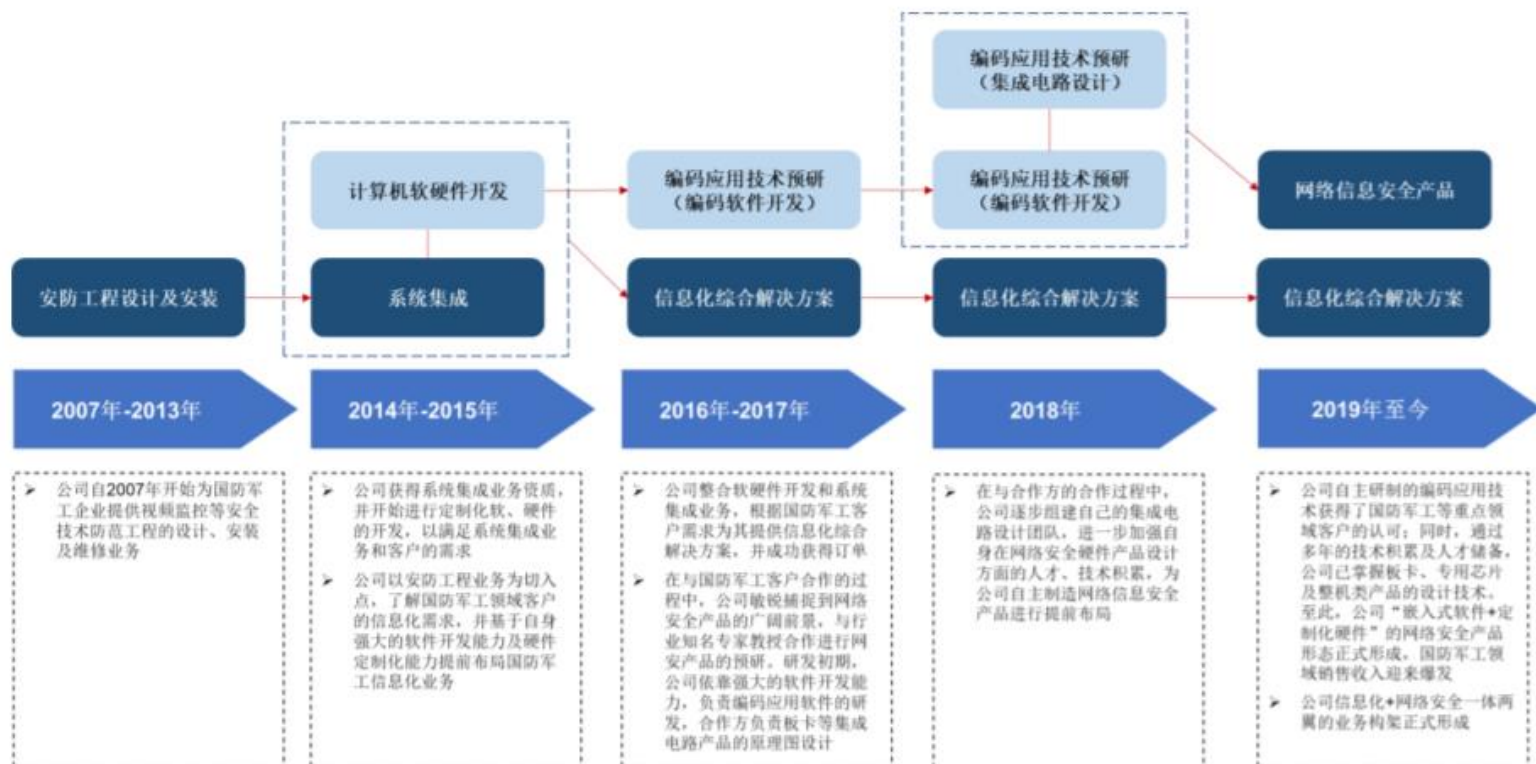
图表：国内卫星互联网安全厂商对比

厂商	产品	部署位置	产品描述	客户
电科网安	星网密码方案	未披露	未披露	中国星网
航天江南	卫星互联网地面密码机系统	地面站、用户终端	包括控制面密码机和用户面密码机，同时支持窄带、宽带技术体制	中国卫通
	量子安全服务系统	地面站	提供量子密钥的分发和密码应用服务	
	卫星网络地面测控系统	地面站	采用虚拟化技术，每个虚拟化测控安全服务分别对应一个卫星的测控加解密处理	
	终端安全模块	地面站、用户终端、卫星	包括窄带终端安全模块、宽带终端安全模块和星载综合安全模块	
佳缘科技	信息安全类板卡	地面站、用户终端	全国产化设计；支持一次一密	保密领域 通信数传 网安产品 军工厂
	四型小型芯片	地面站、卫星	集成CPU、Flash存储器、编码算法芯片的小型高息能信息安全系统SIP成品	
	中低速测控安全系统	地面站	设备形态为1U、2U机箱；全国产化设计	
	高速数据传输安全系统	地面站	设备形态为2U机箱；全国产化设计；支持千兆万兆网络传输	
	基于GPU的高速数传处理平台	地面站	设备形态为4U机箱；采用GPU架构及智能化调度算法	
江南天安	天安天链专线密码机	地面站、用户终端	时延<1ms；支持SM2、SM3、SM4、AES、ZUC、RSA加密算法；支持一次一密；支持2层、3层、4层加密	未披露
天御云安	链路加密VPN	地面站	支持SM2、SM3、SM4加密算法；支持实时更新加密设备的密钥信息，密钥更新周期可配置	未披露
数盾科技	卫星通信加密系统	地面站	时延<10ms；采用SM1算法；密钥定期更换	未披露
国领科技	LineSec链路密码机	用户终端	时延<25μs；支持国密加密；全国产化；支持二层网络加密	未披露

四、佳缘科技：国内卫星通信加密龙头

佳缘科技以自研编码技术为核心，依托信息化业务的技术和客户积累，通过打造网安领域的军工标杆客户案例，快速成长为国内卫星通信加密领军者。佳缘科技成立于1994年，以广告业务起家。2002年开始逐渐转型为信息化综合解决方案服务商，着力研发计算机软硬件产品，并布局医疗、军工、政务三大行业。2016年开始研发编码技术和编码软件，并在2019年凭借芯片、板卡、整机等产品正式切入网络安全领域，并在当年获得军工客户的卫星安全相关订单，受托研发卫星测控平台。在标杆效应影响下，公司随后陆续获得其他军工客户的网安订单，涵盖星载、机载和地面设备，网安业务规模也迅速扩大。目前，公司已形成“网络安全+信息化”的一体两翼业务架构，2022年总营收达到2.70亿元，其中网络安全业务收入2.13亿元。

图表：佳缘科技发展历程



四、佳缘科技：密码产品全覆盖

佳缘科技以密码安全产品为主，包括板卡、芯片、整机全形态，用于星载、机载和地面设备场景中。

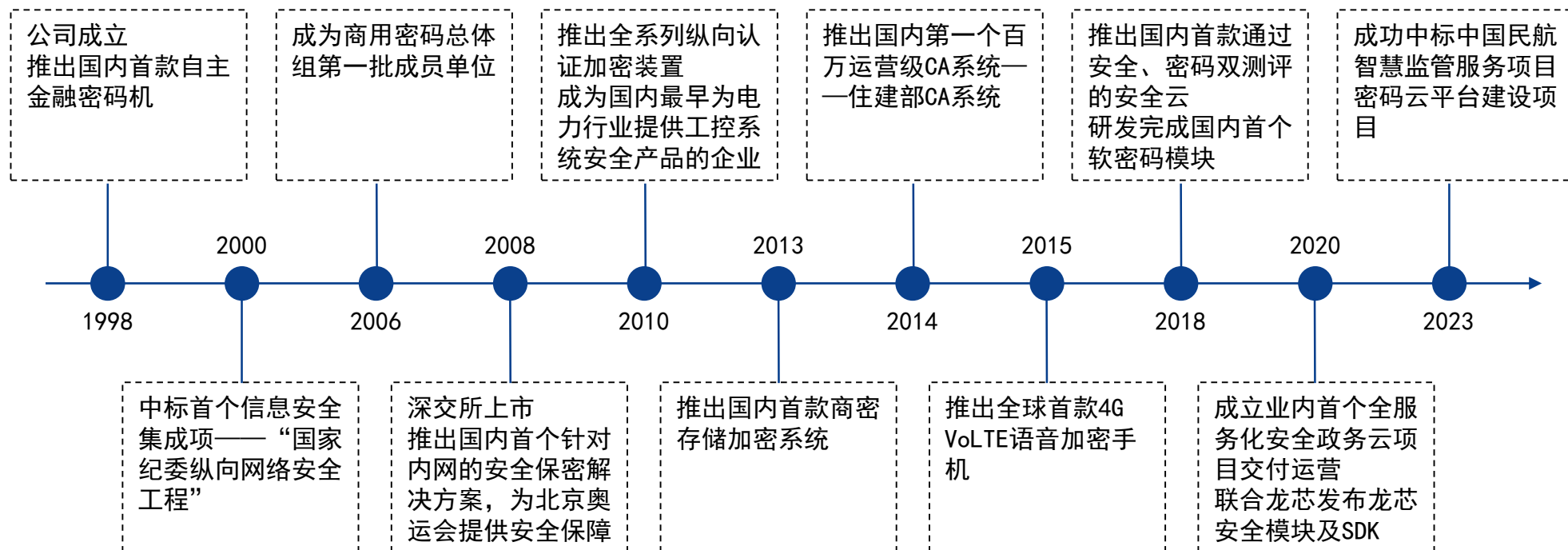
图表：佳缘科技信息安全产品

产品形态	产品	产品简介
板卡	计算平台类板卡	采用国产龙芯1B CPU和千万门级复旦微电子 FPGA 构成处理系统，通过对PCIe总线的 DMA 实时控制，完成基于6.4Gbps 并行超流水信息安全处理。此产品主要用于高速网络的数据传输安全防护
	信息安全类板卡	开机认证模块，采用国产化 CPU 芯片和航空连接器,实现装备合法用户身份认证，关键参数分量存储和在线授权，一次验证更新一次安全参数，防止非法用户网络入侵；同时防止软件被盗版。此产品主要运用于地面终端设备
	信号处理管理平台类板卡	采用国产化 P2020 双核嵌入式PowerPC 通信处理器和国产大规模 FPGA，实现对数十万量级用户进行可信根防护，远程在线授启，身份认证，关键参数安全防护和在线分发，状态监控管理。此产品主要用于信道安全防护
芯片	四型小型芯片	一款集成 CPU、Flash 存储器、编码算法芯片的小型高息能信息安全系统SIP成品
	三型物理噪声源芯片	用于信息系统的随机数提取，确保随机数的产生和应用。目前，此产品主要应用于数字传输控制相关设备
整机	高速数据传输安全系统	设备形态为 2U 机箱，通过设计自主可控的硬件平台，构建高速数据传输安全设备、数传安全单检设备、地检设备以及模拟器构成的高速数据安全系统，完成千兆万兆高速安全传输
	中低速测控安全系统	设备形态为 1U、2U 机箱，其通过设计自主可控的硬件平台，构建以测控安全设备，测控安全单检设备，地检设备以及模拟器构成的中低速测控安全系统
	检测台安全防护系统	设备形态为 1U 机箱，通过构建服务器端/客服端授权访问，身份控制和安全防护策略，实现了对专用设备的身份唯一性认证，安全存储和防信息攻击，防止专用软件被非法复制
	视频安全传输系统	使用国密算法、国产化 CPU 平台实现信息安全防护。目前，该系列产品应用于国家各类办公网络视频系统传输控制

四、电科网安：背靠中国电科，密码基因深厚

背靠中国电科，电科网安密码基因深厚，是国内商用密码安全领域的先行者和领导者。电科网安是中国电科集团旗下子公司，成立于1998年，是国内首家推出金融数据密码机的公司。后以密码技术为核心，一方面将密码安全能力从金融拓展到军队、党政等行业，另一方面快速布局数据安全、网络安全等领域以及云安全、物联网安全、卫星互联网安全等新场景。2022年公司总营收达到34.38亿元，其中密码系统收入13.35亿元，网络安全收入18.83亿元，数据安全收入2.19亿元。

图表：电科网安发展历程



四、电科网安：成功进入星网安全供应链

电科网安已成功进入星网计划密码安全产品供应链。10月24日，电科网安成功中标中国星网2013.49万元大订单，为星网计划提供密码安全方案，提供若干款上星密码产品。星网计划未来累计将发射1.3万颗卫星，对标SpaceX，电科网安作为星网密码的总体单位，并且背靠中国电科，将持续收获大价值量订单。

图表：电科网安密码产品

密码产品

金融数据密码机

金融数据密码机是由卫士通自主研制，通过国家主管部门鉴定的安全密码设备，为金融业务系统提供数据机密性、

服务器密码机

服务器密码机具有数据加解密、签名、验签、MAC、杂凑等功能，支持SM1/SM2/SM3/SM4/SM9及ZUC国密算法，

数字证书认证系统

数字证书认证系统是卫士通研制的一套公钥基础设施解决方案。系统基于PKI关键技术，实现了用户注册、审核，密

移动终端密码软卡

移动终端密码软卡移动终端密码软卡| 产品特色安全性高
● SM2签名私钥分割、混淆，协同签名计算时私钥不会出现

密钥管理系统

密钥管理系统是依据国家及行业相关标准规范研制的安全基础设施产品，使用经国家密码管理局批准的密码设备，

商用PCI-E密码卡

商用PCI-E密码卡是由卫士通自主研制的安全密码产品，该密码卡支持国家密码管理局发布的SM1/2/3/4算法，通常嵌

签名验证服务器

签名验签服务器是卫士通依据国密局、工信部、公安部等主管单位的相关标准规范，自主研发的新一代数字签名服

四、规模测算：24-27年有望新增七十亿的规模

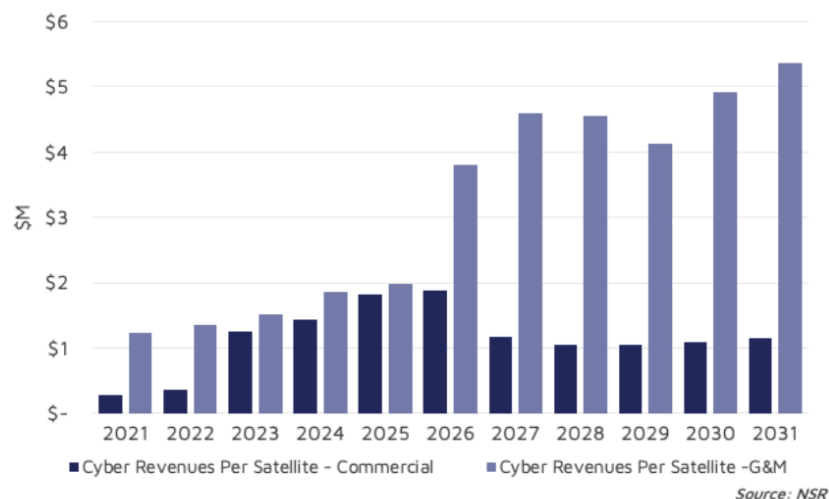
预计2024-2027年中国卫星互联网安全有望新增七十亿元的规模。

- 1) 根据佳缘科技招股说明书，预计在“十四五”期间，卫星安全的总需求约为69-138亿元，即当前平均每年卫星安全市场规模约为14-28亿元；
- 2) 据不完全统计，根据各家公司向国际电联（ITU）递交的申报计划，截止2027年预估我国小卫星数量将达到约1.4万颗；
- 3) 结合NSR对单颗卫星网络安全支出的预测以及卫星制造成本情况，保守假设单颗卫星平均安全支出50万元，即24-27年有望新增70亿的卫星互联网安全相关需求。

图表：中国低轨卫星星座申报情况

公司名称	星座	数量（颗）
中国星网	GW	12922
航天科技	鸿雁	300
航天科工	鸿云	156
银河航天	Galaxy	650
中国电科	天象	120

图表：单颗卫星网络安全支出（百万美元）



- ◆ 卫星建设进度不及预期：卫星建设进度不及预期将直接影响卫星供给
- ◆ 卫星发射进度不及预期：可能会导致未来卫星发射数量增长缓慢
- ◆ 卫星互联网安全需求增长不及预期：可能会导致单颗卫星网络安全支出增长缓慢
- ◆ 市场竞争加剧：卫星互联网安全行业可能会吸引新厂商进入，对现有参与者造成竞争压力
- ◆ 相关政策出台不及预期：政策对卫星互联网安全产业的影响较大，后续政策出台不及预期会对产业发展造成不利影响

公司评级体系

收益评级：

- 买入 — 未来6个月的投资收益率领先沪深300指数15%以上；
- 增持 — 未来6个月的投资收益率领先沪深300指数5%至15%；
- 中性 — 未来6个月的投资收益率与沪深300指数的变动幅度相差-5%至5%；
- 减持 — 未来6个月的投资收益率落后沪深300指数5%至15%；
- 卖出 — 未来6个月的投资收益率落后沪深300指数15%以上。

风险评级：

- A — 正常风险，未来6个月投资收益率的波动小于等于沪深300指数波动；
- B — 较高风险，未来6个月投资收益率的波动大于沪深300指数波动。

行业评级体系

收益评级：

领先大市 — 未来6个月的投资收益率领先沪深300指数10%以上；

同步大市 — 未来6个月的投资收益率与沪深300指数的变动幅度相差-10%至10%；

落后大市 — 未来6个月的投资收益率落后沪深300指数10%以上；

风险评级：

A — 正常风险，未来6个月投资收益率的波动小于等于沪深300指数波动；

B — 较高风险，未来6个月投资收益率的波动大于沪深300指数波动。

分析师声明

方闻千声明，本人具有中国证券业协会授予的证券投资咨询执业资格，勤勉尽责、诚实守信。本人对本报告的内容和观点负责，保证信息来源合法合规、研究方法专业审慎、研究观点独立公正、分析结论具有合理依据，特此声明。

本公司具备证券投资咨询业务资格的说明

华金证券股份有限公司（以下简称“本公司”）经中国证券监督管理委员会核准，取得证券投资咨询业务许可。本公司及其投资咨询人员可以为证券投资人或客户提供证券投资分析、预测或者建议等直接或间接的有偿咨询服务。发布证券研究报告，是证券投资咨询业务的一种基本形式，本公司可以对证券及证券相关产品的价值、市场走势或者相关影响因素进行分析，形成证券估值、投资评级等投资分析意见，制作证券研究报告，并向本公司的客户发布。

免责声明：

华金证券股份有限公司（以下简称“本公司”）的客户使用。本公司不会因为任何机构或个人接收到本报告而视其为本公司的当然客户。

本报告基于已公开的资料或信息撰写，但本公司不保证该等信息及资料的完整性、准确性。本报告所载的信息、资料、建议及推测仅反映本公司于本报告发布当日的判断，本报告中的证券或投资标的价格、价值及投资带来的收入可能会波动。在不同时期，本公司可能撰写并发布与本报告所载资料、建议及推测不一致的报告。本公司不保证本报告所含信息及资料保持在最新状态，本公司将随时补充、更新和修订有关信息及资料，但不保证及时公开发布。同时，本公司有权对本报告所含信息在不发出通知的情形下做出修改，投资者应当自行关注相应的更新或修改。任何有关本报告的摘要或节选都不代表本报告正式完整的观点，一切须以本公司向客户发布的本报告完整版本为准。

在法律许可的情况下，本公司及所属关联机构可能会持有报告中提到的公司所发行的证券或期权并进行证券或期权交易，也可能为这些公司提供或者争取提供投资银行、财务顾问或者金融产品等相关服务，提请客户充分注意。客户不应将本报告为作出其投资决策的惟一参考因素，亦不应认为本报告可以取代客户自身的投资判断与决策。在任何情况下，本报告中的信息或所表述的意见均不构成对任何人的投资建议，无论是否已经明示或暗示，本报告不能作为道义的、责任的和法律的依据或者凭证。在任何情况下，本公司亦不对任何人因使用本报告中的任何内容所引致的任何损失负任何责任。

本报告版权仅为本公司所有，未经事先书面许可，任何机构和个人不得以任何形式翻版、复制、发表、转发、篡改或引用本报告的任何部分。如征得本公司同意进行引用、刊发的，需在允许的范围内使用，并注明出处为“华金证券股份有限公司研究所”，且不得对本报告进行任何有悖原意的引用、删节和修改。

华金证券股份有限公司对本声明条款具有惟一修改权和最终解释权。

风险提示:

报告中的内容和意见仅供参考，并不构成对所述证券买卖的出价或询价。投资者对其投资行为负完全责任，我公司及其雇员对使用本报告及其内容所引发的任何直接或间接损失概不负责。

华金证券股份有限公司

办公地址:

上海市浦东新区杨高南路759号陆家嘴世纪金融广场30层

北京市朝阳区建国路108号横琴人寿大厦17层

深圳市福田区益田路6001号太平金融大厦10楼05单元

电话: 021-20655588

网址: www.huajinsc.cn