新质互联网智鉴报告（V1.0）

新质互联网研究组

前 言

自上世纪末互联网商业化以来，它已深刻改变了人类的生活方式、工作模式以及社会互动的形式。随着社会生产不断迈向新质生产力阶段，各行业数字化、智能化转型的需求日趋迫切，互联网正在经历着前所未有的变革。站在智能化发展的新起点上，我们将见证一个更加激动人心新质互联网时代的到来。

2024年，按照相关工作安排，推进IPv6规模部署和应用专家委秘书处组织部分单位组成“新质互联网研究组”，对新质互联网的概念、架构、技术及发展进行了初步研究。新质互联网不仅是对当前互联网的一次升级，更是面向未来的一种全新构想，旨在通过融合人工智能（AI）、IPv6+、卫星通信、边缘计算、一体化安全等前沿技术，构建一个更加智能、高效且安全可靠的网络环境。新质互联网不仅是对网络技术、网络设备、网络架构的一次重塑，而且将更好支撑数字经济和新质生产力的高质量发展。

本报告作为研究的阶段性成果，阐述了新质互联网的发展背景、核心内涵及其应用场景，并探讨其目标架构和技术基础。我们希望通过这份报告，初步揭示新质互联网所蕴含的巨大潜力以及它对未来社会可能带来的深远影响。同时，我们也期待更多业界专家能够积极参与到这一创新进程中来，共同探索并实现新质互联网的美好愿景，在探索未知的过程中创造无限可能。

本报告在研究和编写过程中得到了中国电信、中国移动、中国联通、中国信息通信研究院，以及全球固定网络创新联盟（NIDA）等单位相关专家的大力支持与帮助，在此表示诚挚的感谢！

目录

CONTENTS

01 “新质互联网”的发展背景

互联网诞生已超过半个世纪，这期间互联网经历了飞速的发展和演变，以TCP/IP技术为基础的数据通信网络技术与产业已经渗透进生产、生活的各个领域，对人类社会产生了深远的影响，催生了全球数字经济的奇迹。

近年来，虽然以硅基半导体性能提升为假设的摩尔定律逐步失效，但雷·库兹韦尔提出的“加速循环定律”并未停下脚步，人类技术前进的速度仍在以指数方式发展，这其中最具代表性的包括人工智能的惊人突破，低空经济的潜在爆发，数据要素的高效流动，等等。

2023年9月，习近平总书记在黑龙江考察调研期间首次提到“新质生产力”。新质生产力是创新起主导作用，摆脱传统经济增长方式、生产力发展路径，具有高科技、高效能、高质量特征，符合新发展理念的先进生产力质态。这种生产力超越了传统的增长模式，其核心在于“新”与“质”的结合，即通过科技创新为核心驱动力，实现生产方式的变革，并符合高质量发展的要求。

“新质生产力”完美阐释了新时代生产力发展的底层逻辑——不再依靠生产资料的简单加工和生产过程的低水平重复，而是依赖技术创新所带来的生产力要素自身的突破性变革。“新质生产力”的劳动者将不再仅限于生物意义的“人”，而扩展为智能意义的“人”；劳动资料从来自物理世界的生产设备，扩展为构建虚拟世界的算力与算法；劳动对象从自然界产出的物质材料，扩展为存在于网络空间的数据要素。

新质生产力的发展必然要以更加高质量、高效率、高智能、高安全的基础网络来承载。业界将这一新型的网络技术体系称之为“新质互联网”。“新质互联网”不仅仅连接传统的网络用户、系统、应用，而且要进一步连接算力、数据，并不断扩展其物理空间范畴；其业务模型不仅仅是信息的访问，而更多表现为信息的产生、爆发、重组、流动，从而极大的改变网络的整体结构和技术需求。

新质互联网是人工智能时代的互联网升级演进，将服务于新质生产力背景下数字经济、数字政府、数字社会的发展。

02 “新质互联网”的内涵与外延

“新质互联网”是国内产业界在总结新产业需求、新应用领域、新技术方向的基础上提出的数据通信网络技术体系，是适应新质生产力发展的网络新底座，是智能化时代网络技术升级的演进新方向，服务于全社会的数字化转型和高质量发展。

“新质互联网”是面向人工智能等新技术大规模应用所带来的算力部署新需求，基于IPv6/IPv6+等网络基础技术，对包括地面、近空、深空的广阔物理空间的各类算力、终端和数据要素实现泛在连接，所构建的可靠、高效、安全、智能、绿色的网络技术体系。

在以新质生产力为支撑目标的前提下，“新质互联网”体现了人工智能与网络协同发展的趋势，进一步扩展了网络的连接主体和服务形态，并在新的场景需求中不断带动了网络的技术创新：

- **新主体**

  算力，尤其是智能算力成为网络连接的新主体，“新质互联网”需要实现算力供应者、算力使用者、样本提供者等各类主体之间，在样本入算、训练推理、模型分发等各个阶段的高效连接。

- **新终端**

  网络的用户不仅限于生物意义的“人”，“新质互联网”需要实现对包括但不限于人（个人用户）、企（企业用户）、机（生产设备）、智（智能体）、物（物联终端）等各类智能化终端的泛在连接。

- **新要素**

  “新质互联网”需要为各类数据资源提供适应其实时性、完整性、隐私性、合规性等要求的可靠连接。

- **新空间**

  “新质互联网”突破近地空间局限，为地面、低空、深空等各层面空间范围的各类网络业务主体和应用终端提供的广泛连接。

03 “新质互联网”的场景

回顾互联网的发展，从PC互联网到移动互联网，从消费互联网到产业互联网，互联网基础设施在促进社会经济数字化转型方面发挥了巨大的作用。当前以生成式AI为代表的人工智能技术发展激荡人心，未来，我们将经历从数字社会向智能社会的转变，人工智能的发展会对应用场景、网络架构和治理模式产生前所未有的影响。互联网从连接主体，终端类型，业务特征，空间覆盖都将面临众多前所未见的新场景，我们将其总结为“联算”、“联智”、“联数”、”联空”。

3.1 “联算”场景

算力是数字经济时代的核心基础设施，对促进经济增长、推动科技进步以及满足日益增长的数据处理需求具有至关重要的作用。随着ChatGPT引爆大模型热潮，让人类看到了通用人工智能“生成创造世界”的曙光，也促使人们对人工智能加快社会各领域数字化转型及智能化发展，促进全社会生产效率提升，抱有极高的期望。算力既是智能时代的“引擎”，也是智算时代最宝贵的资源。联算是在算力供给者和需求者之间架起了连接的桥梁，联算网络就是连接算力、算卡的网络，从算力使用场景上需要关注算内、算间、入算三张网络。

算内网络实现数据中心内算卡的互联，需满足单数据中心算卡从百卡到万卡、十万卡的超大规模集群连接，需要具备超大规模组网、无损高吞吐，以及智能容错能力。生成式人工智能训练的第一性原则就是Scaling law，即大模型的智能水平与模型参数、数据样本和算力三个因素成正比。业界推测GPT-4 参数量约1.8万亿，训练中使用了大约 2.15e25 FLOPS算力，训练集群使用约25,000 个 A100 GPU。随着模型参数量从千亿到万亿、十万亿的增长，模型训练使用的算力卡也从万到十万发展，对数据中心网络提出了超大规模组网调度、超高吞吐、无损传输、快速故障闭环的要求，以实现算力效率的100%释放。

算间网络实现多智算中心间的高速互联，突破地域限制，通过高吞吐，长距无损协同，有效提升算卡资源利用率。大模型算力需求快速增长，由于电力资源等原因限制，单数据中心算力规模受限，业界大模型厂商采用多数据中心资源联合训练大模型。另一方面，当前国内普遍是千卡集群，单体无法满足万卡训练诉求。通过构建多数据中心协同训练能力，城市内多智算中心、区域内（区域省份间）、区域间（国家算力枢纽间）算力可实现高效协同，实现碎片化算力整合利用，提升算卡利用率，支撑更大模型的训练和缩短模型训练时间。多DC互联网络需要具备长距无损、高吞吐的能力，以支持算间协同，突破地域限制，整合全国算力资源。

入算网络作为算力管道，连接大量企业、科研机构与算力中心，需要具备差异化调度和调优能力，满足海量数据高效入算。AI大模型训练催生大数据入算需求，模型数据集通常需要数十GB到数百TB的数据。典型如某车企每天上传一次100T~160T数据，年数据量约38PB；某基因公司每天上传一次15T数据，年数据量约4.5PB。大数据量入算对网络的挑战主要在三方面：一是接入带宽挑战，大数据量上传百兆专线耗时太长，万兆专线成本太高；二

是网络利用率挑战，大数据入算产生大量大象流，现有网络负载均衡策略中无法区分流量规模，将由于流量不均衡而造成网络利用率的大幅下降；三是数据安全挑战，部分企业敏感数据需要入算训练，但又不希望异地存储造成可能的泄露。这些挑战导致目前90%以上的企业还都选择寄硬盘方式传递数据。因此，新质互联网需要给企业构建一张更具备性价比和安全传输的入算网络，提供任务式服务的高弹性，提升整网带宽利用率，并实现数据的高安全传输和数据主权保护。

3.2 “联智”场景

AI技术的广泛应用大幅加速了各行业的数智化转型。随着生成式AI、多模态理解和具身智能技术的发展，虚拟与现实世界的实时交互不断深化。AI智能体（AI Agent）与各类智能终端深度融合，创造出更多的创新应用场景。以智能助手、具身机器人和沉浸式系统为代表的AI终端，已在生活和生产领域产生了显著影响。同时对网络提出了更大带宽，更高可靠，更低时延和更高安全的要求。

面向个人服务，AI终端和数字人作为人与AI连接的入口，重塑了新型人机关系，并引发了多级推理的网络架构变革，端云之间需满足高带宽，低时延的诉求。预计到2030年，随着全息投影、脑机接口技术及新型材料的发展，可穿戴终端和数字人结合多模态识别和自主决策能力将实现更加逼真、自然的交互体验。同时，自动驾驶技术也将从单车视距逐步演进至超视距的车路协同自动驾驶。由于端侧算力的局限，以上服务都将依赖端云协同，远端推理。因此，未来面向个人业务的网络需具备端云及端端之间10至20毫秒的确定性交互时延、每终端超100Mbps的带宽吞吐能力，并具备自动故障感知与快速修复功能。

面向家庭服务，以陪伴型具身机器人为核心的互联互通的家庭智能生态系统成为主流，网络除了提供低时延体验，还需具备安全认证和数据加密功能。到2030年，智能家居设备、个人助理与健康监测设备、陪伴与服务机器人、VR/AR设备以及智能安防系统等终端将得到广泛应用，形成高度智能化的家庭生态系统。家庭服务不仅需要边缘推理的自决策和多系统的联动处理，还对数据安全提出极高要求。网络尤其是BNG等网关设备需要具备终端级的接入认证、业务级的策略控制、以及端到端的业务加密能力，以保障家庭生态系统的安全性与稳定性。

面向企业业务，沉浸式协同办公、AI助手和智能制造机器人等技术正在迅速应用，互动性更强、生产效率更高，人人、人机、机机间紧密协作。网络需要保障虚实融合体验，低时延，厘米级定位，并提供应用级策略控制和数据立体防护。全息投影和虚拟化身将使远程协作更加直观真实，这类全方位的沉浸式体验要求边缘渲染、超高分辨率和低时延交互的支持，办公网络需具备每终端1Gbps、每接入点（AP）100Gbps的超高带宽，并确保低于10ms的超低时延处理能力。同时，AI助手作为不可或缺的支撑系统，需与员工具备一致的访问权限和安全策略，确保内网安全并防止数据泄露。具身智能制造机器人将在工业生产中发挥着重要作用，IDC预计到2027-2030年，中国制造业具身机器人密度将扩展到每万人650台，为满足多机器人协作的需求，生产网络必须提供每终端1Gbps的带宽，并将智能体间的交互反馈时延控制在20ms内，同时确保频繁移动时无信息丢失，并通过厘米级高精度定位，防止碰撞事故的发生。

3.3 “联数”场景

随着数字经济的深入发展，数据已经成为继土地、劳动力、资本和技术之后的又一重要生产要素。近年国家相关数据要素政策法规的加速出台和AI等新型数字技术的爆发式发展，推动数据要素产业进入加速发展阶段。数据要素的流通模式也从组织内部不同部门之间的流通，向跨组织、跨信任域的流通转变。数据要素在流通和处理过程中面临多种安全风险，进而影响数据要素的流通效率和价值实现，给数据供需双方带来损失和风险。安全风险包括：数据传输过程中被外部黑客非法侦听、篡改、重定向等导致数据传输泄密和完整性受损；数据主权在流通过程中被削减，被数据需求方滥用或越权使用等。联数网络就是面向数据要素流通场景构建的跨行业、跨区域、跨主体的新一代安全可信任的数据要素流通网络基础设施，支撑国家数据要素流通市场的安全高效发展。

联数网络需要具备感知数据身份/类型/敏感等级并进行安全控制策略随行，实现数据要素流通路径的可管、可控。网络需要感知数据所属的用户身份，数据类型，敏感程度等信息，在网络边界进行合适的策略控制，避免敏感数据流通到非预期位置。网络需要将数据的信息携带到数据使用方（例如通过IPv6扩展头），对数据使用进行认证和使用管控。网络需要为不同敏感等级的数据提供合适的安全防护措施，既满足数据交易的诉求又不过度保护。

联数网络需要具备差异化数据传输可信路径和更高安全传输加密能力，匹配不同行业、不同数据等级的数据要素流通安全要求。由于数据要素在流通网络中可能通过多种路径（有线/无线/卫星）进行传输，且涉及许多不同厂商、不同类型的网络设备，不同的传输途径和网络设备状态面临不同安全风险。因此，基于不同行业和领域对于数据安全的法律法规和监管要求的约束，对于不同数据提供方数据的传输路径和链路就需要联数网络能提供差异化安全路径和传输加密方式。其中传输加密可以在应用加密或者不加密的基础上，进行更高安全等级的加密，如量子加密等，或者基于行业监管的诉求，叠加进行多重加密。

联数网络需要提供数据接入节点，具备网络、数据安全多合一能力，能基于零信任架构提供数据安全存储、数据精细使用控制、数据安全传输等数据安全增强能力，实现数据的灵活安全接入，降低客户数据连接门槛。将网络和数据安全功能整合到数据接入节点设备，可以避免数据源接在不同设备或系统之间进行复杂的流转并减少数据接入节点的整体风险暴露面，从而提高数据要素接入的效率和安全性。

3.4 “联空”场景

地面移动通信一直在飞速发展，但依然存在着大量地域尚未实现网络的有效覆盖。为破解这些区域的通信难题和推动新兴业务的发展，人类智慧转向了浩瀚的天空。面向未来，多星座卫星通信网络、高空平台通信网络、地面固定和移动蜂窝网络的深度融合，将共同构建空天地一体化的新质互联网，极大地拓展人类信息交流边界，引领我们迈向更加广阔、智能且紧密相连的未来世界。

低空智联，构建稳定、连续、高速可靠的无缝覆盖通信网络，以满足日益增长的各类低空新业务需求。低空经

济的不断发展，将带来日益丰富的应用场景，如建设无人机物流节点，发展低空智慧物流；利用直升机、eVTOL等飞行器探索低空通勤新业态；采用低空飞行器执行应急救援；开展多元化低空旅游产品等。低空通信基础设施不仅需要提供稳定且连续的数据传输服务，确保飞行数据的实时、准确传输，还需要对飞行环境的无盲区感知，增强低空飞行的安全性。同时，需要提供高速、可靠的通信网络以满足低空导航对数字化、精细化的需求。面对这些新需求，低空通信网络需要不断升级与优化，确保低空活动的安全、高效与可持续发展。

卫星物联打破地域限制，构建低成本、广覆盖、大容量的卫星物联网，提供增强型物联网络服务。低轨卫星物联网具有投资小、见效快、带动性强、经济和社会效益显著等特点，是地面物联网的关键延伸与补充。物联网应用大多对通信时延有较高的容忍度，且不需要持续不断的信号覆盖，通过稀疏的卫星网络，如数十颗或百余颗卫星实现低成本组网。通过卫星覆盖解决以往信号覆盖盲区无法解决的信息监测数据回传问题，为农业管理、海上运输和能源行业等应用场景提供广覆盖、大连接量的卫星物联网服务。

卫星互联网的泛在接入，促使构建更广阔、多层次的通信体系，提供广覆盖、大带宽、低时延的网络服务，网络自身需具备高稳路由计算，高可靠，高安全的能力。低轨卫星星座具有发射成本低、传输时延短、路径损耗小等优点，将网络覆盖延伸至偏远山区和广袤海洋，与地面互联网一体化发展和深度融合，构建空天地一体化通信系统。但卫星网络规模庞大，节点高速运转和太空环境复杂，导致网络路由的复杂性显著增加，卫星网络的可靠性面临新的挑战。卫星节点直接暴露于太空中，难以进行物理隔绝，面临着无线链路、载荷和卫星平台的干扰、窃听和攻击等特有的安全威胁，如何保证卫星通信网络的安全，将是一个长期的核心技术课题。

04 “新质互联网”目标网架构

“联算”，“联智”，“联数”，“联空”共同构成了新质互联网的场景，也对新质互联网的架构和能力提出了新的要求。在物理网络结构方面，新质互联网需要构建入算，算间，算内三张网络，构建多级推理中心和高质量的边端网络，构建高速连接的数据网络，构建空天地一体的全域覆盖网络。为了满足业务需求，在物理网络之上，需要有联智，联数、入算的业务网关把用户和算力/数据连接起来。在新质互联网中，控制器仍然是关键的组成部分，多域控制器和编排构成了网络的集中大脑，向业务运营层提供多种网络服务。同时，安全作为基础属性，需要为每个层次保驾护航。

新质互联网整体架构如图1所示。

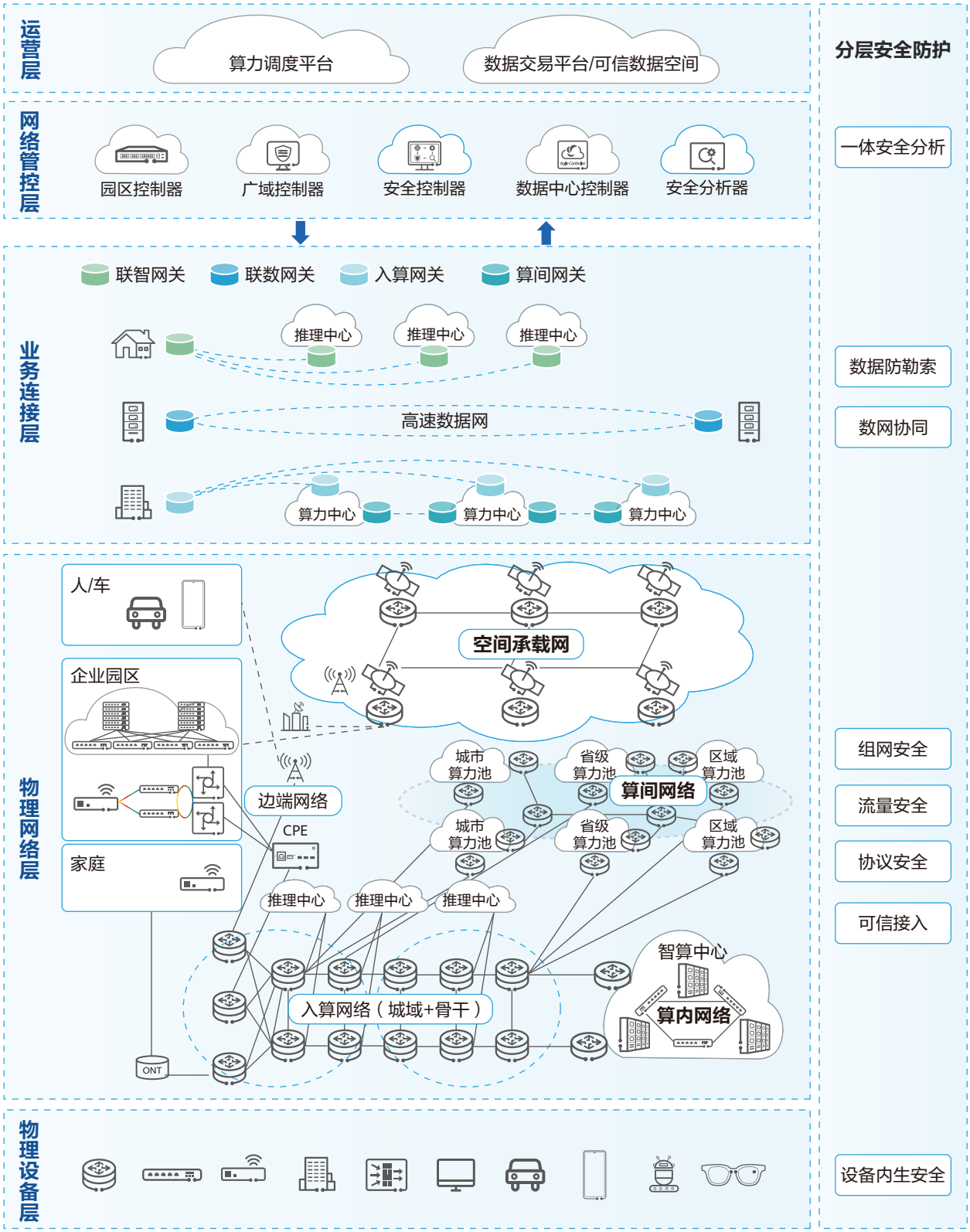

图1　新质互联网整体架构

基于场景诉求，新质互联网需要具备如下关键特征和能力：

极简超宽	智能内生	绿色节能	一体安全
网络拓扑极简，网络端口超宽高密，物理层协议（如Wi-Fi）持续提升带宽容量和体验保障能力。	业务连接层精细识别，物理网络层无损高吞吐，网络管控层和物理设备层向智能化演进并共同实现网络自动驾驶。	物理设备层按需休眠，物理网络层低碳路径，网络管控层实现可视可控。	设备层内生安全，物理网络层实现传输通道安全，业务连接层通过数网协同，数据防勒索等方式保障业务连接安全，网络管控层对全网安全事件进行一体安全分析和阻断。

4.1“联算”目标网架构

“联算”网络有算内、算间、入算三张网络，不同网络有不同的关键诉求。算内网络需要具备超大规模组网、无损高吞吐，以及智能容错能力，使能高算效。算间网络需支持高吞吐，长距无损协同，使能多DC协同训练。入算网络承载海量大数据流入算，需构筑差异化调度和调优能力，实现全网万级节点，千万流并发，整网带宽充分利用，满足不同业务入算的SLA。联算目标网需要结合以上差异化诉求综合考虑网络架构、关键技术与创新应用，助力算力高效释放，像电力一样成为一种公共服务。基于联算场景和网络需求，联算目标网架构由运营层、网络管控层、业务连接层、物理网络层四层组成，如图2所示。

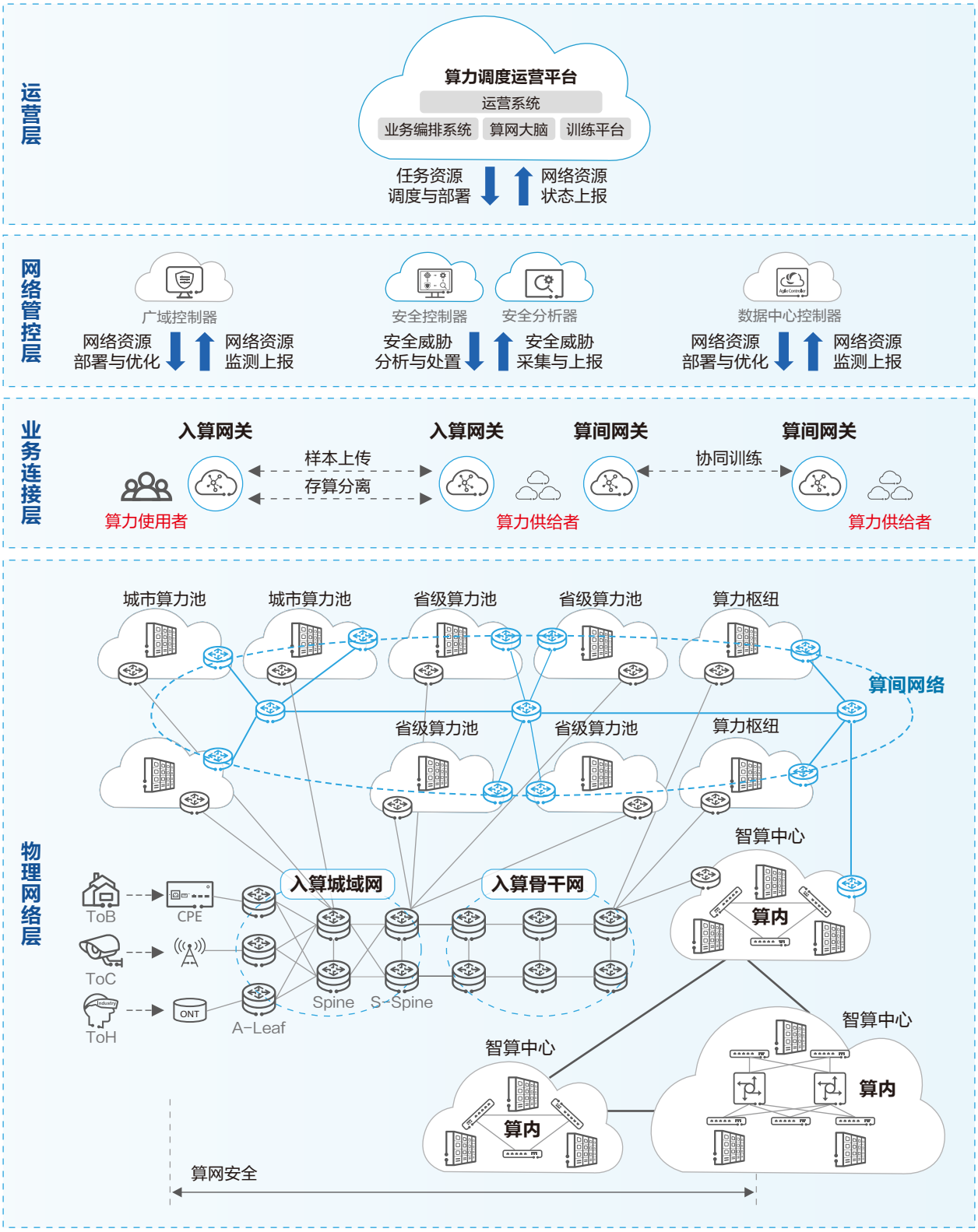
运营层
算力调度运营平台
运营系统
业务编排系统
算网大脑
训练平台
任务资源
调度与部署
网络资源
状态上报
网络管控层
广域控制器
网络资源
部署与优化
网络资源
监测上报
安全控制器
安全分析器
安全威胁
分析与处置
安全威胁
采集与上报
数据中心控制器
网络资源
部署与优化
网络资源
监测上报
业务连接层
入算网关
入算网关
算间网关
算间网关
样本上传
存算分离
协同训练
算力使用者
算力供给者
算力供给者
物理网络层
城市算力池
城市算力池
省级算力池
省级算力池
算力枢纽
算间网络
省级算力池
省级算力池
算力枢纽
智算中心
算内
入算城域网
入算骨干网
ToB
CPE
ToC
ToH
ONT
A-Leaf
Spine
S-Spine
智算中心
算内
智算中心
算内
算网安全

图2　联算目标网架构

物理网络层

算内、算间、入算三张网络位于本层。三张网络需求不同，物理位置不同，需要分别使用独立的网络承载。由于现有网络能力无法满足联算的网络需求，推荐新建平面/POD来承载联算业务。算内网络支持超大规模组网，具备无损低时延、高负载均衡能力，支撑智算集群算力资源高效运行。算间网络实现100km~3000km 多数据中心算力互联，使能多DC长距无损协同训练，有效提升算卡资源利用率。入算网络连接用户与算力中心，支持2B/2H/2C等用户泛在接入，实现高品质入算。

业务连接层

对于入算网络，需要在企业侧和算力中心部署专门的入算网关，入算网关提供传输层协议转换，为入算流量分配标识并选择合适的隧道和路径，并提供计费对账等能力。入算网关为网络的高吞吐传输进行引流，确保流量可以快速入算。对于算间网络，在算力中心部署算间网关，提供RDMA协议联接，为多算力中心协同训练提供超大带宽和长距无损的转发路径。

网络管控层

网络资源和安全防护的配置、部署、运维位于这一层，通过网络/安全控制器/分析器，构建网安自治引擎。网络管控层北向对接算力调度运营平台，获取算力任务订阅信息，南向对网络和安全进行规划部署，通过智能引擎分析并计算算力任务所需最佳网络资源配置和安全防护策略。同时获取网络/连接层的多层多维信息，构建网络和安全数字孪生，全面提升运维效率。

运营层

算力资源的调度、分配、部署，算力服务的业务编排，模型的训练等业务平台位于这个层次。通过统一的算力调度运营平台，让多个业务平台协同服务于算力需求者和供给者。算力调度运营平台南向对接网络管控层，下发任务调度与部署，并获取网络资源信息进行优化调整。

“联算”目标网络需要具备如下特征：

绿色超宽

包括但不限于：网络设备调频调压，动态节能。算内全液冷网络，满足PUE的降低。网络支持节能算路，优选低能耗路径。弹性组网，如算内的Dragonfly+网络架构，组网规模提升10倍同时降低TCO。网络高密互联，单端口带宽向400GE/800GE/1.6T演进。

无损高吞吐

算内网络通过芯片ms级拥塞感知、通告和精准反压，高负载均衡技术等，保障网络有效吞吐达到95%以上，加速AI训练。算间网络通过流级精准流控，全局负载均衡等技术，实现整网有效吞吐率达到95%以上，保障百公里到千公里长距训练效率下降<5%。入算网络通过千万级流调度，最大通量算路等技术，提升整网带宽利用率，实现运力效率倍增。

运力服务化

网络运力服务提供任务级的高弹性，带宽100M~100GE弹性随需，TB级别数据可小时达，未来可支持更大的弹性带宽。网络支持多维实时感知与分析，数字孪生构建高精数字地图。通过网络大模型加持，网络走向自治。保障网络运力可感知评估，服务SLA可承诺。

算网一体安全

数据在网络上安全传输，不泄露、不被篡改。网络需具备高安全传输，超大带宽线速加密的特征，如MACsec国密、PHYSec，Xsec线速加密。网络需提供数据安全保障，数据流动需防泄露、防勒索，实现网存算联动一体防护。

4.2“联智”目标网架构

“联智”网络用于连接各类智能体终端，满足其与推理中心的交互需求，实现实时决策等智能功能。不管是个人服务，家庭服务还是企业服务，智能终端和端云协同都对网络提出了高带宽，低时延，安全认证，数据加密，应用级策略控制等诉求。为确保业务虚实融合体验，推理中心需分级部署，“联智”业务网关需灵活编排满足智能体的多样需求，并通过管控层实现快速部署与调整。基于这些网络需求和业务演变，“联智”网络架构采用基于图3的四层架构。

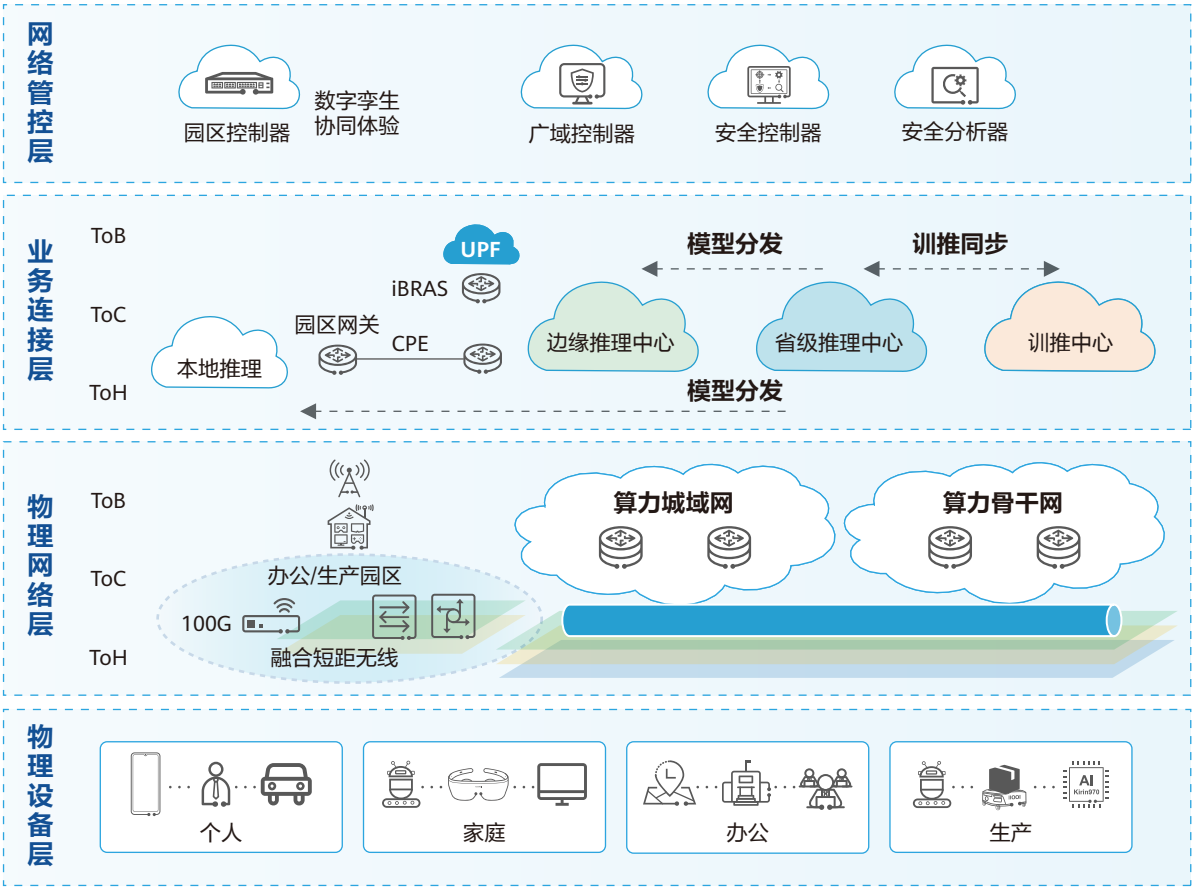

图3　联智目标网架构

物理设备层

指通过5G/Wi-Fi/工业环网等连接到网络的智能终端设备，如AI手机、可穿戴设备、智能车、沉浸式系统、AI助手、工业机器人等，涵盖个人、家庭、办公和生产等场景。相比传统终端，智能终端会产生更大流量，如沉浸式系统的带宽增长10倍；会产生更多用户（session）接入，如AI助手的APP级接入；会使用更复杂的交互模型，与多级推理中心/其他终端/数据中心交互。

物理网络层

指连接智能终端与推理中心的基础设施网络，包括办公/生产园区网络、城域网/无线回传网络和广域网等，满足各类场景下智能终端的大规模接入需求。例如, 办公或生产园区的Wi-Fi网络需具备至少10G~100Gbps的带宽接入能力，并支持大规模用户管理。网络层需按需提供端到端低时延保障，以及在高并发和复杂环境下保持稳定，以满足不同业务的推理需求。

业务连接层

指各类业务融合网关与多级推理中心的衔接，通过动态选择适合的推理模式，确保不同业务的顺畅运行。融合网关作为业务入口，通过业务识别和控制，配合多级推理满足各类业务差异化需求，同时作为数据加密和安全策略的控制点保障数据安全。为了满足业务的时延和安全诉求，推理通常会分多级部署，例如园区内推理/运营商边缘推理/中心推理，融合网关自身也可以成为一个边缘推理节点。

网络管控层

负责对联智网络进行资源调度与安全管理，确保园区和广域网络的稳定运行。通过数字孪生等技术，园区网络和安全管控平台对园区网络和智能终端进行海量用户策略管理，业务质量实时监控和优化，并对故障和安全攻击进行快速响应。广域网络和安全管控平台则负责运营商网络的差异化业务编排，策略控制和质量及安全监控。

构筑“联智”目标网，其网络架构需满足以下特征：

超宽接入

终端设备层通过无线、有线、物联网多种方式接入网络，在沉浸式会议，虚拟元宇宙等高带宽场景至少1G带宽/终端；网络接入层支持100G带宽和海量终端接入。

高品质保障

网络层结合业务标记，通过空口帧级调度，带宽资源隔离和路径实时优化，确保业务的高可靠，0丢包和低时延传输。网络接入层融合短距无线等技术，支持cm级位置定位，以保障安全生产。管控层结合数字孪生和AI大小模型分析协同，实时调整服务参数，实现业务体验保障的分析、决策、闭环。

多层次安全

管控层提供会话的统一管控，配合网络接入层对智能体接入进行严格的安全认证和策略控制，避免数据越权访问，防止数据泄露。网络层对数据流的传输进行安全监控和量子级加密传输，保障业务数据的安全。

4.3“联数”目标网架构

联数网络是面向数据要素流通过程中，为数据提供方和数据需求方提供可信接入、可信流通、随路使用管控和跨域/跨境流通管控的网络基础设施。在有效推动数据要素流通，充分释放数据价值的同时端到端保障数据要素流通的完整性，保密性和可用性。如何进行数据的可信流通和交易，欧盟的IDSA已成为最成熟使用的参考架构。在使用IDSA架构的场景中，联数网络可和IDSA中连接器进行协同或者承担连接器的部分能力。

联数目标架构由物理设备层，物理网络层，业务连接层，网络管控层和运营层构成，如图4所示。

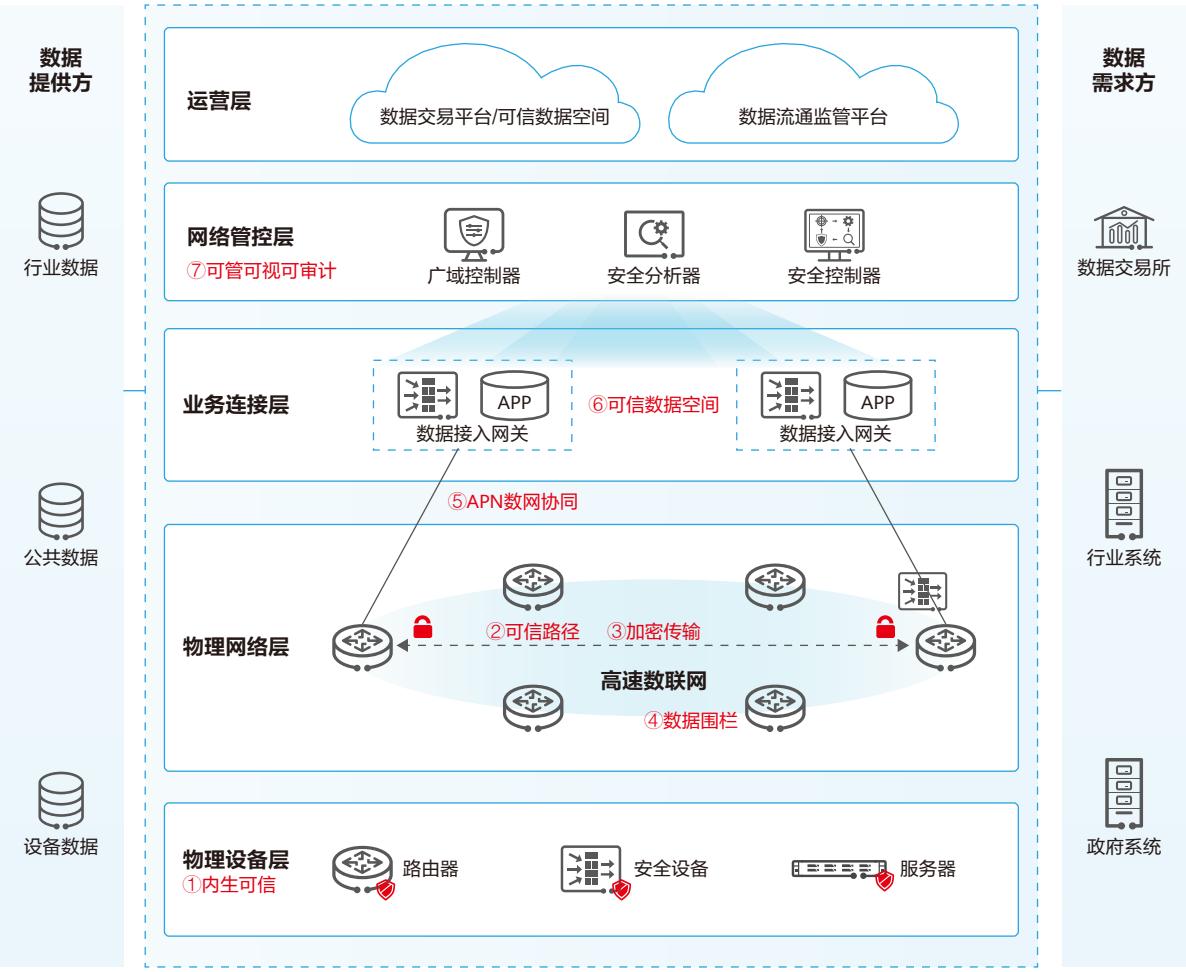

图4　联数目标网架构

物理设备层

设备层包含联数网络的各类网元节点设备，是构筑联数网络的基石，通过设备自身软/硬件的安全可信及对外部攻击的抵御及韧性恢复能力保障网元设备自身的可靠性，可用性和完整性，是构筑联数网络的可信基础。

物理网络层

在设备可信的基础上，网络层负责构筑数据要素流通的可信通道，提供一站式开通、动态调整数据流通网络路径能力。通过基于数据敏感等级、网元可信状态、网络可靠性能力等智能计算生成数据流通的可信路径，并基于IFIT技术实现数据实际流通路径的监测，保障为不同敏感等级的数据流通提供差异化可信传输路径。 通过在数据流通全链路中采用多种密码学技术和方法，通过量子密钥分发、IPSec/MACsec等加密技术保障数据传输安全。

业务连接层

面向数据供需双方提供多场景数据就近可信接入、APN数网协同、数据围栏等能力。通过网络和数据安全融合数据接入节点，实现数据供需方的身份、设备、数据可信接入联数网络并实现数据的加密存储和使用控制策略指定。通过网络标签（如APN6）承载数据的用户身份，数据类型，敏感等级等信息，确保按照数据提供方制定的使用控制策略随路进行严格、精准的数据使用，提供对数据主权的安全保护。通过识别网络标签承载的数据授权使用范围（如：国家、行业等），对于超出授权访问的数据流通进行阻断、深度解析判定等策略管控，实现数据流通过程的“数据围栏”。

网络管控层

管控层是联数网络的统一管理中心，由广域控制器、安全控制器和安全分析器等组成，为数据的端到端流转过程提供统一的认证鉴权，智能化的网络编排调度，可溯源的合规审计及精准的威胁检测等能力。

运营层

“联数”运营层主要由数据流通管控平台和数据流通监管平台组成。其中数据流通管控平台提供身份认证、使用控制、存证审计、数据市场等关键能力，提供全局数据可信流通管控能力。数据流通监管平台提供业务审核、合规监管等关键能力，确保数据流通活动满足国家和行业相关政策法规要求、规范数据流通市场秩序。

“联数”目标网络需要具备如下特征：

设备可信

联数网络的网元设备支持通过硬件、操作系统和平台、业务应用和组件构建三层防御，通过管理面安全、控制面安全和转发面安全的三面隔离和设备安全态势感知等能力实现网元设备的软件完整性保护、数据机密性保护、系统安全防护、运维安全和分层隔离的内生安全。

网络可信

联数网络支持感知数据敏感等级和安全控制策略随行能力，满足数据按需差异化安全路径转发和路径动态调整要求。支持基于网元设备可信状态、数据敏感等级等可信算子动态编排可信数据流通路径。支持采用MACsec、IPsec、量子加密等多种加密传输方式实现网络传输链路的安全性，为应用安全提供更强的加密保护或者多重加密保护。

业务可信

面向跨行业、跨区域、跨主体的数据流通场景，联数网络支持极简数据接入能力，在网络设备上融合增强数据安全存储和使用控制能力，并支持将数据敏感等级和使用控制属性等映射到网络流量上，实现整个数据流通阶段的可管和可控。

4.4 “联空”目标网架构

联空网络由多种异构网络混合而成，是具备空天地融合、高可靠、高安全的新型IP网络体系，需要综合考虑网络架构、关键技术与创新，并在标准化和应用场景方面进行深入研究和探索。整体网络架构自顶向下分为四层，分别是：网络管控层、空间段网络层、地面段网络层、物理设备层。

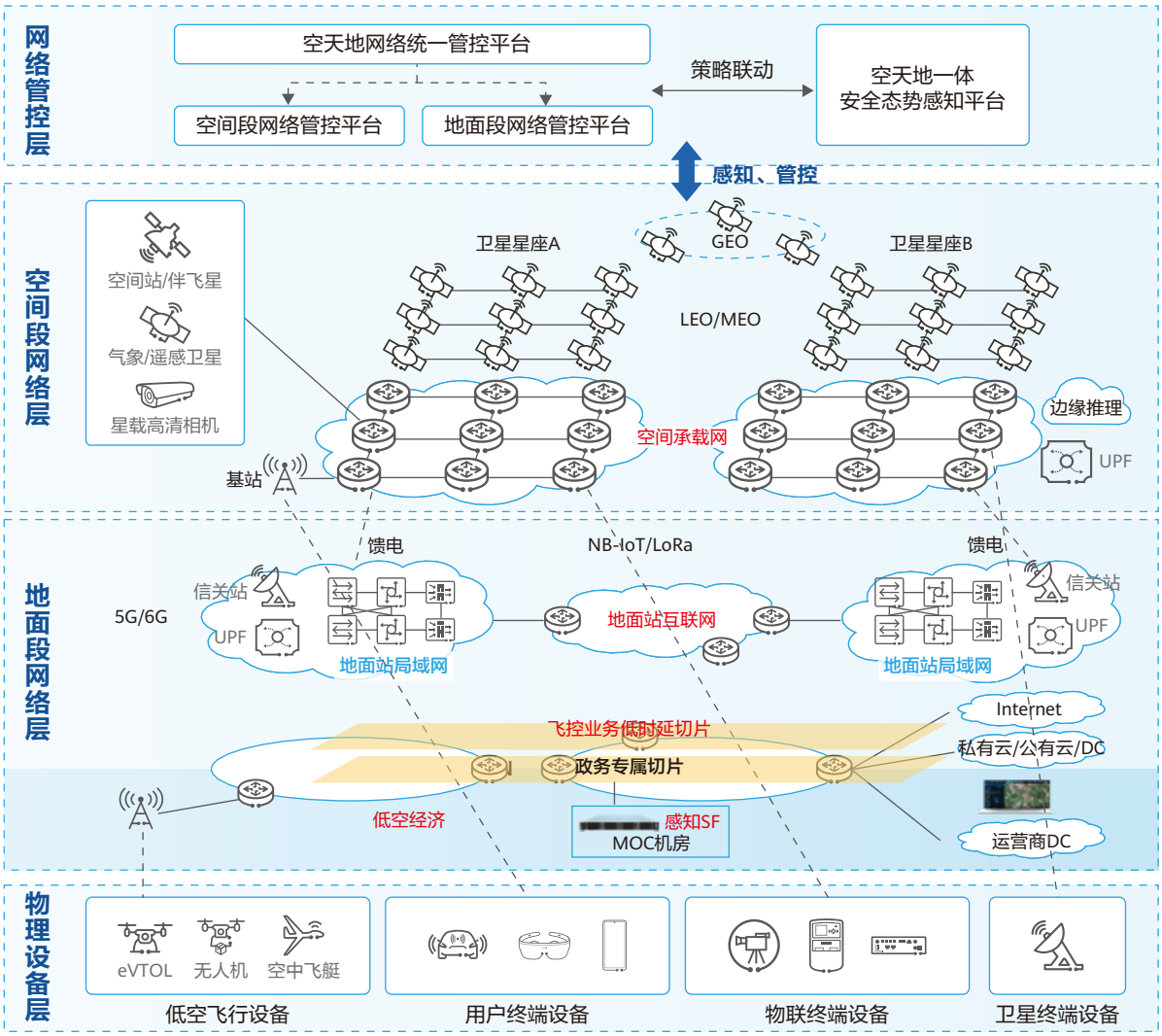

图5　联空目标网架构

物理设备层

根据不同的应用场景连接终端分为四大类：通过5G/6G空口连接地面基站的低空飞行设备；通过5G/6G空口连接星上基站的2C终端，如手机终端和车载通信终端；通过NB-IoT或LoRaWAN连接卫星的物联网终端；在无网地区，通过馈电链路连接卫星的企业或家用卫星终端。

地面段网络层

包含卫星通信的地面站互联网、传统的固定和移动通信网络。卫星通信地面站互联网在局域网中部署信关站、业务网关和综合运控管理系统，使用骨干网连接地面站局域网和Internet网络。通过网络间的互联互通，提供业务的综合承载能力。

空间段网络层

由部署在每颗卫星内部的路由设备组网形成，主要用于卫星之间通信。通过部署在卫星中的基站接入地面终端，通过馈电链路连接地面的信关站。通过与地面段网络通信，将业务回传地面，实现访问Internet、核心网系统和企业分支/总部等能力。

网络管控层

由空天地统一网络管控平台和空天地一体安全态势感知平台组成。网络管控平台对空间段/地面段网络进行统一管控、业务路径编排、故障识别和自动定位；安全态势感知平台对整网的安全事件进行统一分析，智能编排安全策略，构建高效威胁防护体系。

联空网络是一个综合性通信系统，融合卫星网络和地面网络的通信资源，以实现全球范围内的无缝覆盖和高效服务。以下是空天地一体化网络需要具备的一些特征：

时变动态性

卫星节点的高度动态性，导致卫星与地面用户、信关站之间的链路频繁切换，带来网络拓扑实时变化。这种时变特性给卫星网络的路由协议和算法设计带来新的挑战。星间路由需要减少节点发现、链路重建、路由规划等引起的时延和网络中断，实现卫星间有效的数据传输；星地路由需要保证在频繁的星地链路切换过程中业务流量的连续性和高效性。

宇航级可靠

由于空间环境的复杂性和不可预测性，卫星通信载荷和卫星网络需要具备宇航级的高可靠性，保证关键通信任务的连续性和稳定性。通过抗辐射加固、故障预测管理等避错技术，结合多维度三模冗余、故障域隔离等容错技术，全面提升在空间环境的网络可靠性。

空地融合管控

空天地一体化网络需要统一的融合管控架构，将地面网络与空间网络资源进行统一管理和调度，并向智能化方向不断演进。如对卫星服务时间进行预测，自主感知、学习环境的特性与变化，智能决策实现用户终端的无缝接入；通过感知业务指标要求，结合用户密度和网络资源状况，利用AI/大数据分析等技术，构建自适应调度机制，优化业务体验。

空地一体安全

空天地一体网络的安全威胁主要涉及通信链路安全、地面系统安全、卫星载荷安全、供应链的安全以及用户终端安全。通信链路安全要重点考虑卫星与地面站、终端和卫星间的防私接，以加密和认证技术为主；卫星通信载荷安全，需要从板卡、芯片、软件等多维度构建整机的内生安全。

05 “新质互联网”的关键技术

新质互联网四联场景和目标网架构对网络技术提出了新的挑战与要求。

- **物理连接实体智能化**

  云端智能算力、边缘智能算力、终端智能算力的三种模式相互协同，要求网络大带宽、高可靠、确定性体验与绿色节能。

- **网络连接扩展新领域**

  从连接企业、家庭、蜂窝、DCN，扩展到空天地融合网络；从保证连通性的树、环等形状变化拓扑，扩展到卫星网络的时变拓扑。组网、拓扑对协议栈提出了挑战。

- **网络与智能融合**

  网络连接AI的同时，AI也在增强网络，智能连接、智能安全、智能运维增强了网络性能与安全，提升了网络运维、运营的质量和效率。

- **业务承载多样化**

  混合云改变了业务部署，安全物理边界消失；网络承载业务从语音、上网业务，到可交易数据，从数据生产到数据消费，从数据治理到数据监管，安全诉求持续增强。

这些挑战与要求需要对当前网络的能力进行增强和重构，在物理连接、网络连接2个水平层次和智能融合、安全融合2个垂直方向上形成系统化的技术体系，包含超宽新联接、IPv6+新扩展、网络新智能、安全新机制四大技术方向。

5.1 超宽新联接

园区网络100Gbps空口+超融合短距无线：终端AI算力不断增长、具身智能等形态多样、沉浸式协同等应用推动园区宽带接入全无线化，要求大带宽、高可靠。全无线化从Wi-Fi7演进到Wi-Fi8，在Sub7GHz频谱之外，引入60GHz毫米波（59～64GHz）和5GHz中频（5.3～5.7GHz）Local License频谱。**在大带宽方面，**毫米波的引入将空口接入带宽从30Gbps提升到100Gbps，通过高增益算法、介质HBF天线等技术不断挑战突破功耗约束下的10~15m的覆盖距离，实现毫米波与Sub7G共AP，支撑大带宽，尤其是工业AOI回传、XR视频本地生成等大上行场景。**在可靠性方面，**Local License专频授权企业在园区/厂区范围内专用，设备受控授权接入，避免开放频谱环境中的随机冲突，叠加终端受控制调度等技术，可实现99.9999%的可靠性，支撑生产无线化中固定接入、固定回传、移动接入、移动回传等高可靠新场景。

广域网络绿色超宽800GE+弹性无损：AI训推数据产生分散，而计算存储集约，需要物理世界和数字世界的绿色超宽连接、面向海量数据流量的弹性无损传输。**在绿色超宽方面，**800GE成为下一代广域组网端口，电层从112Gbps向224Gbps演进，光层200G PAM4和低功耗相干调制技术支持不同距离的组网，IEEE802.3正在制定800GE/1.6TE以太网接口规范。**在弹性无损方面，**海量企业数据上传数据中心，传统固定带宽为量纲的专线模式带宽资源利用率低，通过基于智能化控制的任务式数据传输服务，对网络资源动态调度和匹配，实现TB级数据小时级低成本传输；通过广域流量测量、自适应均衡调度和广域精准流控技术，在实现90%以上的网络带宽利用率的前提下，达成千公里长距传输业务零丢包，实现跨广域分布式AI训练计算效率不下降。

数据中心网络单卡800GE/1.6TE接入带宽+新型以太网：AI大模型规模效应不断显现，集群规模正在从数万卡扩展到数十万卡，要求新型以太网保证大规模组网的通信效率，承载通用计算、超级计算和智能计算负载。**在800GE/1.6TE大带宽接入方面，**预计业界分别在25年/27年商用，网络系统的光侧采用高速VCSEL、高密度光互连等技术；电侧采用高速电接口、低功耗设计和先进信号处理技术，实现高速、低延迟和高可靠性的数据传输；组网上做大交换机扇出，采用新型网络拓扑，支撑更加扁平化的组网架构，降低组网成本，提升网络可靠性。**在新型以太网方面，**AI训练流量流数少、流量大、周期性同步突发，严重的路径冲突导致传统网络吞吐量仅为30-50%，业界的超融合以太、GSE、UEC均通过扩展以太网来提升通信效率。在大规模组网约束下，采用全局流量路径规划，或者将数据包均匀分散到多路径上由最后一跳交换机或接收端网卡进行重排序或乱序接收，都能将解决网络路径冲突问题，将吞吐量提升至95%以上。在AI训练或推理过程中，全归约（Allreduce）是关键的通信操作，通过将归约操作卸载到网络设备上进行计算，可以减少一半的数据传输量，理论上可以将全归约操作的算法带宽提高一倍。

综上，通过100Gbps空口、800GE广域、800GE/1.6TE DCN超宽连接，叠加短距无线融合、弹性无损、新型以太网技术，实现对称大带宽、确定可靠、网络与算力资源高效利用的新联接。

5.2 IPv6+新扩展

连接数和流量高速增长要求网络持续提升服务能力。IPv6具备三层可编程空间：

① 128位地址空间，可标识位置，还可标识转发、VPN、增值业务等所有网络功能；
② 有序的IPv6地址列表可灵活组合网络功能；
③ IPv6扩展头可携带网络资源、检测、组播等信息。

利用IPv6地址空间和灵活可编程扩展头，IPv6+统一并简化了网络层协议，已经提升了上云业务部署效率。未来AI大模型、算力等高速发展，要求IPv6+继续向末梢网络和应用延伸，全面标识应用、算力和数据，提升网络性能、体验、安全和可靠性。

IPv6+联算

算间、算内高速互联需要网络高吞吐、零丢包，提升算力资源利用率，IPv6+无损技术实现智算网络高性能互联。算间网络利用IPv6地址列表编程能力，精确指定拥塞反压路径，避免传统PFC头阻、死锁、风暴等问题，实现千公里长距无损传输；算内网络利用网络级负载均衡、精准流控技术在100%吞吐下保证零丢包。

IPv6+联智

AI入端、推理进园区，端网混合AI应用服务连接数和短流激增，带来确定性交互时延需求，IPv6+APN应用标识，端网协同保障应用体验。利用IPv6扩展头可编程能力，携带APN　ID应用信息，为应用提供精细化网络服务。将网络从基于“IP地址”的网络服务体系升级为“IP地址 + APNID（应用/用户信息）”的网络服务体系，通过云网边端协同保障应用体验。

IPv6+联数

数据要素从生产到消费需要流转路径安全、数据可监管，IPv6+APN数据标识保障数据安全。利用IPv6无限地址空间和扩展头可编程能力，全面标识数据属性类型、数据空间，以保障数据流转过程中的可识、可管和可视，保障数据安全，促进数据的开发利用。

IPv6+联空

卫星网络拓扑高度动态变化、链路频繁切换，IPv6+时变路由保障动态网络可靠性。利用IPv6地址列表编程能力，结合预测性路径技术，实现时变网络路径预先编排，满足卫星网络在高动态时变拓扑、路径快速变化下路径切换不丢包、确定性SLA保障以及99.999%可靠性。

综上，通过IPv6+无损、IPv6+APN应用标识、IPv6+APN数据标识、IPv6+时变路由等技术，在网络性能、体验、安全和可靠性全面提升IP能力。

5.3 网络新智能

新模型架构演进和量化蒸馏等模型轻量化技术发展，为设备部署高性能AI模型增强网元智能感知和决策能力提供了更多技术可能；以Agent为代表的大模型创新范式在理解意图和复杂任务推理方面取得了显著成功，为网络交互式运维和安全运营奠定了基础。

设备新智能

网络传输路径多样性、业务流量模式复杂性加剧，要求设备新智能通过AI主控、AI线卡和AI算力卡提升网元实时感知与决策能力，实现网络优化保障、安全防护和运维闭环。**AI主控板**提供了相对轻量级的AI算力用于控制面快速推理，为设备提供智能节能、攻击检测、拥塞感知等应用。**AI线卡**提供了极轻量级的算力用于转发面实时推理，为设备提供了实时流量感知和异常发现的能力。**AI算力卡**能够提供更高的AI算力用于高性能推理，可以部署流量感知专业模型以服务于流量感知、运维等相对深度算力分析场景。模型通过预训练+调优的训练范式，利用更多的无标注数据对流量建模以提升模型泛化效果，满足联智和联数等场景对业务流量精细化感知准确率>90%的要求。

网络新大脑

不同业务跨域多云部署，对网络资源和体验要求差异大，网络新大脑引入数字孪生和生成式大模型，达成面向业务体验高度自智的AN L4。**在数字孪生方面，**多维高精网络数字孪生为网络新大脑提供推理知识和决策基础。采集异构数据，构建网络、安全、应用、用户、体验等多维数据关联统一建模的网络数据湖；将历史、实时、未来通信数据转换成关联知识支撑网络新大脑决策；提供复杂网络预测式动网仿真评估，共同保证大模型决策精度达成99%+。**在生成式大模型方面，**网络领域大小模型协同实现决策和任务闭环。大模型采用RLHF、LoRA、SFT等微调技术，领域大模型自主迭代能力对未知问题处置实现泛化决策，采用ReAct、反思等技术实现自主迭代；小模型或系统工具接受大模型智能编排调用实现任务闭环，采用prompt工程、思维链COT等技术。网络新大脑实现从AN L3基于面向网络运维的条件自智转向面向业务体验的高度自智，实现业务跨域周级E2E开通，平均故障修复时长（MTTR）小于3分钟，重保业务0质差。

综上，网络新智能通过设备新智能和网络新大脑，设备级实现网络优化保障、安全防护和运维闭环，网络级达成面向业务体验的高度自智AN L4。

5.4 安全新机制

设备内生安全

面向网络攻击手段不断升级，设备内生安全构建一套安全机制，设备既具备自保护能力防攻击，又具备韧性防护能力，异常场景自恢复，优先保障业务运行。**在设备自保护方面，**通过构建防入侵、防驻留、防破坏能力抵御APT攻击。防入侵实时检测业务系统异常行为，发现潜在的入侵行为，采取防御措施；防破坏对内部关键组件进行加密保护、限制修改、隔离等机制，防止被恶意篡改；防驻留防止恶意代码在设备内部长期潜伏，实时监控系统资源占用、可疑进程等，发现异常立即进行隔离和清除。**在设备韧性防护方面，**在遭受攻击或面临其他扰动时保持功能性和服务连续性。对硬件、软件和网络连接的保护，实现备份、容错和冗余设计，确保在主设备故障时能够无缝切换到备份设备，维持业务运行。在攻击发生时快速响应和恢复服务，以最小化潜在的损害并保障业务的连续性。

网络全程可信

量子计算加速传统加密技术破解，后量子密码和量子安全网络是新一代互联网的关键安全技术保障。**在后量子密码（PQC）方面，**网络整合数据空间、隐私计算、联邦学习技术，为数据传输过程提供全方位安全管道服务。网络运用IPSec技术构建端到端线速加密安全传输通道，利用MACsec技术建立设备间的安全连接，并从传统加密算法向抗量子计算攻击的密钥协商和分发算法演进，做到数据零泄露。针对高安全级别用户及其数据，引入抗量子数据加密传输技术，通过实施后量子密码学（PQC）技术加固网络管理层和设备控制层的抗量子能力。**在量子安全网络方面，**通过量子密钥分发（QKD）技术与设备数据转发层的深度融合，实现数据传输的T级抗量子加密保护。考虑到现有网络架构的分阶段演进，初期可以通过外置QKD设施，随后逐步推进至网络设备内置QKD模块，以实现内生量子安全网络，确保高安全级别数据的传输安全。

云网边端一体化安全

黑客利用生成式AI等技术，攻击更为系统和隐蔽，需构筑云网边端一体的安全防御体系。**云侧，**安全智能体具备语义理解和丰富上下文感知能力，进行威胁溯源，狩猎高危入侵，并能构筑红蓝博弈，提前预警和消除风险。**网侧/边侧，**提供基于边界网关和边缘云的下一代SASE安全服务，基于零信任网络接入、高性能一体化安全引擎，实时AI检测，对已知、变种和未知威胁流量检测。**端侧，**下一代EDR针对勒索犯罪，金融欺诈，敏感信息窃取等攻击，通过动静态对抗、溯源图分析、恶意指令检测等技术，实现未知威胁，0day漏洞攻击的快速发现和全网同步。

数据可信流转

构筑数据可识、可视、可管能力，标识数据、确保数据不出信任区域、实现可监管。**在数据可识方面，**利用先进的语言模型（LLM）进行语义理解和数据标注，明确识别数据的安全等级要求。**在数据可视方面，**运用多层数字孪生技术实现对数据流通路径的100%全面可视监管，并通过基于安全因子的集中或分布式路由算法，在计算路径时规避敏感地区和低安全设备。**在数据可管方面，**基于IPv6+的网络策略精确控制数据流通路径，并依托随路验证算法确保路径一致性管理，做到异常传输秒级阻断，保证重要数据不出信任区域边界。

综上，通过设备内生安全、网络全程可信、云网边端一体化安全及数据可信流转技术，构建从设备到网络到关键业务的安全保障体系。

06 “新质互联网”的发展愿景

新质互联网是在IPv6+技术体系的基础上，面向联算、联智、联数、联空等新场景，对数据通信网络在网络架构、技术协议、设备形态、管理模式、安全体系等方面的整体创新。虽然底层IP网络体系架构不会根本变化，但无论是运营商网络还是行业专网，都将产生巨大的变化，进而影响和促进新质生产力的发展和释放。

从发展来看，随着人工智能产业的成熟和发展，未来3-5年将是新质互联网从起步到成熟的关键时期。新质互联网将从局部的算网应用和行业专网场景逐步扩展到运营商大网和更多行业网络，进而重塑数据通信的产业生态和技术生态。