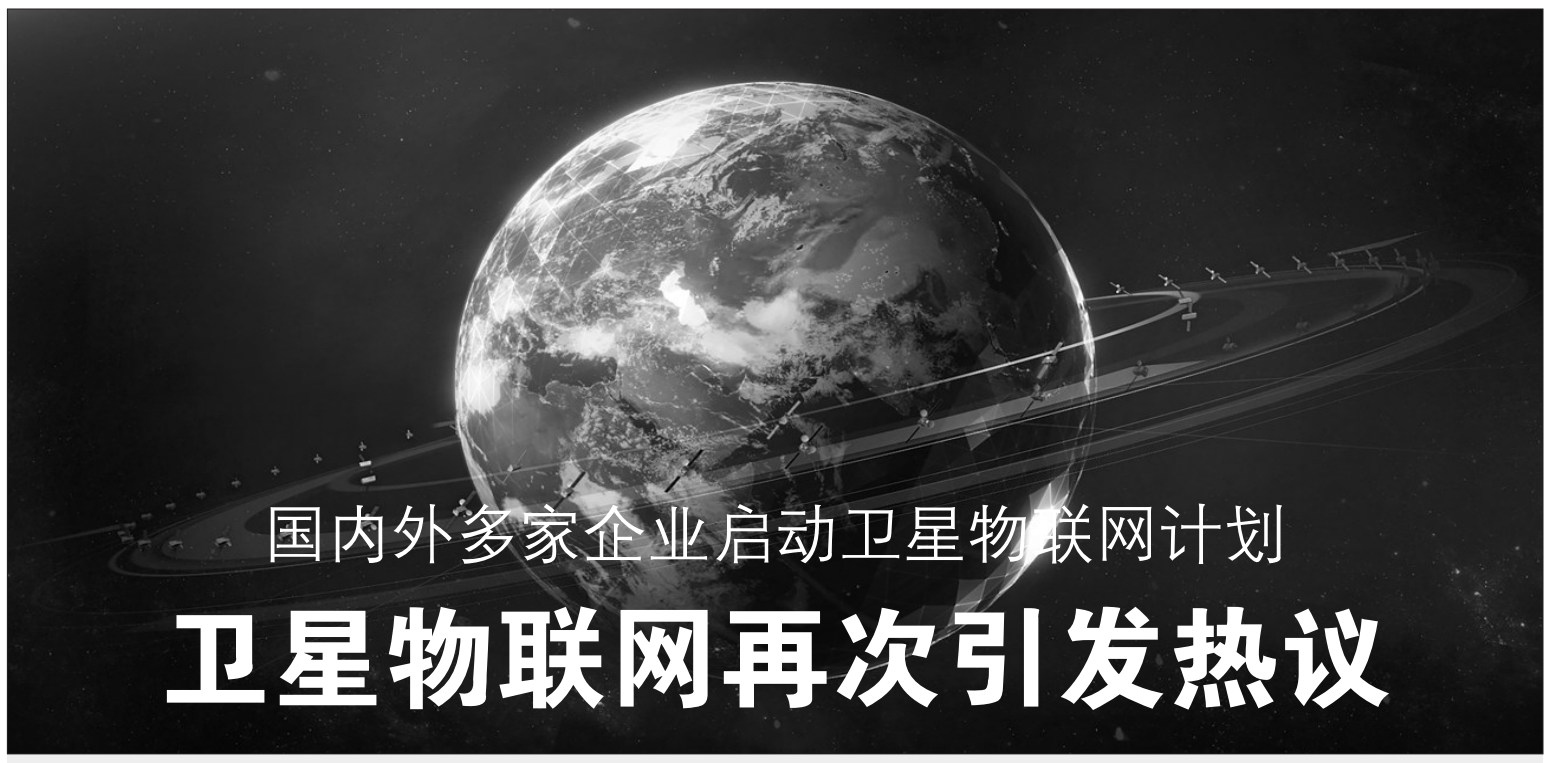

国内外多家企业启动卫星物联网计划

卫星物联网再次引发热议

本报记者 齐旭

日前，联发科宣布成功利用高轨卫星测试了NB-IoT卫星基站的数据传输能力，证明移动网络的技术应用在地球同步轨道卫星也能有效工作，这将为无处不在的全球物联网覆盖提供一种更具经济性的方式。一时间，卫星物联网再次引发热议。

世界银行数据显示，目前地面物联网（IoT）业务在陆地的覆盖率仅为20%，而海洋覆盖率则不到5%。在这些人迹罕至却又需要通信的区域，建设基站和铺设线路的难度大、成本高。这降低了实现“万物互联”的可能性。为突破地面基站覆盖范围的限制，近年来物联网向太空进军的势头开始增强。目前，国内外已有多家企业启动了卫星物联网计划，让卫星物联网市场绽放出了巨大的潜力。

卫星成助力“万物互联”关键一环

移动物联网的快速部署已经成为5G时代乃至未来的重要趋势。

5G时代，万物互联当道。移动物联网的快速部署已经成为5G时代乃至未来的重要趋势。然而，物联网技术需要依靠基站等基础设施来完成区域的覆盖，而这种连续不间断的覆盖需要大量地投资基础设施建设。由于在岛屿、沙漠、海洋等人迹罕至的偏远地区安装基站和铺设光纤线路的难度大、成本高，目前地面蜂窝基站的陆地覆盖率约为20%，而海洋覆盖率则不到5%。

卫星物联网通信技术能够突破因地面基站所不能及而带来的物联网覆盖限制。因此，不受地理环境和气候环境影响，且具备全天候服务能力的卫星通信近年来常常获得业内的青睐。

中国航天科工集团行云工程总设计师刘萧磊对《中国电子报》记者表示，与卫星互联网相比，卫星物联网不追求传输速率。物联网连接的是人与物、物与物，且主要追求的是“广链接”，因此对速率没有过高要求。

根据全球多家咨询机构的预测情况，卫星物联网产业在未来全球物联网生态系统中表现出了巨大的发展潜力。从市场规模来看，美国权威卫星行业咨询公司NSR预测，2022年将有1亿至2亿台物联网设备有接入卫星的需求。麦肯锡公司预测，天基物联网的产值在2025年可达5600亿美元至8500亿美元。

从应用场景来看，农业管理、工程建筑、海上运输和能源行业将成为卫星物联网最重要的应用方向，能够对相关行业的发展模式产生重大影响。在农业应用方面，卫星物联网能够大面积收集农场的土壤成分、温度、湿度等数据。在工程应用方面，卫星物联网能够实现对偏远地区土木工程项目的远程监控。预计到2022年，该市场将以每年25%的增速达到34亿美元。在海运应用方面，卫星物联网能够全程跟踪海上船舶和集装箱，并提高货运的效率。在能源应用方面，卫星物联网可以监控天然气、石油和风能等能源在市场上下游的流动数据，以此得到投资回报比更高的解决方案。此外，水资源监控可以提高缺水地区的水资源利用率，而这也将促进缺水地区的可持续发展。

各国加紧布局卫星物联网计划

以“行云工程”和“鸿雁星座”为代表的低轨卫星物联网星座计划正在稳步推进。

卫星物联网并不是新兴概念。自20世纪90年代末以来，以铱星（Iridium）、全球星（Globalstar）、轨道通信（Orbcomm）为代表的低轨移动星座均展开了各自的物联网计划，并持续推动了应用范围和深度的不断拓展。

近年来，随着商业航天领域的快速发展，可回收运载火箭、“一箭多星”等技术正在持续降低卫星发射的成本，因此利用小卫星及其先进的制造技术来推动流水线的批量生产已经成为行业标配。随着卫星研发和制造成本的不断下降，准入门槛正在进一步降低，而这能够帮助许多初创企业缩短建设周期、降低研制成本并实现快速组网。

轨道通信公司的Orbcomm-2是较早在轨运行的卫星物联网计划。该计划的18颗微型卫星在2012—2015年间全部完成了发射，目前已有数百万个卫星物联设备部署在工业物联网领域。天空和空间全球公司由英国、以色列和澳大利亚三国联合建立，该公司计划在2020年创建200颗由3u立方体星组成的大型星座，前三颗实验卫星已于2017年发射成功。欧盟Eutelsat公司初期部署的物联网星座由25颗卫星组成，第一批四颗卫星预计于2020年至2021年之间发射，入轨后将提供商业服务。

以中国航天科工的“行云工程”和中国航天科技的“鸿雁星座”为代表的低轨卫星物联网星座计划正在稳步推进。今年5月，中国航天科工集团的卫星物联网计划取得进展，“行云工程”的“行云二号”01星、02星两颗卫星全部发射成功。据悉，“行云工程”计划分三个阶段，由80颗低轨通信卫星组成的卫星物联网星座将在2023年前建成。这能够为极地环境监测、地质灾害监测、气象数据预报、海洋环境监测、海上运输通信等多个行业提供应用测试，并为后续卫星物联网的组网奠定基础，以实现真正的全球万物互联。

高、低轨联合提供卫星物联网新型解决方案

高、低轨联合提供的卫星物联网解决方案将成未来卫星物联网发展的趋势之一。

中国航天系统科学与工程研究员战略规划研究部咨询师刘洁在接受记者采访时指出，从轨道分布来看，GEO（高轨）、LEO（低轨）两种轨道配置均被用来提供物联网服务，且各具优势。从SpaceX、亚马逊、OneWeb等新入局的新兴初创企业的星座计划来看，低轨已成为卫星通信计划的“新赛道”。

低轨卫星在卫星通信计划中的优势明显。“低轨卫星传输的延迟更短、路径损耗更小，因此发射成本相对更低。”中国科学院国家空间科学中心空间频谱感知技术研究室副主任闫毅告诉记者。

目前，已有多家互联网企业和卫星运营商提出星座计划，并发射了多颗试验星和业务星以抢占蓝海市场。一时间，低轨空间变得拥挤不堪。根据赛迪顾问发布的《“新基建”之中国卫星互联网产业发展白皮书》，近地轨道可容纳约6万颗卫星。预计到2029年，地球近地轨道将部署约5.7万颗卫星，因此轨位空间将所剩无几。

基于此，高、低轨联合提供的卫星物联网解决方案将成未来卫星物联网发展的趋势之一，而高轨也将在星座计划中释放出更多的潜力和更大的市场空间。2019年8月，澳大利亚物联网企业Myriota与澳大利亚最大的GEO卫星运营商Optus合作，结合高低轨卫星的各自优势来服务于卫星物联网市场。

日前，联发科基于标准NB-IoT芯片开发出了支持卫星功能的设备。该设备通过国际海事卫星组织的Alphasat L波段卫星，已成功与商用GEO卫星建立了双向链路，实现了物联网业务的全球覆盖。国际海事卫星组织产品高级总监Jonathan Beavon先生介绍，此次试验表明，通过小幅修改即可让移动通信技术有效地应用于GEO卫星。这将为混合型全球物联网的覆盖提供一个极具成本效益的途径，同时也能释放出高轨卫星的更多应用价值。”

高、低轨共同发展物联网业务可以打造立体式的物联网服务模式，并为行业提供卫星物联网发展的新解决方案。

“天地一体化”服务仍有待探索

虽然“天地一体”物联网服务的前景被广泛看好，但尚未形成真正成熟的商业模式。

实现卫星和地面设备的互联会涉及地面通信和卫星通信等多种手段的结合，因此这种“天地一体化”的服务需要将二维地面网络与近地三维卫星通信网络进行融合与升级，以此打破通信基础设施由于空间分布不同而导致的业务、服务的隔阂。目前，虽然“天地一体”物联网服务的前景被广泛看好，但尚未形成真正成熟的商业模式。

在赛迪顾问物联网产业研究中心高级分析师刘暾看来，卫星物联网会更多地面向行业用户。卫星物联网具有传输覆盖广、不受地理环境限制、可靠性高等特性，将有望为行业客户提供更加优质的专网服务。然而，由于“天地一体化”网络涉及复杂的通信环境和多个通信系统，其节点比传统的物联网环境更加繁多和复杂。与此同时，由于多个通信系统的运营者不同，更多安全、可靠、高效的网络接口需要被设计出来，以此实现网络深度和安全的融合。这将给整个通信设备产业带来更多挑战。

赛迪智库无线电管理研究所副研究员周钰哲此前向记者表示，这种“天地一体化”网络需要攻克技术难题。要做到地面物联网信号和非地面网络信号的无感切换，一是要重新设计兼容的星地通信协议，比如优化通信系统间的切换流程；二是要考虑智能、高效的频率共享与干扰消除方法，以应对每条链路上不同的数据速率需求；三是要实现卫星等非地面通信设备小型化和轻量化设计，以此避免非地面通信网络的载荷限制。

此外，由于卫星与地面运营商之间的利益关系还有待协调，这种协议体制竞争存在着极大变数。刘洁指出，“天地一体化”的网络融合需要优化资源配置，并平衡好协议体制的竞争，从而更好地发挥作用。目前，国际通信卫星公司、欧洲卫星通信公司、天空完美日星公司等卫星运营服务商在融合服务方面已经进行多种尝试并积累了成功的经验，因此能够向用户提供融合天地通信网络资源的解决方案。

“天基和地基通信服务之间存在的激烈竞争会带来降价和利润率降低等问题。在优化资源配置之后，融合服务能够有效地避免这些问题。”刘洁说。

随着物联网终端数量的跳跃式增长，万物互联的时代已经到来。在当前的应用场景中，很多物联网设备在“上云”时处于“裸奔”状态，这就造成了安全防护机制缺乏、用户隐私泄露和系统安全存在风险等严重问题。在万物互联的时代下，提升物联网设备的安全性是当前的重要任务之一。

万物互联 安全为先

本报记者 张依依

万物互联时代下的海量连接

在数字化转型时代，物联网已经成为了最重要的互联模式。物联网基础设施与云计算技术的互联“编织”成了无处不在的物联网，而这也让物联网的自动化和设备之间的有效通信成为可能，给用户带来了更高的效率和更低的成本。

作为信息技术发展的重要载体，物联网在多个领域都大有作为。国民技术产品与规划部执行总监钟新利在接受采访时告诉《中国电子报》记者，物联网的应用涉及工业、汽车、安防、医疗电子、通信、智能三表（水电燃气）和智能家居等多个领域，使物与物、物与人的连接变得无处不在。

交通是物联网的重要应用领域。物联网可以将人、车和路紧密地结合起来，因此能够显著地改善交通运输环境，保障交通安全并提高资源利用率。作为智慧交通的细分领域，车联网也是近些年各大厂商及互联网企业争相进入的领域。

安防是物联网的又一大应用市场。传统安防对人员的依赖性比较大，因此非常耗费人力，而智能安防仅通过设备就能实现智能判断。目前，智能安防最核心的部分在于智能安防系统。该系统能对拍摄的图像进行传输与存储，并对其进行分析和处理。

物联网在医疗领域也能够“大展拳脚”。作为数据获取的主要途径，物联网技术能有效地帮助医院实现对人和物的智能化管理。例如，传感器可以对人的生理状态进行监测，而可穿戴医疗设备则可将获取的数据记录到电子健康文件中，以方便个人或医生查阅。与此同时，RFID技术还可对医疗设备和物品进行监控与管理，以此实现医疗设备和用品的可视化。

物联网在多个领域的广泛应用使得物联网的市场规模正在不断扩大。英飞凌科技安全互联系统事业部市场经理成皓表示，到2025年，全球物联网市场将有4万亿美元至11万亿美元的高速增长，而截至2020年，中国物联网的市场规模将达到7500亿美元。

在物联网市场规模迅速扩张的同时，全球范围内物联网设备的数量也在不断增加。相关统计数据表明，全球每秒大约有127台新的物联网设备连接到网络。目前，全世界运行着大约230亿台物联网设备。截至2020年，全球用户采用的物联网设备数量可以达到约300亿台。未来，由于2000亿台或更多的物联网设备将连接到全球互联网，物联网设备数量将呈指数级增长。

终端安全面临六大挑战

海量的互联网设备与云端连接使得物联网成为了网络攻击的目标，而这也使得物联网安全支出在全球范围呈现上升趋势。钟新利向记者介绍，根据Gartner在2018年的调查，近20%的企业组织在过去三年中至少发现过一次基于物联网的被攻击事件。根据相关预测，为了防止黑客等入侵网络，全球物联网安全支出在2020年将达到24.57亿美元，在2021年将达到31.18亿美元。

物联网的云业务平台、管道端和接入物联网的海量终端存在明显的安全隐患。钟新利表示，在实际应用中，物联网的云业务平台经常面临着未授权访问、敏感数据挖取、伪造请求攻击、假冒服务器等安全问题。管道端则面临着中间攻击、数据监听、劫持、数据协议分析等安全威胁。接入物联网的海量终端也面临着可信根提取、固件提取、逆向分析、硬件破解、设备伪造等多种潜在风险。

在众多风险中，物联网终端面临的主要风险来自硬件、固件、通信、数据、应用和数据采集。紫光国微副总裁苏琳琳告诉记者，硬件风险是物联网终端面临的首要风险。如果终端硬件的功耗信息被泄露，黑客就可以通过侧信道攻击来获取终端的敏感信息。黑客也可以通过控制终端侵入网络，进而对整个网络造成影响。

物联网终端面临的第二大挑战来自固件安全，尤其是固件升级过程中的安全。苏琳琳表示，如果固件被黑客刷新、控制，那么黑客就可以劫持或伪造终端，并进入网络。

第三大挑战来自通信安全。“2016年10月，美国最主要的DNS服务商Dyn遭遇了大规模的DDoS攻击，而这导致了Twitter、CNN等数百家网站无法访问。这就是黑客通过控制城市摄像头而发起的攻击。”苏琳琳对记者说。

第四大挑战来自数据安全。苏琳琳表示，当物联网设备，尤其是摄像头、扫地机器人等设备被攻击的时候，终端数据就会被泄露。被泄露的数据如果被不法分子利用，可能会对个人的财产和生命造成严重威胁。

第五大挑战来自应用安全。当部分物联网设备使用开源开发软件时，黑客可能会利用软件漏洞，通过植入木马、病毒等攻击终端。这可能会造成应用失效，甚至病毒感染整个网络等严重问题。

第六大挑战来自数据采集安全。“终端传感器的数据采集是否可信，以及数据是否被攻击者替换也是目前亟待解决的问题。”苏琳琳说。

安全防护多管齐下

面对如此多的安全漏洞，用户对物联网安全的关注度日益提高，国家也颁布了一系列保障物联网安全的政策。27项物联网安全技术国家标准和《中华人民共和国密码法》的出台为物联网安全领域的健康发展提供了重要保障。近期，工业和信息化部办公厅印发了《关于深入推进移动物联网全面发展的通知》，提出要建立健全移动物联网安全保障体系。

在政策的助推下，企业在物联网安全领域纷纷布局。赛普拉斯面向物联网开发者推出了保证物联网安全的方案；紫光国微的THD89芯片在敏感信息加密存储、安全认证等方面提供了完整解决方案，可有效保障物联网的终端安全；国民技术推出了一系列嵌入式应用的安全芯片及安全MCU产品；英飞凌也推出了基于硬件的安全解决方案，以保障物联网设备“上云”的安全性。

目前，基于硬件的安全方案是最佳的解决之道。成皓以英飞凌推出的产品OPTIGA Trust M2 ID2为例介绍了这种安全方案的优势。它能防御针对硬件的攻击和高强度的软件攻击，使用户数据无法轻易被复制和截取。此外，其专用的设计和非标准的代码实现很难被解析，能为系统提供可信根。安全通信和安全固件升级等功能可以更好地为物联网安全“保驾护航”。

AI、边缘计算和区块链等新兴技术的发展能为物联网安全性的提升带来新的机遇。

AI技术能高效地分析物联网中的大量数据，从而更精准地鉴别出潜在的安全问题。赛迪智库无线电管理研究所副所长彭健告诉记者，AI具备强大的信息处理能力，在提高物联设备信息采集和应用效率的同时还能赋予物联网设备相互学习的能力。通过海量、高质量的数据，AI引擎能对信息安全攻击做出实时反应，并提供与安全攻击有关的分析，以此更好地保证信息安全。

边缘计算的发展有望为物联网安全带来新的活力。彭健表示，边缘计算能为物联网带来更智能的服务、更低的交互延迟和更高的安全性。

区块链技术的发展也能提升物联网系统的安全性。彭健表示，区块链的去中心化安全基础设施能提升物联网系统的安全监测控制能力，从而保障物联网系统的安全可信。此外，基于共识机制的分布式管控可以保证物联网策略与行为验证的一致性，以此保障物联网系统的“健壮性”。

围绕物联网安全的防护措施将会更全面。彭健告诉记者，从物联网连接的角度看，未来要实现“从端到端”的防护，包括从终端、通信网络、服务端、应用端到用户端等环节的全闭环安全防护。从防护内容的角度看，未来要形成多维度的防护，包括终端物理安全、数据泄露风险、恶意软件感染、服务质量等多方面的防护。