CUBE-Net
新网络 新服务 新生态

中国联通
China unicom

韧性互联网白皮书

中国联通研究院

2026 年 07 月

版权声明

目录

前 言

互联网作为数字经济与关键信息基础设施的核心承载底座，深度支撑政务、金融、能源、算力调度等全领域数字化运转，其稳定存续能力直接关乎社会经济运行与网络空间安全。

当前，网络架构日趋复杂、业务形态持续迭代，常态化设备故障、人为变更失误、流量突发扰动等问题频发，叠加高级网络攻击、极端自然灾害等极限场景冲击，传统以被动防护为核心的网络建设模式，已难以适配复杂不确定环境下的高可靠运行需求。

在此背景下，网络韧性成为下一代互联网建设的核心发展方向，实现从“被动抵御风险”向“感知冲击、弹性承压、持续演进”的理念跃迁。本白皮书立足网络全生命周期保障需求，构建“事前预防、事中控制、事后演进”的闭环韧性能力体系，依托架构、协议、智能管控、安全抗扰、知识图谱五大技术底座，形成多层次、一体化的网络韧性支撑能力，旨在破解传统网络运行脆性难题，为关键基础设施稳定运行、数字经济高质量发展筑牢高韧性网络根基，为行业韧性网络建设、技术创新与规模落地提供体系化参考。

联合发布单位：

中国联合网络通信有限公司，下一代互联网宽带业务应用国家工程研究中心，华为技术有限公司，中国信息通信研究院，中讯邮电咨询设计院，全球固定网络创新联盟（NIDA）。

编写组成员：（排序不分先后）

唐雄燕，曹畅，庞冉，佟恬，高星，王南，赵菁，燕飞，冯海东，张仕勇，黎宇，朱敏晓，董杰，韩淑君，张桂玉，胡中锋。

一、当前互联网面临的挑战

（一）网络常态化运营存在的痛点

随着社会运行与经济活动对互联网依赖程度持续加深，互联网作为支撑数字经济发展的关键信息基础设施，其稳定运行直接关系国计民生。在常态化运营场景下，网络运维团队需保障网络的可用性、性能与安全性，但当前运营模式面临多重结构性挑战。对 2019 年至 2025 年全球运营商发生的 84 起重大事故的统计分析表明，IP 网络与业务复杂性的持续升级是故障频发的根本原因（见图 1）。在故障诱因分布中，业务异常占比最高，占 32%；其次为设备故障，占 25%；动网操作引发故障占比 19%；网络连接故障占比 14%；外部攻击占比 10%。

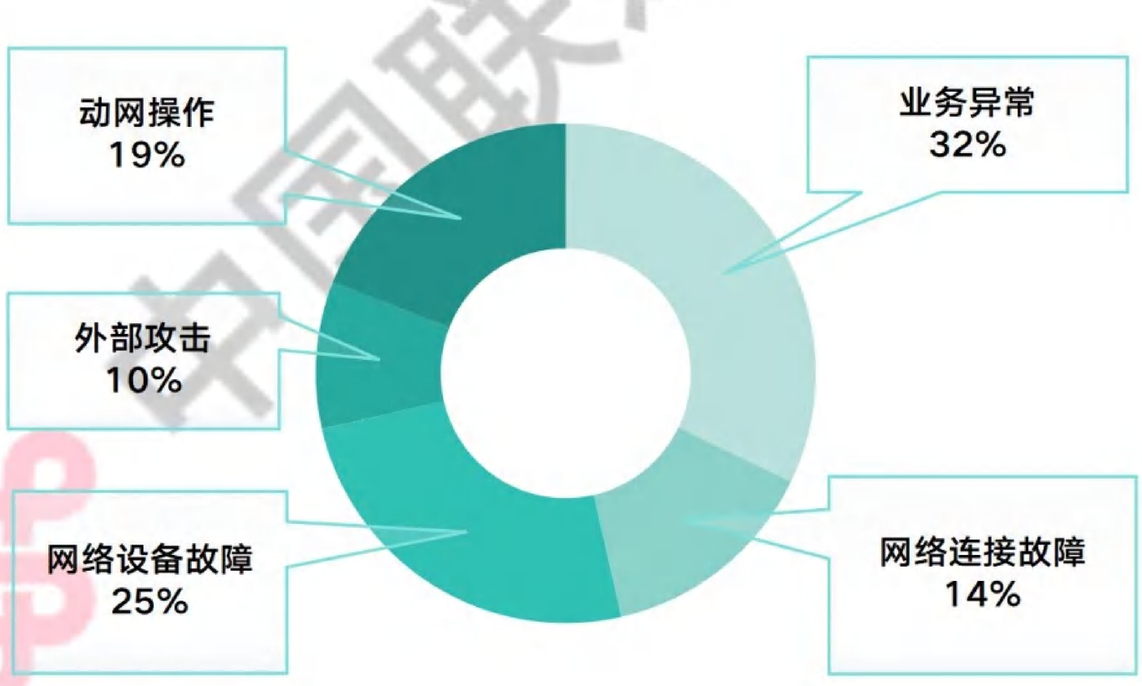

图 1 2019~2025 年全球运营商 84 起重大事故分析

1. 架构弹性不足：冗余缺失与外部冲击暴露承载脆弱性

网络架构层面的缺陷，使基础设施在面对内部流量突变和外部物理威胁时缺乏足够的缓冲能力。在冗余设计方面，部分网络组网不规范，存在单点故障隐患，灾备体系有效性不足。Uptime Institute《2026 年度停机分析报告》指出，电信相关停机从 2020 年的 29

起攀升至 2025 年的 39 起，反映出广域连接基础设施在极端天气、意外损坏等因素下的暴露程度持续上升。在流量承载方面，绿盟科技《DDoS 攻击威胁报告》（2026 版）显示，2025 年超过 500 Gbps 的 DDoS 攻击同比增长 115.72%，年度攻击峰值达 2.6 Tbps，攻击流量的目标加速向企业、教育和公共部门转移。

架构冗余不足与弹性调度能力缺失，使网络在物理损毁与流量冲击的双重压力下面临高概率的全局性服务降级风险。单点故障隐患意味着局部问题缺乏有效的隔离机制，极易横向扩散；而灾备体系的形式化部署则导致故障发生后无法按预期切换，实际恢复时间远超设计指标。网络在常态下呈现"高可用"假象，一旦遭遇超设计阈值的冲击即迅速崩溃。因此，网络架构需从"功能可用"向"损伤可承受"演进，消除单点故障隐患，构建地理分散、异构冗余的多活架构，建立跨域弹性调度能力，将物理安全威胁纳入架构设计约束，并构建分层分级的 DDoS 防御与流量清洗体系，确保极端流量冲击下核心业务带宽不被挤占。

2. 协议标准滞后：底层信任机制脆弱制约内生安全基线

互联网核心协议的设计建立在默认开放、默认信任的基础之上，这一架构性特征与当前高威胁环境严重脱节。在路由层面，BGP 作为互联网互联互通的基石协议，缺乏源认证与路径验证的原生机制，路由劫持、泄漏与误配置事件频发。在域名层面，DNS 体系的信任链同样脆弱，DNSSEC 部署率长期低迷，缓存投毒、劫持与篡改攻击持续威胁用户可达性与数据完整性。此外，传统网络管理协议安全

机制薄弱、IPv4 地址枯竭导致的 NAT 大规模部署增加网络复杂性等问题，均反映出协议标准滞后于安全需求。

协议层面的先天不足与产业升级缓慢相互叠加，使网络在逻辑层面临与物理层同等严峻、却更难防御的系统性风险。与设备故障或光纤中断不同，协议层面的攻击具有隐蔽性强、扩散快、溯源难的特点，且难以通过传统的物理冗余手段缓解。一旦核心路由或域名系统遭受攻击，影响范围可瞬间跨越多个自治域，造成大面积服务不可达，且恢复过程涉及跨组织协作，响应周期极长。因此，协议层需从"默认信任"向"持续验证"转型，推动 BGP 安全扩展的原生部署，加速 DNSSEC 规模化应用，升级网络管理协议的安全基线，并在协议演进中嵌入韧性设计原则，使安全机制成为协议标准的内在组成部分，而非事后补丁。

3. 运维流程失守：人工操作与变更管理缺陷导致故障频发

常态化运营中，人为错误与流程执行不到位是引发各类重大停机的深层共性诱因，集中体现在操作标准化不足和变更管理失控两个层面。Uptime Institute《2025 年度全球数据中心调查》显示，50%的运营商在过去三年内经历过影响较大的停机事件，92%的运营商指出人为错误至少是重大停机的次要诱因。传统运维高度依赖专家经验，缺乏标准化操作流程，与 2020—2025 年均值相比，因光纤和连接事故引发的停机数量增加了一倍以上。升级、割接、扩容等变更操作频繁，但管理执行不到位——较 2024 年，因未遵循程序导致的人为错误中断比例上升了 10 个百分点;近 40%的组织在过去三年中

因人为失误遭受重大中断，其中 85%的事故根源在于员工未能遵守程序或流程本身存在缺陷。

操作随意性与变更管控薄弱直接削弱网络运行的确定性和可预测性，更为深层的影响在于，缺乏标准化和审计机制导致同类错误反复发生，网络运营无法从失败中系统性学习。因此，网络常态化运营亟需提升全流程标准化与自动化能力，制定并强制执行标准化操作流程，构建变更管理的全链路审计与回溯机制，并引入自动化配置与验证工具，在变更下发前进行策略冲突预检和仿真验证，将人为失误阻断在执行之前。

4. 自愈能力薄弱：级联失效、组织协同制约恢复效率

当故障发生后，复杂的网络拓扑、可观测性体系的覆盖盲区与诊断工具的碎片化，会严重拖慢恢复进程。复杂拓扑使单节点故障能够快速蔓延，形成级联效应，跨业务、跨层级的故障溯源链路长，多因素叠加导致根因定位难度持续上升。当前监控体系普遍存在指标数据丰富但关联分析能力不足的问题——单点指标异常难以自动映射到业务影响路径，跨域、跨厂商的日志格式不统一导致数据难以关联分析。同时，常态化运营要求运维人员具备跨协议、跨厂商、跨业务域的综合能力，但当前普遍面临技能断层和知识传承困境，网络、系统、安全、业务部门之间的协作机制不畅，导致问题升级缓慢、责任推诿频发。

上述短板共同加剧了故障感知能力不足、根因定位效率低下、业务恢复周期冗长的系统性困境。基于软件的分布式弹性工具虽在一定

程度上提升了正常运行时间，却增加了运维复杂度，模糊了故障责任边界，使根因分析和中断分类更加困难。传统依赖人工经验的逐层排查模式难以满足快速恢复要求，智能监控体系缺失、自动化根因分析能力不足与故障自愈机制薄弱的问题突出。因此，运维体系需从"人工经验驱动"转向"数据智能驱动"，构建跨域统一的可观测性平台，打造智能根因分析与自动化故障定界能力，建立故障自愈与剧本化恢复机制，并完善跨部门协同流程与知识管理体系，消除组织壁垒，形成故障响应的合力。

综上所述，上述挑战表明，网络常态化运营亟需从事后响应模式转向主动防御与智能运维模式，通过流程标准化、架构弹性化、协议安全化、监控智能化和人员专业化，构建面向未来的网络运营韧性体系。

（二）新兴业务的需求与挑战

数字经济与实体经济加速融合，生成式 AI、AI 智能体、算力网络等新兴业务在创造巨大价值的同时，也从根本上改变了网络流量的特征与运行逻辑。这些业务不再是网络边缘的“外部负载”，而是深度耦合的生产要素，其高动态、强依赖和跨域协同等特性，正将网络推向一个高度不确定性的运行环境，催生对韧性的全新要求。

1. 流量模型突变引发瞬时过载

端边云协同推理、大模型分布式训练等场景推动网络流量流向从南北向为主转向东西向高并发。据测算，到 2030 年全球 AI 流量在网络总流量中的占比将达到 64%，东西向流量增长幅度将超过南北

向流量。截至 2025 年，我国生成式人工智能服务用户规模已达 6.02 亿，普及率 42.8%，终端侧 AI 应用规模化扩展，流量结构变化已成为现实。尤为突出的是模型参数面数据的传输特性：大模型分布式训练中的梯度同步、参数更新、中间激活值等数据单次同步可达数百 GB 至 TB 级，且对丢包极其敏感，千分之一丢包即可能导致训练吞吐量下降超过 30%。

传统基于统计复用的带宽规划与尽力而为的转发机制，难以应对参数面数据的秒级突发与确定性传输需求。局部拥塞若无法被快速识别与隔离，将在短时间内扩散并引发端到端性能劣化，直接冲击高敏业务的完成质量与训练效率。网络在常态下能够承载传统互联网流量，但面对 AI 业务的突发并发时，缺乏有效的过载缓冲与优先级隔离机制，极易从局部拥塞演变为全局性能衰退。因此，网络需具备弹性过载控制能力，建立动态带宽调整机制，实现多路径负载分担与智能选路，构建业务优先级隔离体系，确保参数面数据等高敏流量在拥塞场景下获得确定性传输保障，并构建随流检测与微观性能感知能力，在拥塞初发阶段即触发调度响应，防止劣化扩散。

2. 任务强依赖导致故障快速传播

业务交互模式正从单次请求演变为多节点深度嵌套的任务链。以智能体互联为例，一个用户请求往往需要跨越本地智能体、协作智能体、第三方专业智能体等多个环节协同完成，构成具有强状态依赖的多跳任务链。在端边云协同推理场景中，推理任务质量同样取决于整条算力链路上最薄弱节点与链路的性能。任一节点出现时延增加或连

接中断，故障将沿链路扩散，造成整体任务失败。

这种多节点强依赖关系显著放大了故障传播半径。传统以单点故障隔离为核心的可靠性机制，在此类场景下难以有效界定影响边界与控制连锁反应。一个边缘节点的拥塞或闪断即可导致推理结果劣化甚至任务中断，且故障沿任务链向上游和下游双向传导，使影响范围远超故障原点。网络在设计上缺乏对业务上下文和任务链全生命周期状态的感知能力，无法实施精准的故障阻断与业务逃生。因此，韧性建设需要从保障单一连接质量，升级为面向任务链的全局韧性能力，构建业务上下文感知机制，建立快速故障隔离能力，实现自愈切换与任务重编排，并引入任务级服务质量保障，对关键任务链提供端到端的时延、丢包与带宽保障。

3. 安全边界消解增加防护难度

大模型训练上云、智能体间互联等业务模式使模型参数、企业私有数据等敏感信息频繁在终端、边缘、云端及不同信任域之间流动，传统基于物理位置和固定网络边界的安全模型逐步失效。据 IBM《2025 年数据泄露成本报告》，13%的受访企业明确遭遇过 AI 模型或应用的安全漏洞，其中 97%尚未部署 AI 访问控制机制，导致 60%的 AI 安全事件造成数据泄露、31%引发业务中断。安全能力建设显著滞后于业务扩张速度，已成为制约韧性体系发展的结构性瓶颈。

安全边界瓦解意味着网络在遭受攻击或节点受侵时缺乏快速收敛能力，安全事件直接转化为业务中断与数据泄露，动摇韧性体系的信任根基。传统的外挂式安全防护在跨域流动场景下存在覆盖盲区，

一旦传输路径穿越多个信任域，中间节点的攻陷即可导致数据暴露。网络在设计上将安全视为边界问题，而非内生属性，导致在开放互联环境中难以维持基本可信的通信保障。因此，网络需构建攻击面动态收敛与内生安全能力，建立跨域持续认证机制，实现参数面数据与私有数据的端到端加密和细粒度隔离，构建受损组件快速隔离与服务恢复能力，并将安全能力内生于网络架构，使安全从外挂式防护转化为网络运行的固有属性。

综合来看，新兴业务带来的流量突发、任务强耦合与安全信任边界瓦解，正推动网络韧性从关注统计意义上的平均无故障时间指标，向构建涵盖弹性过载控制、快速故障隔离与自愈、攻击面动态收敛与内生安全的动态防护体系演进。韧性不再只是网络自身的可靠性属性，而已成为保障业务连续性的核心能力。

（三）网络极限场景的挑战

现有网络架构的规划设计、部署策略与运维规程，主要依据常规社会环境与自然条件下的业务需求制定。极端自然灾害、大规模网络攻击等极限场景下的生存性要求，尚未作为系统性约束融入网络体系的设计原点。一旦面临此类极端事件，关键节点的脆性失效可能导致千万级乃至亿级用户同时失联，通信中断的后果将穿越信息域，直接冲击应急指挥、社会动员、经济运行和国家治理，形成跨域级联的系统性风险。网络基础设施在极限场景下维持最低服务能力、快速感知损伤并自愈恢复的能力，已成为国家战略层面的刚性需求。

1. 大规模网络攻击场景下的多向量打击与防御困境

通信基础设施作为数字经济的核心底座，其战略价值使其成为极限场景下网络攻击的首要目标。攻击手段已从传统的流量消耗型DDoS，拓展为数据擦除、工控系统破坏、DNS 与路由劫持、供应链污染等多向量协同作战。攻击目标从短暂中断服务，升级为永久性瘫痪系统、窃取关键数据、破坏网管控制体系及长期潜伏渗透。关键节点的层级集中性与上游依赖效应，进一步放大了攻击的级联影响——一个核心枢纽的沦陷即可引发大面积区域性退服，且修复对专用设备、技术力量和恢复时间的要求极高。

多向量攻击的协同趋势加剧了防御难度。攻击方可通过网络攻击先期瘫痪态势感知与指挥调度系统，制造感知盲区，为后续更深层次的渗透或破坏创造条件；也可利用物理层面的基础设施暴露性，将网络攻击与实体设施损毁相结合，形成复合式打击。通信中断还会产生次生放大效应，局部断网迅速传导为社会恐慌、交易停摆和指挥链路断裂，形成攻击破坏与秩序失稳之间的恶性共振。因此，面对多向量协同攻击，网络需构建纵深防御与动态收敛能力，关键节点需具备分布式冗余与去中心化生存能力，建立跨攻击向量的统一态势感知与协同处置机制，具备攻击面快速收敛与受损组件自主隔离能力，以及快速重构与数据恢复能力，在系统遭数据擦除或配置破坏后能够在分钟级乃至秒级内恢复核心功能。

2. 极端自然灾害场景下的全面冲击与运维失效

全球气候变化导致极端天气事件的频次与强度持续上升。与人为

瞄准的破坏不同，自然灾害对通信网络的冲击具有影响范围广、多节点并发失效和恢复环境恶劣等特征。基础设施层面，洪涝可致机房淹没与电力中断，地震可造成管线断裂与铁塔倾倒，冰雪可引发大面积倒杆断线，台风可摧毁室外基站和架空光缆。此类灾害的共性是损伤呈面状分布，多个节点可能同时失效。当主备节点同处灾害影响范围，或备用电力依赖同一受损电网时，冗余体系将同步失效。业务层面，极端灾害期间业务需求出现急剧分化与瞬时聚集——公众求救和报平安等基本通信需求形成远超常态的并发呼叫高峰，而应急指挥与救援协同等关键业务同样需要高优先级保障。运维层面，灾害导致的现场不可达、管理通道中断和故障信息缺失，使传统依赖人工到场和手动排查的运维模式基本失效，远程管理手段随通信中断而丧失。

传统基于单点故障假设的冗余设计在面状损伤场景下难以发挥预期作用。在大量网络资源已遭摧毁的约束下，有限的幸存容量若无法动态调配，将同时陷入公众基本通信与应急救援通信的资源争抢困境。传统基于预设优先级的刚性分配机制难以匹配此类高度动态的保障需求。更为严峻的是，当通信中断本身即是灾害后果的一部分时，网络在无人值守条件下缺乏自主故障检测、损伤评估、拓扑重构和业务恢复能力，运维体系事实上处于能力归零状态。因此，面对极端自然灾害，网络需构建面状损伤下的生存与自主恢复能力，冗余设计需从"单点备份"升级为"地理分散式韧性布局"，具备动态业务优先级调度能力，在资源极度受限时保障应急救援通信的最低可用性，具备无人值守条件下的自主运维能力，通过内置的故障自检测、损伤自评估、

拓扑自重构和业务自恢复机制维持网络最低服务能力，并具备快速现场恢复与应急接入能力，在基础设施损毁后通过便携式应急设备、空天地一体化补充链路等手段快速重建关键通信节点。

综上所述，极限场景的挑战是网络韧性建设的严苛检验。网络空间的竞争正从单纯追求性能与效率，转向以生存与恢复能力为核心的韧性较量。将极限生存能力作为网络架构设计的基础性约束，进行全生命周期的系统性建设，是应对这一挑战的必要路径。

二、韧性互联网核心理念与研究现状

（一）政策背景与发展回顾

（1）概念起步阶段（2010-2012 年）

2010 年，MITRE 发表《构建安全的、弹性的架构以实现网络使命保障》（Building Secure, Resilient Architectures for Cyber Mission Assurance）论文，首次提出“不以彻底防攻破为目标，局部受损仍保障核心业务持续运行”的架构思想，开启了网络弹性架构领域的研究。2011 年，MITRE 正式提出网络弹性工程框架（Cyber Resiliency Engineering Framework），为韧性网络的技术研究与实践提供了基础框架。2012 年，世界经济论坛（World Economic Forum，WEF）描述了系统和组织抵御网络事件的能力，进一步推动了韧性概念的传播。

（2）政策升级阶段（2013 年-2015 年）

2013 年，韧性网络的政策定位显著升级。美国总统奥巴马签署《关键基础设施的安全与弹性》总统政策指令（PPD-21），明确将韧性与安全并列看待，作为保障关键基础设施的两大重要方面。美国国防科技委员会发布《Resilient Military Systems and the Advanced Cyber Threat》报告，强调建立安全系统需关注网络弹性。美国国防部发布《国防部网络、系统和数据防卫战略 2013-2020》，将“建立弹性的网络防御姿态”列为四大战略焦点之首，标志着韧性网络上升为国家战略层面的核心议题。

（3）目标明确阶段（2016-2020 年）

2016 年，世界经济论坛治理与信任部主管撰文指出，网络弹性与网络安全存在本质区别，厘清了两者的边界。2017 年，ISO 国际标准化组织将韧性定义为“组织在不断变化的环境中吸收和适应的能力，使其能够达成自身的目标，从而生存下来并实现繁荣”；MITRE 则提出网络韧性的设计原则，包括战略原则（聚焦共用或关键资产、支持敏捷和自适应架构、减少攻击面、限定部分资源失陷、预料对手演进）和结构原则（战术原则），为韧性网络的设计提供了方法论指导。2018 年，美军网络司令部发布《获取并维持网络空间优势——美国网络司令部的指挥愿景》，强调增强自身韧性以抵御近邻、持续接触对手；美国国防部发布《国防部网络战略 2018 版》，明确提出在平时强化自身网络和系统的安全性与弹性，进一步提出了网络弹性指标、有效性度量和评分模型，完善了 CREF（网络弹性评估框架）。2019 年，美国国土安全部下属的 CISA 发布《关键基础设施安全与弹性的部门指南》，美国国防部发布《国防部数字现代化战略 2019-2023 财年》，提出 4 大目的、27 个目标，将韧性网络纳入数字化转型的核心框架。

（4）行业聚焦阶段（2021-2026 年）

2021 年，RSA 网络安全大会将“Resilience（韧性）”定为大会主题，标志着行业对韧性网络的关注度达到新高度。2026 年，国际电信联盟（ITU）将世界电信和信息社会日主题定为“数字生命线——在互联世界中增强韧性”，进一步推动全球范围内韧性网络的建设与实践。

（二）韧性互联网的核心理念

网络韧性已成为全球网络安全与网络建设领域的核心战略共识，各国权威标准化、行业组织机构基于自身研究视角与应用场景，对韧性网络的内涵作出界定，虽表述各有侧重，但核心理念高度统一，均打破了传统网络“被动防御、零故障苛求”的固有思维，聚焦网络在复杂扰动、恶意攻击与突发故障下的存续与服务保障能力。

美国国家标准与技术研究院（NIST）：容纳 IT 资源的系统针对有害情况、压力、攻击和危害等具备预先处理、承受、恢复和适应的能力。

欧洲网络与信息安全局（ENISA）：网络在面对正常运行的各种故障和挑战时，提供并保持可接受的服务水平的能力。

中国通信标准化协会（CCSA）：IP 承载网网络韧性（IP Bearer Network Resilience）是指 IP 承载网在遭受各种可能的故障、攻击或其他类型的扰动时，能够维持其功能、性能和服务质量的能力。一个具有高韧性的网络可以在遭受攻击或故障时快速恢复正常运行，而不会对网络中的数据、用户或资源造成过大的损害。

综合国内外权威定义的共性特征，结合当前互联网全域互联、动态演进、攻防交织、故障多发的运行现状，本白皮书对韧性互联网作出统一定义：韧性网络(Resilient Network)是一种旨在保障业务连续性和网络稳定性的先进网络体系。它不再局限于被动地抵御和消除每一个潜在威胁，而是通过构建一套具备智能感知、主动防御、快速恢复与持续适应能力的动态闭环系统，确保在面对故障、攻击或极端环

境时，能够将业务影响和损失控制在可接受范围内，实现从“被动防护”到“主动适应”的范式转变。

相较于传统网络安全理念，韧性互联网的核心内涵实现了根本性升级：防护重心从“全力规避、消除各类威胁与故障”，转变为“包容有限扰动、承压存续运行”；建设目标从“追求网络绝对安全稳定”，升级为“复杂不确定环境下的业务连续性与网络可生存性”，构建起“事前预判规避，事中承压可控、快速恢复、事后迭代优化”的全生命周期网络安全韧性能力体系。

（三）韧性互联网的核心特征

从核心定义与能力边界来看，韧性（Resilience）是可靠性、安全性的综合扩展，更强调网络在不确定性、复杂性、对抗性环境下的整体表现。其中，可靠性（Reliability）以规避故障发生为核心目标，聚焦常态运行场景下的网络运转的稳定性与持续性，通过规范化架构设计、设备冗余部署、链路优化等手段，最大限度减少运行中断、故障宕机等问题，保障网络基础服务持续可用，是网络稳定运行的基础保障能力。安全性（Security）以抵御内外威胁、防范恶意入侵为核心目标，聚焦网络风险的前置拦截与规避，通过防护技术、安全策略、权限管控等手段，防范黑客攻击、病毒入侵、数据泄露、资源篡改等内外安全风险，保障网络数据、资源的完整性、保密性与可用性，是网络安全运行的核心防护能力。韧性作为高阶综合能力，承认复杂网络环境下故障、攻击、扰动无法被完全杜绝的客观现实，核心目标是实现风险扰动下的功能存续与快速复原。其核心逻辑不再局限于事前

规避风险，更强调在故障发生、防御失效、系统遭受冲击的场景下，通过动态适配、风险吸收、承压运行、快速自愈等机制，维持网络核心业务与基础功能不失效，并快速恢复全域正常运行状态，是复杂对抗环境下保障网络可持续运行的关键核心能力。

从能力运行周期来看，可靠性与安全性属于典型的事前防御能力，核心价值在于通过前置设计、前置防控、前置加固，在风险、故障、攻击发生前完成规避、拦截与消除，从源头降低网络异常概率；而韧性能力还包括事中承压响应、事后迭代恢复，聚焦传统事前防御失效后的兜底保障，填补了传统网络能力体系的短板，实现了网络从“规避风险、杜绝异常”到“包容风险、承压存续、快速复原、持续优化”的理念跃迁。

基于韧性互联网的核心定义与能力内涵，结合复杂对抗场景下的网络运行保障需求，韧性网络主要包含感知性、抵御性、恢复性、适应性、演进性五大核心特性。

感知性：实时、准确地感知网络状态、异常流量和潜在威胁。

抵御性：在扰动发生时，网络能够承受并减少损伤。

恢复性：故障/攻击发生后，快速恢复业务至可用状态。

适应性：从历史事件中学习，持续优化防御和响应策略。

演进性：随技术迭代和威胁演变，主动升级架构和能力。

（四）韧性互联网的研究进展

网络韧性的研究方向主要包括：组网韧性，研究关注网络结构本身对故障的容忍能力；控制面韧性：当前学术界研究最活跃的领域之

一，包括对路由安全增强机制和控制平面稳定性的研究；数据平面韧性：随着业务需求的变化，研究重点正在从传统网络的负载分担和快速倒换转向对短时拥塞、时延抖动和瞬时丢包的响应与缓解。此外，在研究中还呈现安全与韧性融合的趋势。

全球各国及权威标准化组织已围绕网络韧性开展一系列理论研究与标准体系建设，为韧性网络的架构设计、能力界定、场景落地等方面提供了重要理论支撑与技术依据。ITU-T《网络安全概述：信息安全技术-网络安全：网络弹性-定义、术语和模型》，明确了网络弹性的定义和生命周期模型；ITU-T L Suppl. 35《网络弹性和恢复的灾害管理框架》明确提出了网络韧性与恢复的灾害管理框架，确立了应对物理灾难的五大战略支柱：物理冗余、网络拥塞控制、快速修复、替代设施以及架构鲁棒性；ISO/IEC《信息安全-网络安全-网络弹性-第 1 部分：术语和定义》，提出“PDRR-A”能力框架，丰富了韧性网络的能力维度；Gartner《网络弹性架构指南》，提出网络弹性的四大支柱，为企业架构设计提供了指导；ITU-T SG13《面向未来网络的韧性场景及能力要求》，定义了未来网络韧性的通用能力考量和特定能力考量，为未来网络韧性的技术发展指明了方向。IETF 通过其 SAVNET 和 SIDROPS 工作组，在域间路由和防欺骗领域取得了历史性突破，推动 ASPA 技术从理论走向生产环境部署。

国内标准组织 CCSA 牵头制定了两项核心标准，推动 IP 承载网韧性的标准化进程。《IP 承载网网络韧性技术要求及评估方法》定义了 IP 承载网网络韧性等级的分级标准、网络韧性评估总体框架和网

络韧性能力评估标准。《IP 承载网网络韧性评估的测试方法》旨在为 IP 承载网韧性的评估提供可操作的测试规范，进一步推动完善国内韧性网络标准体系的落地性。学术界也在将控制论、复杂系统理论以及生态韧性理论引入通信网络的韧性研究。

产业界积极响应战略共识，推出面向网络韧性的构建能力与解决方案。思科（Cisco）提出 Cyber Resilience（网络韧性）理念，并在网络韧性白皮书中针对新业务场景提出网络韧性的七种能力，为企业级韧性网络建设提供了实践路径。华为提出韧性网络解决方案全景图，构建了从识别到恢复的全套解决方案，聚焦“防得住”“扛得稳”“可逃生”的核心目标，解决金融、能源、交通等多个行业面临的韧性问题，助力客户打造具备全生命周期韧性能力的网络系统。

三、韧性互联网总体架构

面向未来网络高可靠、高可用、高生存性的发展需求，针对网络运行常态化故障、突发性冲击、极端化场景等多元风险挑战，韧性互联网以“**固本御危、承压稳运、应急存续、迭代优化**”为核心目标，构建覆盖“**事前预防、事中控制、事后演进**”全生命周期的韧性能力体系。依托架构韧性、协议韧性、智能管控、安全抗扰与知识底座的协同增强，韧性互联网可对各类网络风险形成系统性、整体性、兜底性支撑能力，实现网络在常态故障、突发冲击与极端场景下的持续稳定运行，为关键业务提供可靠承载保障。

图 2 韧性互联网系统架构图

韧性互联网以全生命周期闭环能力建设为核心，形成事前预防、事中控制、事后演进三阶段递进式能力体系，构建“防御—感知—隔离—恢复—优化”的可持续迭代闭环（见图 2），实现网络韧性能力随运行实践持续升级。韧性互联网的核心目标与能力映射：

（1）**事前预防阶段**：核心目标是构建韧性防御能力，减少网络

故障发生概率，实现固本御险。在架构设计和容灾保护能力方面：从水平维度构建从本地保护到路径保护的多粒度冗余与多样性，从垂直维度实现网络各层冗余保护与跨层、跨域协同，通过过滤和吸收下层异常事件，为业务存续提供兜底保障。

（2）事中控制阶段：核心目标是当业务受损不可避免时，将影响程度最小化，实现承压稳运，应急存续。通过状态感知、隔离防扩散、事件恢复三大核心能力，实现故障的快速发现、精准隔离与业务快速恢复，防止故障扩散并降低业务中断影响。针对极端故障、高强度攻击、极端环境等极限场景，保障关键业务 100%存续运行。事中阶段主要依托三大核心能力筑牢兜底屏障：

状态感知能力：通过对设备层、网络层、链路层、协议层、VPN层及业务层的多维度感知，实现对网络状态的全面掌控，并支持异常状态与事件的检测、回溯，为故障处置提供精准依据。

隔离防扩散能力：要求网络中各个组件都具备隔离和遏制异常故障事件的能力，通过限制故障影响范围、隔离故障事件，有效缩小故障域或故障波及范围。

事件恢复能力：通过网络故障的定位、诊断与恢复技术，结合包含团队协作、工作流程设计、应急预案与资源准备的恢复管理流程，支撑故障快速修复与业务复原。

（3）事后演进阶段：通过故障复盘、根因分析、经验沉淀、策略迭代机制，优化网络体系与处置流程，实现“处置一次、优化一轮、提升一级”的能力闭环，推动网络韧性能力动态演进、持续升级。

为支撑上述全生命周期韧性能力，韧性互联网搭建多层次、一体化的韧性技术支撑体系，涵盖架构韧性、协议韧性、智能管控、安全抗扰、网络知识五大核心能力底座。

一是架构韧性，筑牢拓扑层抗毁基础。采用扁平化 Spine-Leaf 网络架构、搭配多层逃生路径设计与跨域容灾方案，通过物理链路冗余、设备资源池化调度、路由多样性规划等手段，从网络拓扑层面提升抗毁与容灾能力，减少单点故障影响范围。

二是协议韧性，激活网络层快自愈能力。通过控制平面路由协议的资源保护、故障隔离机制保障系统稳定；通过转发平面快速重路由、多路径负载分担等技术提升故障切换与容错能力；并结合 IFIT 等高精度检测协议强化全网可观测性，构建网络自愈抗扰、风险隔离的底层协议支撑。此外，基于 SRv6、BFD 等协议技术，实现亚秒级故障检测、毫秒级路径切换与业务快速倒换，同时强化业务隔离、流量调度与故障溯源能力，在协议层面为网络提供快速自愈与隔离防扩散能力。

三是智能管控，赋能网络运维智能自治。融合 AI、数字孪生等技术，构建“可视-仿真-预测-自愈”一体化智能管控能力，实现全网状态实时感知、变更与故障仿真预演、潜在风险预测预警、故障自动定位与闭环处置，推动网络运维从被动响应向主动预防、智能自治演进。

四是安全抗扰，构建网络内生防护屏障。抵御内外部各类安全威胁，提升网络在强对抗、高扰动场景下的抗毁存续能力。

五是知识底座，提供体系化迭代动能。以网络运营知识图谱为核心，沉淀故障处置、变更优化、架构演进等全场景运营知识，为故障定位、根因分析、策略优化提供数据支撑，推动网络韧性能力的持续迭代升级。

五大技术相互协同、层层支撑：架构韧性与协议韧性构建网络的“硬防护”基础，智能管控和安全抗扰提供“软赋能”手段，知识底座则为韧性体系的持续演进提供数据与经验支撑，共同实现“常态少故障、异常快处置、极端可存续”的韧性目标。

四、韧性互联网关键技术

（一）网络架构韧性：筑牢拓扑层抗毁基础

架构韧性是互联网韧性体系的底层基础，以保障业务连续性为核心目标，针对设备故障、链路中断、节点失效、局址受损、流量突发、配置异常、网络攻击等多元风险场景，开展网络架构、资源配置、保护恢复与运维协同的一体化设计，赋予网络先天抗毁、容错、容灾能力。

架构韧性设计需围绕预期、承受、恢复、适应四个核心阶段，综合运用隔离、冗余、多样性、故障域控制、爆炸半径收敛、跨层跨域协同恢复等关键技术手段，从底层架构层面构建网络持续承载、稳定运行与长期演进能力（见图 3）。

针对不同网络层级与业务场景的组网特征、承载需求和风险差异，架构韧性实行差异化、精准化的保障策略，实现能力按需适配。骨干网聚焦抑制大范围级联故障，强化跨区域路径多样性部署、核心节点与控制节点解耦设计，有效阻断全局故障扩散，保障全网骨架稳定；互联网出口立足开放边界安全防护，重点提升路由异常抵御、大流量攻击承压与出口网关冗余备份能力，筑牢网络对外互通的安全防线；城域汇聚面向大规模高密度接入场景，强化故障域收敛管控、环网风险治理与邻域快速逃生能力，杜绝局部故障向上蔓延、影响全域；移动承载网聚焦移动通信业务特征，强化低时延低抖动传输、高精度时钟同步、海量基站接入保障与控制面/用户面分级防护能力，支撑移动业务高质量稳定承载；政企云专线场景重点强化租户安全隔离、确

定性 SLA 保障、业务与承载解耦、故障一键切换能力，精准适配政企行业高可靠、高专属的业务需求；算间网络围绕算力调度场景，依托大带宽低时延传输能力、大象流冲击抑制机制、跨数据中心多路径冗余与多站点容灾部署，保障跨域算力调度持续稳定、可靠可控。

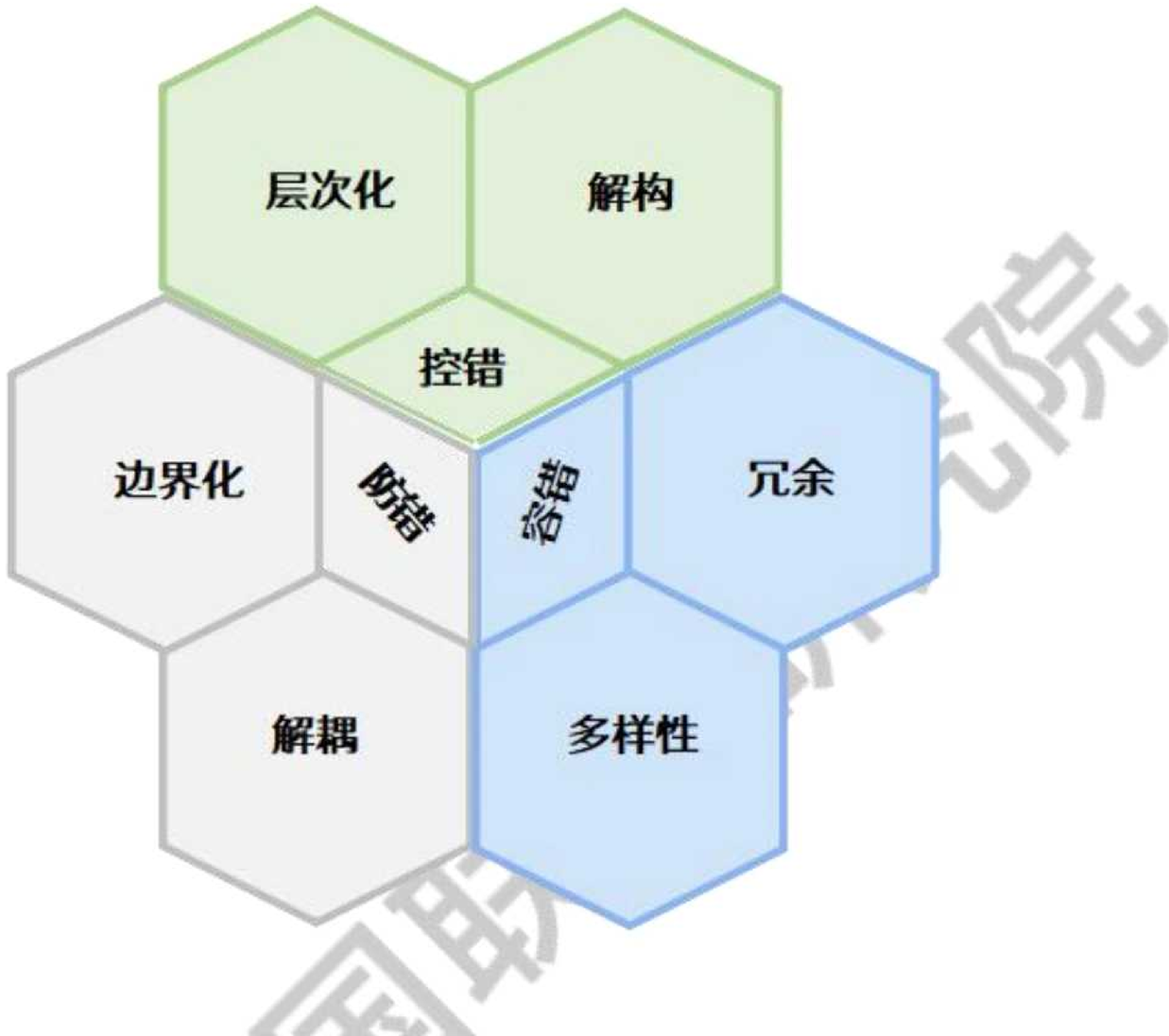

图 3 架构韧性规划原则

架构韧性需兼顾稳定性、可控性、可演进性。在预期阶段，扰动发生前完成风险识别、组网优化、边界防护、容量预留，从源头降低故障发生概率；在承受阶段，扰动发生时通过异构冗余、故障隔离、资源调度、业务分级保障，有效抑制故障扩散，维持关键业务连续运行；在恢复阶段，业务受损后支撑跨层跨域定界、毫秒级路径切换、业务有序回切与修复，最大限度缩短业务中断时长；在适应阶段，基于历史故障复盘、仿真测试验证与风险动态变化，持续优化架构设计、资源布局、保护策略与运维流程，推动网络韧性水平迭代升级，为互联网长期高质量发展提供坚实架构支撑。

（二）网络协议韧性：激活网络层快自愈能力

网络协议是实现全域互联互通的核心基石，其自身的韧性水平与智能化程度，是构建高可靠网络架构的关键要素。随着网络拓扑复杂度的持续攀升及业务应用场景的日趋多元，网络协议体系正经历系统性演进，应构建多层多域的多协议韧性体系（见图 4），以实现更高阶的可靠性、弹性及可观测性。

在控制平面，传统路由协议（如 BGP、IGP）通过引入多重韧性机制强化自身稳定性。一是实施资源保护，对 CPU、内存及会话数等关键资源进行精细化管控与动态限速，确保在流量突发或网络攻击等压力场景下核心控制功能的可用性；二是强化故障隔离，依托独立进程重启与故障域隔离技术，实现局部故障的快速遏制与业务无损恢复，提升系统整体鲁棒性。在转发平面，结合快速重路由（FRR）机制，显著提升路由收敛速度，支持路径故障时的毫秒级备份切换；同时，利用 ECMP 等多路径负载分担技术，实现流量的智能调度与均衡分布，在提升资源利用效率的同时，提升了对单点及多点故障的容忍能力。此外，为支撑精准快速的故障感知，BFD、TWAMP、IFIT 等高性能检测与诊断协议被广泛部署，持续强化网络状态的可观测性，为故障感知、抵御及业务恢复提供关键数据支撑。

以 SRv6 为代表的新一代 IP 架构，进一步强化了数据平面的智能管控与韧性承载能力。依托端到端可编程路径特性，SRv6 构建了高度敏捷且弹性的数据面体系：在常态运行下，支持基于业务策略的智能选路、多路径负载分担与冗余传输，优化资源调度；在故障场景

下，基于预置策略迅速启用备份路径，实现业务的无感知切换。

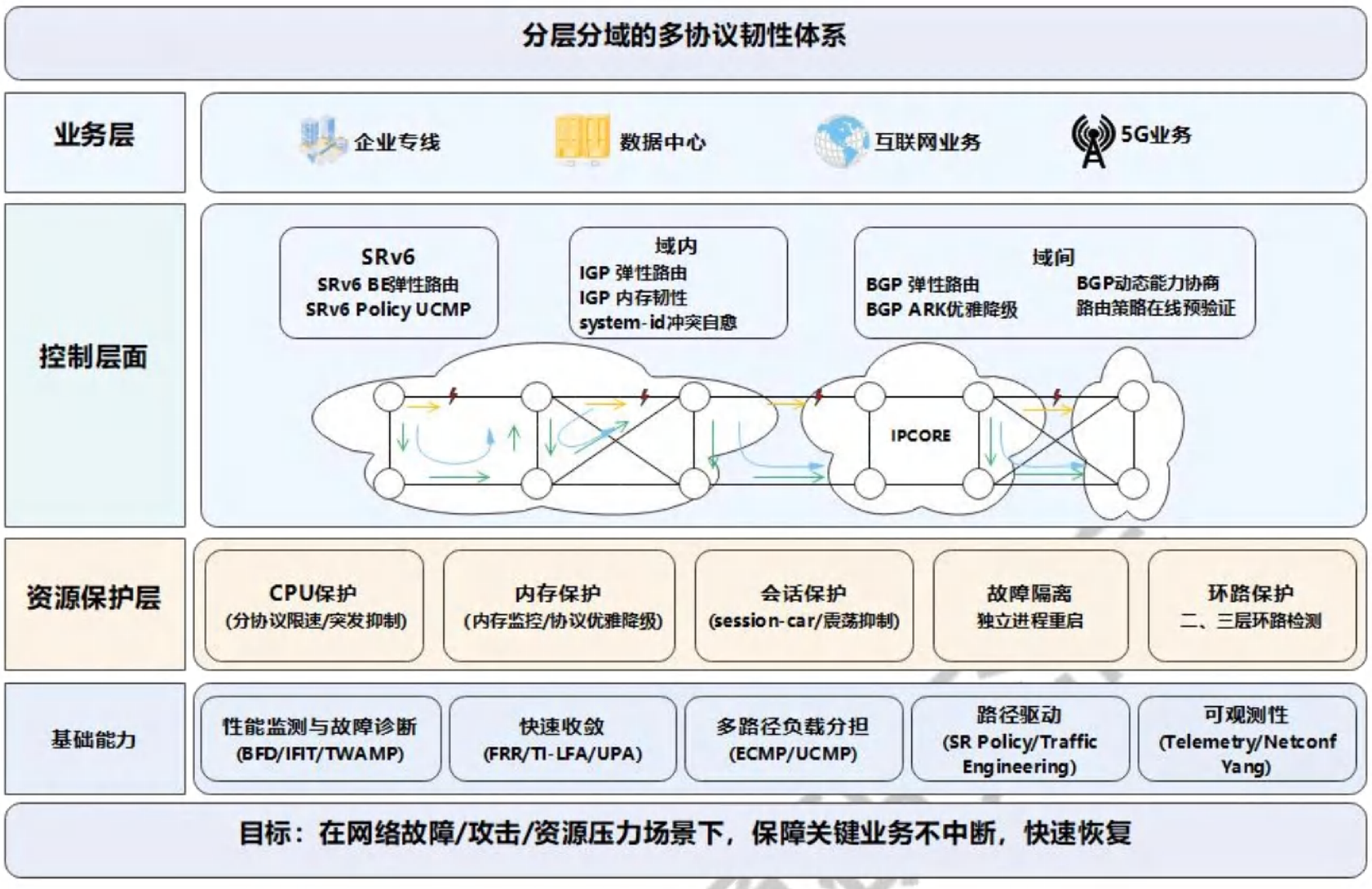

图 4 多层多域的多协议韧性体系

综上所述，网络协议正从资源管控、会话维持、故障隔离、快速收敛及可观测等多个维度，系统化构建其韧性能力。传统协议持续夯实可靠性基底，而 SRv6 等新型协议则从架构层面推动网络向智能化、自适应与高业务连续性方向演进，共同为建设高韧性互联网奠定坚实的协议基础。

（三）网络智能管控：赋能网络运维智能自治

网络智能管控是提升互联网韧性的关键技术，涵盖四个核心能力维度：全域实时感知与弹性调度构成数据基础和执行手段，全意图驱动网络实现运维范式升级，网络和业务快速自愈提供故障恢复能力，持续学习与适应演进保障长期有效性。四者形成"孪生推演—智能决策—闭环执行"的协同架构，贯穿基础设施健康管理、网络弹性调度

到运营编排的全链条，使韧性能力从离散补救措施转化为内生于网络运行全过程的系统特性。

1. 全域多维实时感知与弹性调度

网络感知能力决定异常发现的时效性、故障定位的精确性和风险预判的准确性，是韧性体系中事前预防环节的核心支撑。面向韧性网络全链路管控需求，全域感知围绕设备运行状态、链路传输质量、协议运行状态、业务策略配置、端到端业务流特征五大维度开展数据采集，完整覆盖从基础设施到上层业务的全层级运行画像。

传统采集模式受限于分钟级时延、粗粒度采样和多厂商数据壁垒，无法捕捉瞬态异常与短时微故障。新一代感知体系采用双层协同架构：上层通过标准化数据建模与高效传输机制，变被动拉取为主动推送，实现秒级乃至亚秒级全网宏观态势采集，支撑日常监控与异常初筛；下层通过随流检测技术，将轻量级检测标识嵌入业务报文，逐跳采集单流转发时延、丢包、队列深度等微观数据，精准定位间歇性拥塞和微突发故障，实现从宏观告警到单流定界的快速闭环。

智能决策引擎基于实时感知数据完成多维度态势关联与策略寻优，驱动由轻及重的三层弹性调度机制：

（1）流量调度：依据实时链路质量与负载状态，动态调整业务流路径，实现多路径负载分担与拥塞快速规避。当检测到链路质量劣化或节点过载时，自动触发流量迁移，将受影响业务切换至最优路径，保障关键业务传输确定性。该机制作用于路径层面，响应速度达秒级。

（2）资源调度：根据业务优先级与实时资源占用，动态分配带宽、

缓存与计算资源。在突发流量冲击或资源争抢场景下，优先保障高敏业务的资源需求，实现差异化服务质量保障。该机制作用于资源层面，响应速度为秒级至分钟级。

（3）拓扑调度：在节点故障或链路中断场景下，基于实时感知数据快速评估网络损伤范围，自主生成拓扑重构方案，激活备用路径或动态建立新转发路径，缩短业务恢复时间。该机制作用于结构层面，响应速度为分钟级。

上述感知与调度能力的深度融合，使网络具备从微观异常识别到宏观资源调配的全域闭环控制能力。面向未来，随着业务场景的持续复杂化和极限挑战的常态化，感知精度将向毫秒级演进，调度决策将向预测式、自治式升级，最终实现网络在无人干预条件下对各类扰动的自适应响应与自愈恢复，使韧性从被动防御能力转化为网络的内生属性。

2. 全意图驱动网络

网络运维管理的复杂性是影响网络韧性的重要因素。大规模网络涉及路由策略、服务质量策略、安全策略、切片配置等多维度参数的协同设置，人工操作难以确保配置的正确性与一致性，配置错误已成为导致网络中断的主要人为因素之一。意图驱动网络推动运维从命令式配置向意图式管理演进，通过自动化手段消解配置复杂性带来的韧性风险。意图驱动网络包含四层功能模块：

（1）意图翻译层：将管理员通过自然语言或结构化模板表达的业务需求解析为网络可执行策略；

（2）策略编排层：将翻译结果映射为具体配置参数，生成标准化配置模板；

（3）自动化部署层：将配置模板下发至相关设备并验证生效状态；

（4）闭环验证层：持续监测网络运行状态，比对实际性能指标与意图目标，自动执行偏差校正。

多业务并发部署时，内置冲突检测与仲裁机制在配置下发前对策略进行预验证，识别资源重叠与优先级冲突，依据业务优先级、申请时序等规则进行化解，保障复杂场景下多业务稳定共存。

上述意图驱动机制将业务需求与网络配置直接贯通，显著降低人为操作失误概率，提升配置一致性与变更可控性。面向未来，意图表达将向自然语言深度理解演进，策略生成将向跨域协同、全局最优方向升级，最终实现业务需求到网络行为的零延迟、零差错自动映射，使网络运维从人力密集型转向智能自治型。

3. 网络和业务快速自愈

快速自愈是韧性网络区别于传统高可用网络的关键特征。传统高可用主要依靠冗余部署实现故障时的静态切换，而韧性网络强调故障发生后的动态感知、精准诊断与自主恢复，构建分钟级乃至秒级自愈闭环是实现高可靠运营的必要条件。

数字孪生体在虚拟空间中对物理网络进行高精度镜像，为故障复盘、处置推演和极限场景演练提供零风险仿真环境，支撑自愈策略的预验证与优化。在此基础上，自愈闭环包含三个核心环节：

（1）故障发现与定界：智能根因分析技术融合全网运行数据、告

警信息与遥测数据，采用多模态数据融合和时序关联分析，对故障特征进行智能匹配与精准定位。在告警风暴场景下，算法自动识别告警的拓扑关联与时序关系，将大量衍生告警收敛至根因事件，将传统人工排查的小时级定位时间压缩至分钟级。

（2）恢复决策与执行：剧本化自动恢复机制针对常见故障场景预定义标准化处置流程，明确触发条件、执行步骤、预期结果与回滚方案。故障触发后，系统依据匹配的根因类型自动选择对应剧本，按序执行配置修复、端口隔离、流量切换、路由收敛等操作，全程无需人工介入。未知故障场景基于相似历史案例推荐处置方案，处置经验持续沉淀为剧本更新，扩展自动化覆盖范围。

（3）效果验证与反馈：引入自愈评分体系，从故障识别率、根因定位准确率、自动处置成功率、平均恢复时长、自愈闭环覆盖率等维度量化自愈能力。评分结果驱动"处置—评估—优化"正向迭代，低分项标记改进方向，优化后通过实战或演练验证效果，推动自愈能力从部分场景向全域覆盖演进。

上述自愈机制使网络具备从故障感知到业务恢复的全流程自主处置能力。面向未来，随着数字孪生与智能决策技术的深度融合，故障预判将从"发生后响应"转向"发生前干预"，自愈执行将从"剧本化恢复"转向"生成式处置"，最终实现网络在极限损伤场景下的自主生存与快速再生，使韧性从故障恢复能力升级为系统再生能力。

4. 持续学习与适应演进

网络智能管控策略和模型的有效性依赖于对网络环境变化的持

续适应能力。网络环境处于动态演进之中：业务流量模式随应用发展而变迁，网络拓扑随扩容和割接而调整，设备能力和软件版本随迭代而更新，攻击手段和异常模式随对抗升级而演变。离线训练、一次性部署的静态管控模型难以长期保持最优性能，构建具备持续学习与适应演进能力的智能管控体系是保障网络韧性长期有效的必要条件。核心机制包含五个维度：

（1）闭环反馈通路：智能管控系统持续接收网络遥测数据、业务质量指标、告警事件和运维操作记录等多源反馈信息，通过比对管控决策执行后的业务指标变化，自动标注决策效果形成带标签训练样本，增量式纳入数据集进行在线微调，使模型逐步适配新的运行环境特征。

（2）概念漂移应对：跟踪遥测数据的统计分布变化，检测数据层面的特征漂移信号，当漂移程度超过预设阈值时触发模型重校准或增量更新。运维人员对告警的确认与误报标记构成重要反馈信号，据此持续调整异常判定边界，在保持检出率的同时降低误报率。

（3）策略泛化优化：在新环境中执行策略并采集效果反馈，评估策略的迁移性能。对于效果退化显著的策略，启动基于反馈的强化学习微调，使用新环境下的奖励信号更新策略参数，在保障基本可用性的前提下逐步提升适应性。维护策略效果历史评估数据库，训练元模型实现策略选择的自适应优化。

（4）仿真验证与模型版本管理：数字孪生体为模型演进提供零风险的仿真验证环境。新模型在正式部署前，通过数字孪生环境进行历史数据回放和极端场景推演，评估关键性能指标是否优于当前在线版

本。验证通过后采用灰度发布策略，先在部分网络区域或业务场景下与旧模型并行运行，对比分析输出差异和业务影响，确认无退化后逐步全量替换。在线运行期间持续监控推理性能与资源消耗，指标劣化超过阈值时自动回滚至上一稳定版本。

（5）样本复用与场景复现：对历史运行数据进行分类存储和版本标记，记录采集时间、网络环境快照和管控上下文。针对网络攻击、大规模故障等稀有但高影响的极端场景样本，在数字孪生环境中进行复现验证与增强训练，避免模型在长期演进过程中遗忘对关键场景的应对能力，并持续提升对未知极端情况的泛化处置水平。

面向未来，随着边缘智能与联邦学习技术的成熟，模型更新将从集中式训练转向分布式协同进化，知识积累将从单网络经验转向跨网络共享，最终实现全行业韧性能力的协同提升与永续进化，使网络韧性从静态基线能力转化为动态生长能力。

（四）网络安全抗扰：构建网络内生防护屏障

为应对路由劫持、源地址伪造、分布式攻击、域名体系扰动等高频高发安全威胁，重点打造路由安全、源地址验证、DDoS 流量压制、DNS 韧性加固四大核心能力，形成从源头阻断、跨域联动、纵深防护的全链条安全屏障，在威胁转化为大规模损伤之前，形成有效阻断和衰减，保障网络基础设施与关键业务的持续稳定运行。

（1）路由安全体系（RPKI+BGPsec+IRR）

路由劫持和路由泄漏是网络重大安全风险，易导致流量黑洞、业务中断、数据窃听等严重后果。为此，构建以 RPKI、BGPsec、IRR

过滤为核心的可信路由安全体系，实现路由起源、路径、策略的全链路可信验证。RPKI 为 IP 地址段与 AS 号建立绑定关系，使运营商能够在接收路由通告时验证其合法性，从源头阻断非法路由注入，防范前缀劫持与虚假路由扩散。BGPsec 在 BGP 更新报文中携带 AS 路径数字签名，确保路由传递过程中路径信息不被篡改、伪造或替换，防止中间 AS 恶意篡改路由方向或制造路由环路，实现路由传递全链路可信。同时，将 IRR 互联网路由注册库校验与 RPKI 验证联动，形成双保险过滤机制，进一步拦截异常路由、冲突路由与未授权路由。构建起“源头可信、路径可信、策略可信”的路由安全闭环，从根本上提升路由层韧性。

（2）源地址验证 SAVNET

SAVNET（域内域间源地址验证架构协议）是韧性互联网核心技术体系的重要组成部分。SAVNET 聚焦 IPv6 网络中伪造源地址攻击这一核心痛点，通过生成 SAVNET 表项识别并阻断非法伪造的 IPv6 源地址报文，有效解决非对称路由场景下严格型 uRPF 的误检测问题，提升源地址验证的准确性与可靠性。源地址验证技术从源头防范网络攻击，提升互联网抗扰性与可恢复性。

（3）DDoS 流量压制

面对 DDoS 攻击向大规模、高频化发展的严峻挑战，传统基于安全系统的防御方式难以应对瞬时高强度、多 IP 扫段的 DDoS 冲击，需构建具备智能识别、秒级处置的高效防御体系。通过设备自身 AI 算力，实现短平快突发性攻击的秒级发现，通过轻量化的流量压制技

术解除攻击导致的网络拥塞，避免攻击流量在网络中长距离传输造成链路拥塞和设备性能下降，有效提升网络应对大流量冲击能力，确保核心业务在大流量攻击下仍能稳定运行。

（4）DNS 韧性加固

DNS 作为互联网基础设施的“导航系统”，其稳定性直接决定业务可达性，易受域名劫持、放大攻击、缓存污染等威胁影响。通过 DNS SEC 规模化部署、多中心 Anycast 架构、DNS 防火墙与速率限制等措施，全面强化 DNS 体系韧性。推进 DNS SEC 全链路部署，为域名解析数据添加数字签名，防止域名劫持、响应篡改与缓存污染，保障解析结果真实可信。构建多中心、多活、全球分布式 Anycast DNS 架构，实现解析服务就近接入、负载分担、故障自动切换，避免单点故障导致全域解析中断。部署 DNS 防火墙（RPZ）与响应速率限制（RRL），精准识别并阻断 DNS 放大攻击、泛洪攻击与恶意查询，限制异常请求频率，保护 DNS 服务器资源，提升整体抗攻击与抗扰动能力，确保极端场景下域名解析持续可用，为全网业务连续性提供基础支撑。

（五）网络知识图谱：构筑智能化知识底座

网络运维涉及海量异构数据，涵盖设备配置、拓扑关系、业务路径、告警事件与历史故障等多个维度，这些数据长期分散存储于各类网管系统之中，数据割裂问题直接造成故障根因定位难、跨域故障联动分析难、应急处置依赖人工经验，故障处置周期拉长、预发现能力不足，从底层制约网络事前预警、事中快速隔离、事后优化的全链路

韧性落地。知识图谱将网元实体、拓扑连接关系、业务承载链路、故障传导机理、运维处置规范、历史应急经验进行结构化关联建模，将零散异构运维数据沉淀为互联互通、可智能推理的标准化知识资产。基于图谱的关联检索与因果推理能力，可实现故障传导路径自动推演、隐性关联隐患提前挖掘、故障处置方案智能推荐，缩短故障定位与业务恢复时长，从数据治理层面支撑网络事前隐患排查、事中快速止损、事后迭代优化，全方位赋能韧性网络全生命周期保障。

围绕"看清网络、识别风险、快速处置、持续优化"的目标，构建面向网络韧性保障的网络知识体系，如下图 5 所示。基于知识来源与功能定位的差异，网络知识体系可划分为两大类：一类是网络资源与业务承载知识，主要描述网络自身的组成结构、连接关系以及业务与资源之间的映射关系；另一类是业务保障与故障处理知识，主要沉淀面向业务连续性保障和故障恢复处置的经验、规则与策略。前者提供网络运行的事实基础，后者提供面向异常场景的判断依据和处置能力。两类知识相互支撑、协同作用，共同构成 IP 网络韧性保障的知识底座。

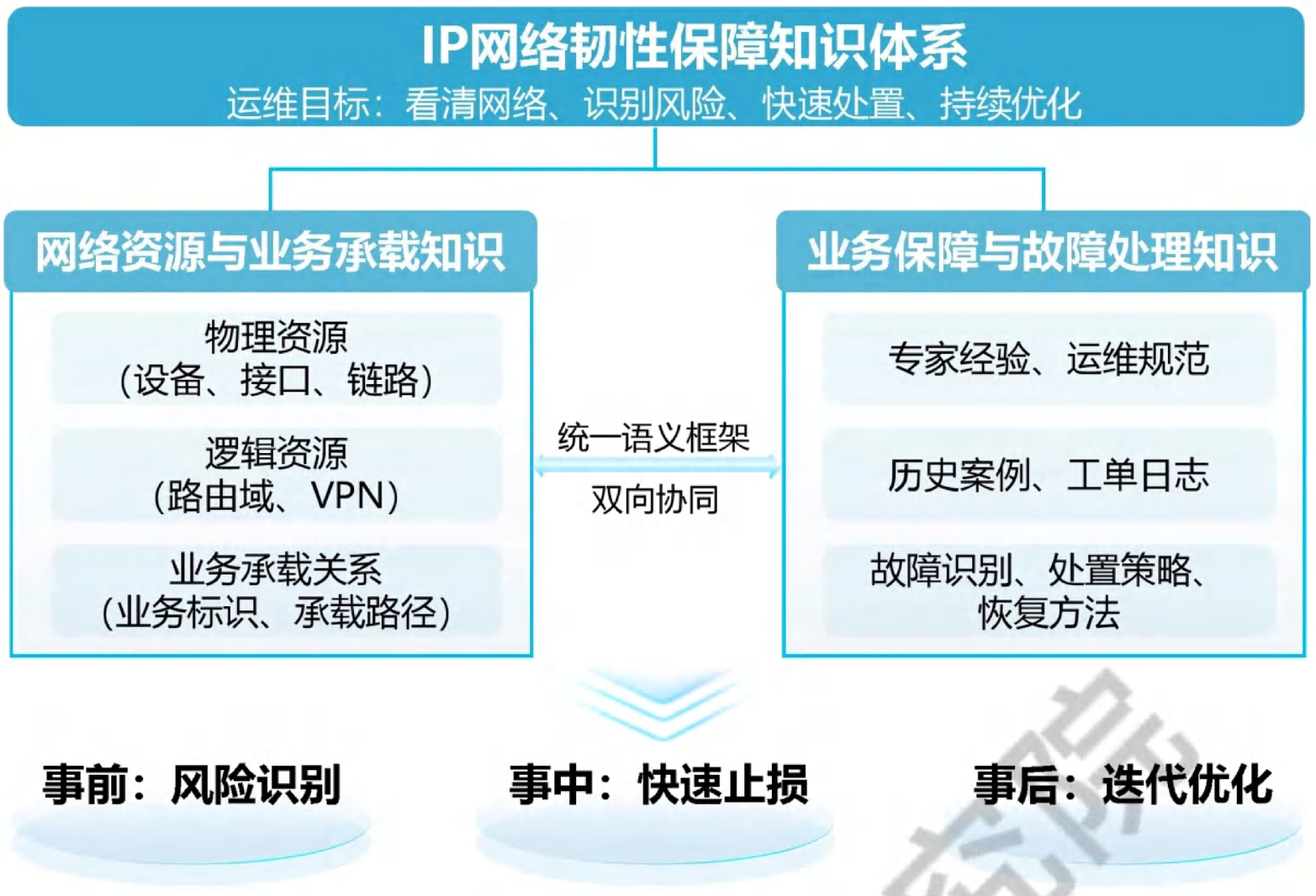

图 5　网络韧性保障知识体系

（1）网络资源与业务承载知识

网络资源与业务承载知识主要用于回答“网络由什么构成、资源如何连接、业务承载在哪里”的问题，为网络韧性保障提供准确的事实基础和分析依据。

网络资源知识用于刻画 IP 网络中的设备、接口、链路、板卡等物理资源，以及路由域、VPN 等逻辑资源。通过建立资源之间的连接和依赖关系，形成语义统一、关系可追溯的全局网络资源视图。在此基础上，业务承载知识进一步描述业务依赖的网络资源和关键路径等信息，使业务对象与网络资源之间形成清晰的承载关系，以从业务视角理解资源状态变化的影响，支撑服务连续性保障。

由此，运维分析不再局限于单条告警或单个设备，而是能够从网络拓扑结构、资源依赖关系和业务承载的整体视角出发，系统性地研判问题的根因与影响边界。网络资源与业务承载知识不仅服务于故障

发生后的应急响应，更能有效支撑故障发生前的风险识别、韧性评估与主动加固工作，从而推动运维模式从被动响应向主动预防转变。

（2）业务保障与故障处理知识

业务保障与故障处理知识旨在解决“异常如何识别、故障如何处置、业务如何恢复”的问题，是网络知识体系中支撑韧性能力的关键部分。该类知识广泛汇聚自专家经验积累、历史故障案例复盘及运维规范文档，重点刻画业务需求、网络状态、故障现象与处置策略之间的内在关联关系。

在业务保障方面，将业务等级、服务质量要求、保障时段、网络运行状态和保障策略进行多维度融合表达，构建面向业务连续性风险的识别与决策框架。当业务出现性能劣化或资源负荷异常攀升时，系统能够结合实时告警信息与当前网络状态，自动匹配并推荐路径优化、流量调度、资源适配等差异化保障动作。在故障处理方面，该类知识对典型故障的现象特征、关联告警、可能根因、传播路径及恢复方法进行结构化表达，形成可供推理引擎调用的故障知识库，辅助完成故障类型识别、根因推断与处置建议生成的全流程闭环。

业务保障与故障处理知识并非一次性构建的静态资产，而是随着保障实践的持续开展与故障复盘的不断深化而动态演进的活性知识体系。相关规则、典型案例与保障策略在运维实践中持续得到补充与迭代完善，推动网络韧性保障能力逐步实现从经验驱动向知识驱动的范式跃迁，为 IP 网络在复杂故障场景下的快速恢复与持续优化提供坚实的知识底座与能力支撑。

五、韧性互联网技术实践

（一）网络带宽池化：网络资源智能调度与高效利用

骨干网、城域网等基础网络的光纤链路易受自然灾害、工程施工、环境扰动影响，该类故障区别于链路完全中断，其网络路由协议仍可正常运行，转发逻辑无异常，但链路实际可用带宽大幅下降，造成流量拥塞。现网中出现多次链路中断引起的流量拥塞问题，因此，亟需网络节点自身进行流量动态调度，降低故障影响范围和影响时间。

为解决以上问题，韧性互联网构建了网络带宽池化技术体系，覆盖域内、域间场景，实时感知链路状态与流量负荷，通过智能算法实现流量动态分流、负载均衡，实现带宽资源池化整合与高效复用。

（1）域内带宽池化场景

骨干网或城域网一般采用 IGP 协议指导 underlay 流量转发，在 IGP 网络中，流量通常遵循最短路径原则进行转发。当最优路径因光纤故障或流量突发发生拥塞时，可能导致业务受损。域内带宽池化技术旨在打破这一限制，通过将 IGP 域内所有可用路径的带宽资源整合为一个“资源池”，实现网络级的非等值负载分担（UCMP），从而快速缓解流量拥塞。如图 6 所示，其核心工作机制如下：首先，网络实时监测所有 IGP 链路的带宽利用率，并通过 IGP 协议将该信息在全网泛洪，确保每个节点都拥有全局的链路状态视图；其次，当监测到某条链路的带宽利用率超过预设阈值时，系统自动触发流量调优流程；最后，基于域内带宽池化算法，系统计算出若干条次优路径作为备选，并根据路径的可用带宽比例，智能地将超额流量分流至这些

次优路径，实现流量的均衡分布。

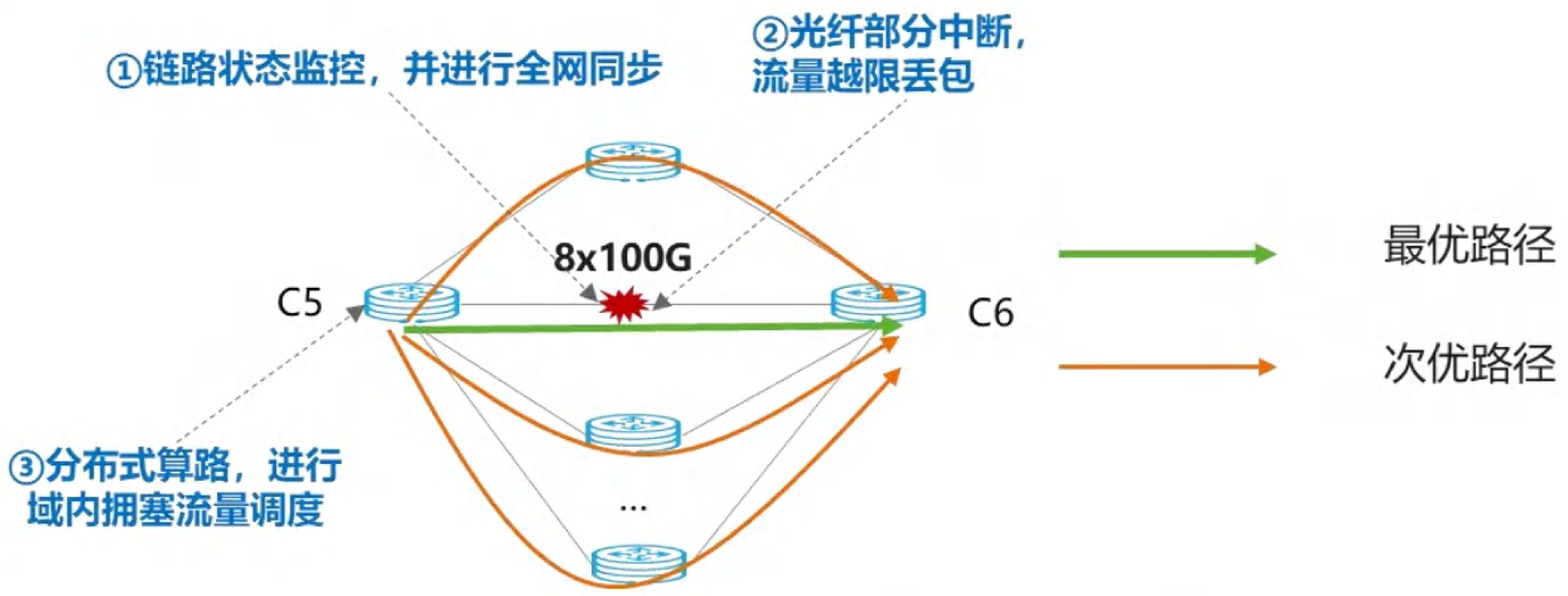

图 6 域内网络带宽池化案例

（2）域间带宽池化场景

在跨域互联场景中，域间链路流量分布不均衡可能导致单点链路拥塞，域间带宽池化技术通过精细化的流量分析与策略调控，引导流量智能选择最优链路，提升多节点间的带宽资源复用能力。

在城域网与骨干网双上联互联场景中，如图 7 所示，城域网核心路由器（CR）之间部署 BGP-LS（链路状态）协议，用于交换与骨干网相连端口的带宽及利用率信息，形成域间资源的全局视图。同时，CR 设备开启智能流量分析功能，识别出入方向的 Top-N 流量，为精准调度提供依据，基于流量分析结果，识别出待调整的 Top-N 路由前缀。通过 BGP RPD（路由策略分发）协议下发临时策略，例如，通过调整 AS 路径属性（AS-Path Prepending）降低特定路由的优先级，从而将部分流量从拥塞的入口节点疏导至其他有冗余带宽的节点，调优结束后，策略自动撤销，确保网络配置的简洁性。城域网出口核心路由器节点应用带宽池化技术，可引导回城域方向流量调度，当单个节点链路带宽不足时，复用跨节点的可用带宽，充分利用网络

资源。

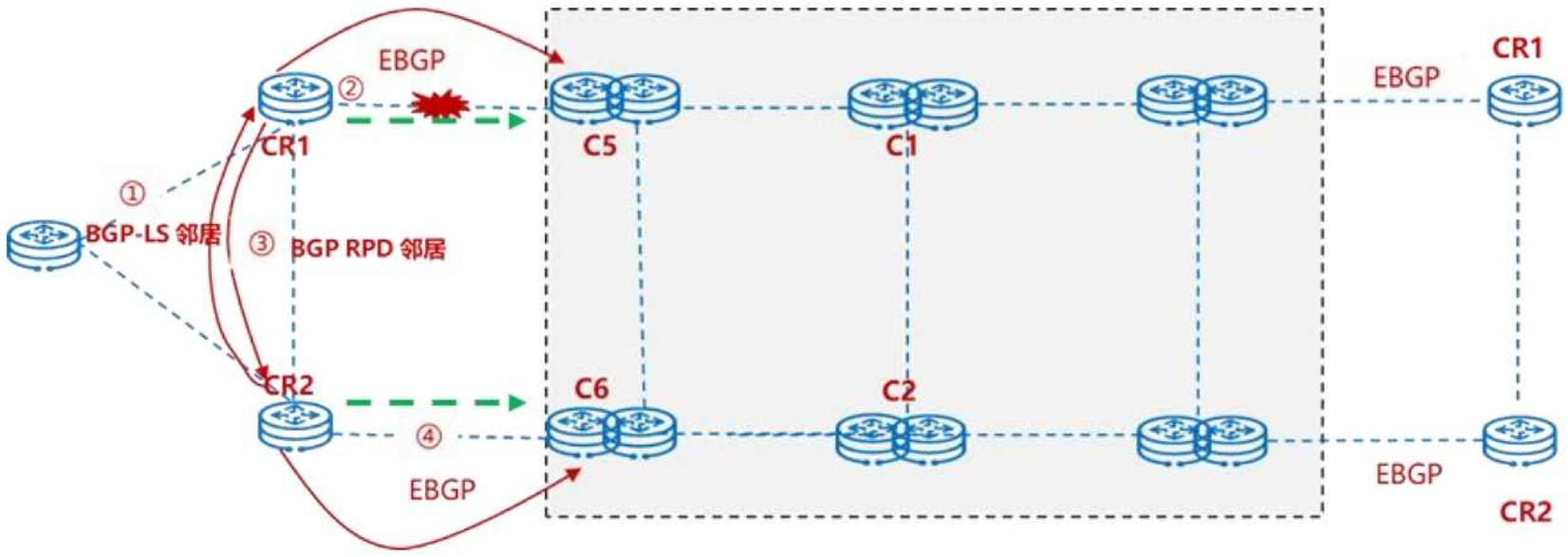

图 7 域间网络带宽池化（入方向）案例

针对城域网至骨干网的出方向流量，基于域间带宽池化技术以及 SRv6 TE（段路由流量工程）的可编程能力，构建灵活的流量调度通道，实现故障场景下的快速、无损流量切换，如图 8 所示。核心工作机制如下：城域网 CR 之间通过 BGP-LS 实时同步域间出链路负载状态，并基于带宽池化算法，预先计算并规划好 SRv6 TE 隧道作为备用路径，当 CR 设备监测到某条出方向链路拥塞时，系统自动触发调优，将超额流量通过预先建立的 SRv6 TE 隧道进行疏导。例如，当 CR1 至骨干网的直连链路拥塞时，流量可自动切换至 CR1->CR2->骨干网的 SRv6 隧道路径。在隧道终结点 CR2，确保流量能够正确地继续传输至最终目的地。

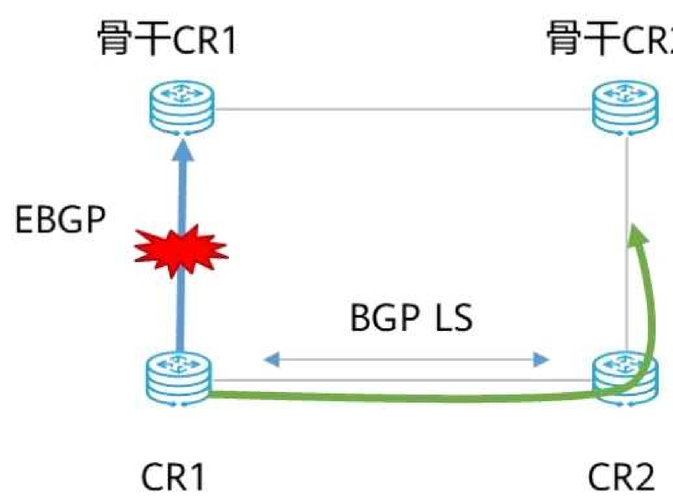

图 8 域间网络带宽池化（出方向）案例

（二）BGP 优雅降级：控制平面过载管控与平滑自愈

现网运维过程中，受突发业务流量暴涨、异常配置、恶意路由前缀注入、大范围路由震荡等因素影响，路由器控制平面极易出现内存资源骤增、资源超限等问题。若内存资源被耗尽，将直接造成设备进程异常、整机重启，诱发大面积业务断网，严重破坏整网运行稳定性。

针对上述挑战，BGP 优雅降级技术通过实时监控内存水位，构建了一套“监测-决策-执行-恢复”的闭环韧性体系，将设备内存占用控制在安全阈值内，防止系统因资源耗尽而崩溃，从而保障核心业务的连续性与网络整体的稳定性。

面对大规模路由振荡、突发前缀注入等极端场景，BGP 优雅降级技术能够实现故障有效处置，核心工作机制如下：系统持续、实时地监控控制平面的内存水位，为后续决策提供精准的数据依据，当监测到内存资源快速消耗并触及预设的阈值时，系统自动触发相应的分级保护策略，根据内存紧张程度，系统执行一系列主动防御措施，例如，通过智能调整 BGP 路由的学习速度，减缓路由信息的接收速率，或缩减次要路由的处理优先级，释放其所占资源。这些措施旨在将内存占用强制控制在安全阈值内，确保核心控制功能的稳定运行，当内存占用率回落至安全水位后，系统并不会立即恢复所有业务，而是启动一个分级恢复流程，它会逐步、平滑地恢复路由学习速度和分批放开受限路由，确保整个过程平稳过渡，避免因业务瞬间恢复引发的二次冲击。

针对持续的路由攻击注入，传统的解决方案通常会触发 BGP 邻居

复位、BGP 进程重启，甚至导致整机重启，造成业务完全中断，更严重的是，设备重启后可能因路由量巨大而无法快速收敛，再次陷入高负载状态，形成“故障-重启”的恶性循环。而 BGP 优雅降级方案则通过策略控制，使得设备的控制平面得以保持存活状态，核心的数据平面转发业务完全不受影响，一旦攻击停止，系统便自动执行恢复策略，业务在短时间内即可平滑恢复至正常状态，两种方案的表现具体如下图 9 所示。

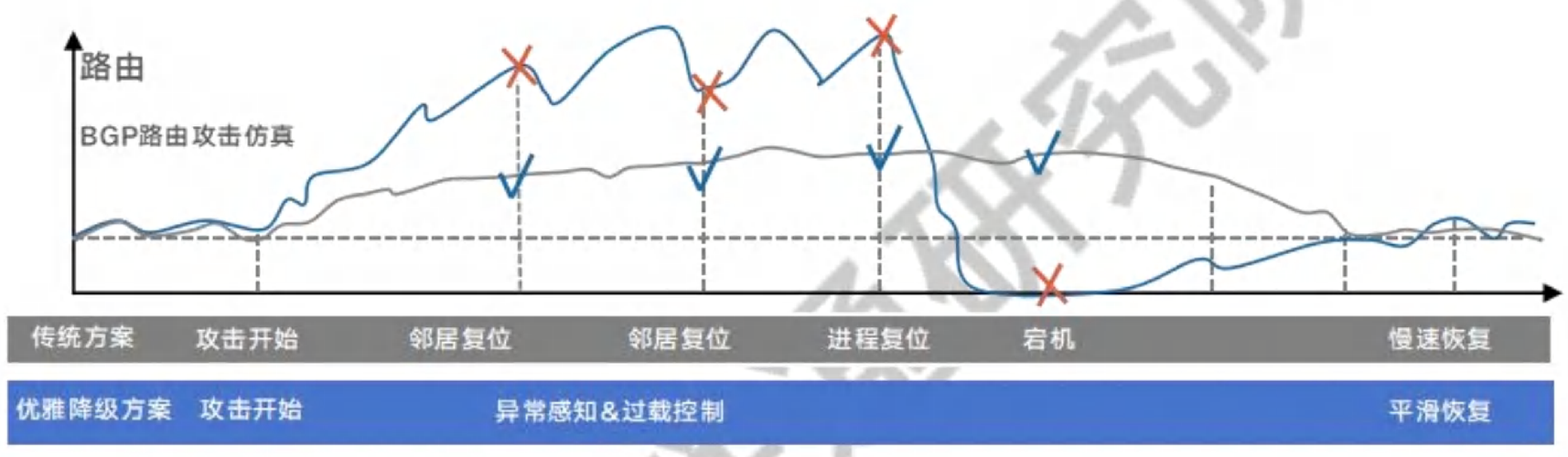

图 9 BGP 优雅降级和传统方案的效果对比

BGP 优雅降级技术显著提升了网络设备在极端资源压力下的生存能力，它成功地将可能导致全网瘫痪的“系统性崩溃”转化为对业务影响极小的“可管可控的平稳降级”，有效避免了因单点设备资源耗尽而引发的全网性连锁风险，是构建高韧性网络的关键技术之一。

（三）数字孪生仿真预演：网络变更风险前置治理

网络设备迭代升级、链路割接、新业务上线是网络运维体系中的常态化工作，传统运维模式高度依赖人工经验进行方案落地与变更实施，无法提前排查配置适配风险、流量转发异常及业务兼容冲突等隐性隐患，极易诱发路由震荡、链路波动乃至核心业务中断，对网络基础设施的稳定运行造成严重影响。

针对传统运维模式的短板与痛点，构建网络智能仿真分析平台，如下图 10 所示，基于此平台，可在设备更替、网络割接等高危变更作业实施前，通过智能推演模拟完整操作流程，提前校验配置匹配度，预判流量分布走势与业务连通状态，精准排查各类潜在运行异常。基于本平台构建与物理网络高度契合的仿真镜像，完整还原全网拓扑架构、设备转发逻辑、链路负载特征与业务承载关系。同时，建立仿真前置校验的刚性闭环机制，将虚拟预演、风险评估、方案优化作为所有重大网络变更的前置必经环节，未通过仿真验证的配置方案与割接操作禁止上线落地，从源头杜绝人工变更失误与架构适配问题引发的网络扰动，构建“事前预演、事中可控、无错入网”的韧性运维体系。

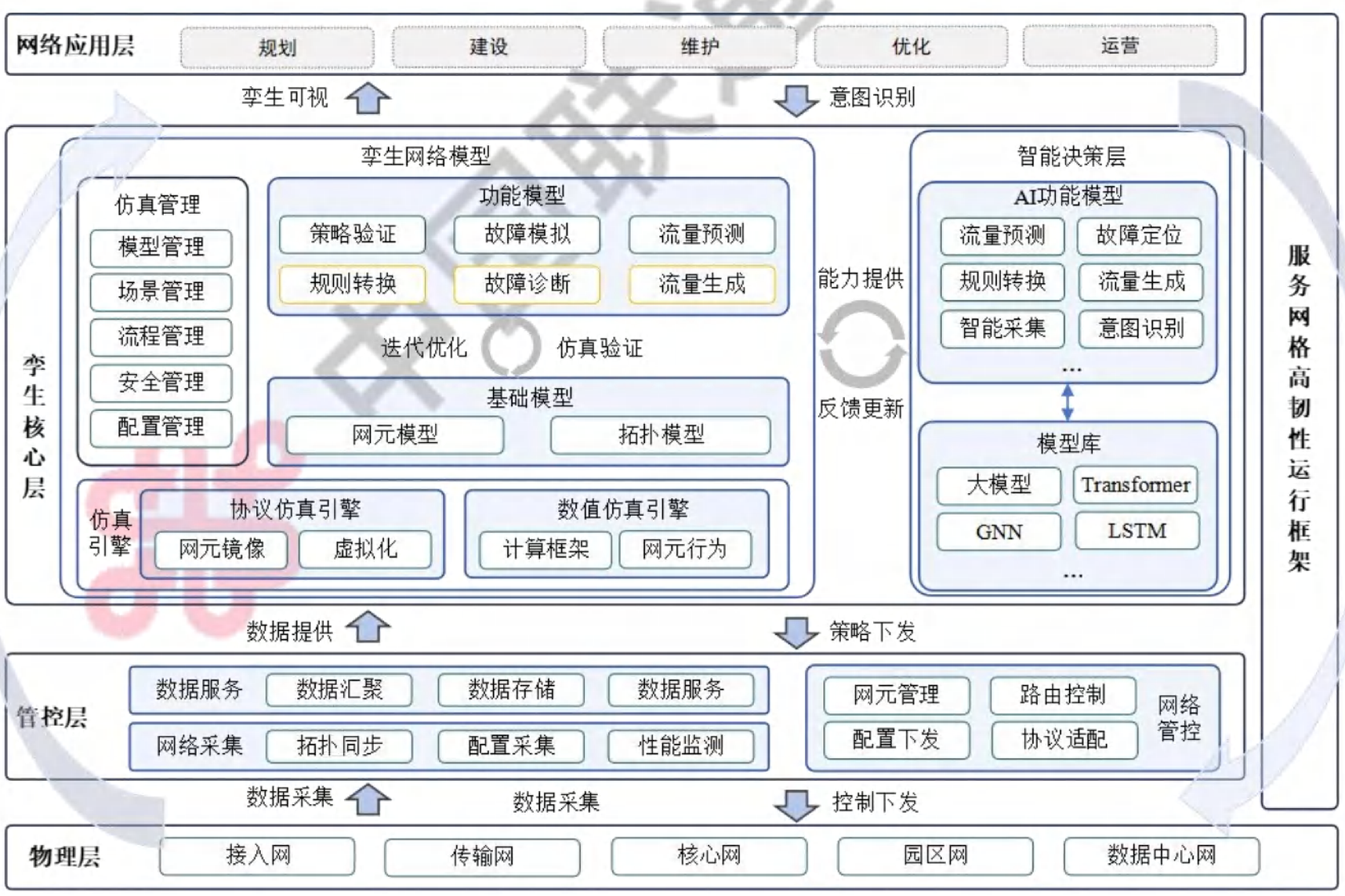

图 10 网络智能仿真分析平台功能架构

在设备迭代换新场景中，依托网络智能仿真分析平台，在设备替换前完成全网配置预校验与替换模拟，提前规避设备兼容风险与业务

适配问题，通过智能化预演替代传统专家人工兜底模式，大幅降低设备迭代的运维成本与变更风险，实现设备平滑焕新、业务零中断，有效提升骨干网络基础设施的迭代稳定性与自主可控能力。在新方案入网部署场景中，例如，新路由策略、流量调度新算法等新技术批量上线前，在仿真环境灌入现网真实流量与路由表，测算资源开销、收敛性能、异常边界，完成方案可行性论证。

（四）DDoS 冲击防御：异常流量识别溯源与拥塞解除

当前网络空间 DDoS 攻击威胁持续升级，攻击模式不断迭代演化，呈现出大流量突发、短时高强度、扫段攻击低速隐蔽化的全新特征，具体表现如下：

（1）现阶段主流 DDoS 攻击呈现极强的突发性与短时破坏性，T 比特级超大流量攻击成为常态化威胁，攻击流量爬升速度极快，可在 10 秒内将攻击速率攀升至 500Gbps-1Tbps，高强度攻击状态可持续 30 秒，随后 10 秒内快速回落，完成一次短时高强度攻击闭环，具体如下图 11 所示，传统 DDoS 防御体系依赖分钟级抽样检测机制，检测响应周期长、流量捕捉滞后，无法精准识别、快速处置此类短时突发攻击，对“短平快”的新型 DDoS 攻击抵御能力严重不足。

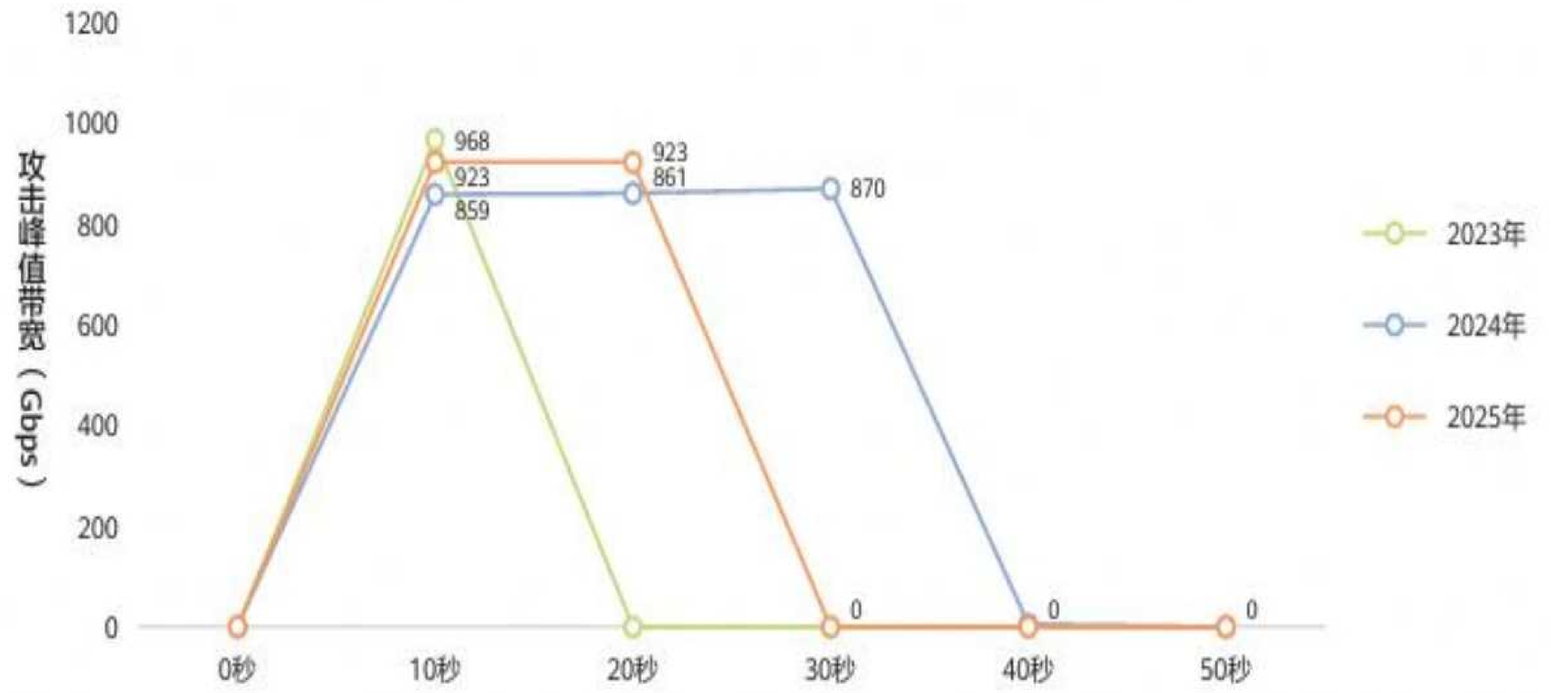

图 11 DDoS 攻击爬坡速率

（2）扫段攻击的隐蔽性特征愈发突出，从 2025 年 DDoS 攻击态势监测数据来看，62.89%的扫段攻击单 IP 流量低于 500Mbps，具体如下图 12 所示，低速低流量的攻击特征能够有效规避传统单 IP 攻击检测算法的识别规则，导致传统检测机制准确率大幅下降，隐蔽式攻击威胁持续加剧。

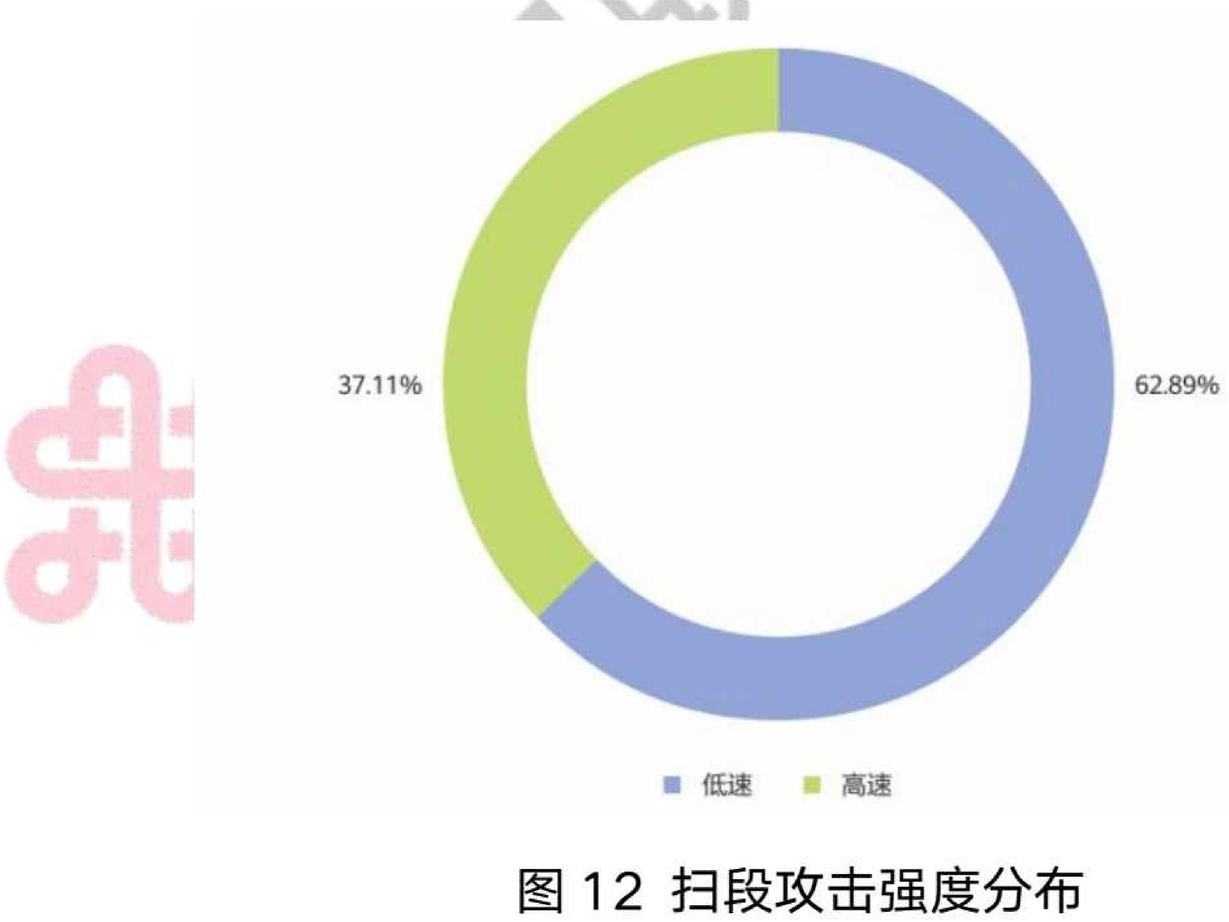

图 12 扫段攻击强度分布

当前 DDoS 攻击的危害场景主要分为两类，具体如下图 13 所示，第一类为节点防护能力不足场景：攻击目标节点虽部署基础防护策略，但防护带宽、检测能力、处置能力无法匹配攻击强度，导致目标业务

直接受损，出现服务卡顿、中断、丢包等问题。第二类为路由节点拥塞连锁影响场景：攻击流量聚焦父节点路由设备，造成设备带宽资源耗尽、网络拥塞，虽非直接攻击同节点终端用户，但会引发同节点全域用户上网卡顿、时延升高、业务掉线等次生故障，影响范围更广、受众更多。

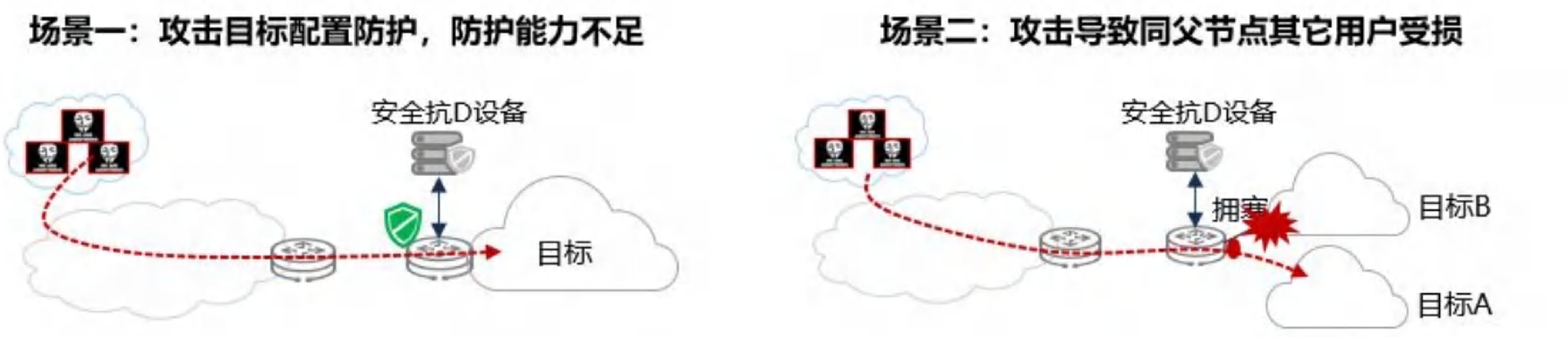

图 13 DDoS 攻击场景

针对上述挑战，通过 AI-DDoS 秒级“闪防”技术，构建高精度、高时效、全自动的新一代 DDoS 防御体系，该技术彻底摒弃传统抽样检测模式，在路由器设备中嵌入 AI 技术和可编程 NP 芯片，实现全网 1:1 全量流量采样，无遗漏捕捉全网流量数据，在此基础上，对流量微突发特性、SYN 报文占比、碎片报文占比、数据包长度、包流速、流量波动规律等多维核心特征进行精细化、智能化深度分析，实现秒级攻击流量精准诊断与攻击类型判定，在防御处置层面，技术具备双重应急防护能力，可实现分层、快速攻防响应。一方面，设备端依托本地流表，实时识别 TOP-N 高危攻击流并进行压制，缓解网络拥塞状态，遏制攻击扩散；另一方面，系统可同步生成标准化安全告警，实时上传至上层检测系统，该系统随即解析上报的攻击时间，并迅速触发与清洗中心的协同机制，依据预设策略执行精确的流量牵

引操作，将受攻击流量引流至专门的 DDoS 清洗设备进行清洗动作，以此高效应对网络攻击威胁，具体如下图 14 所示，其中 Flow 采集设备的主要功能为 Netstream 日志采集和 DDoS 攻击流分析，DDoS 清洗设备的主要功能为过滤攻击流量和回注业务流量。

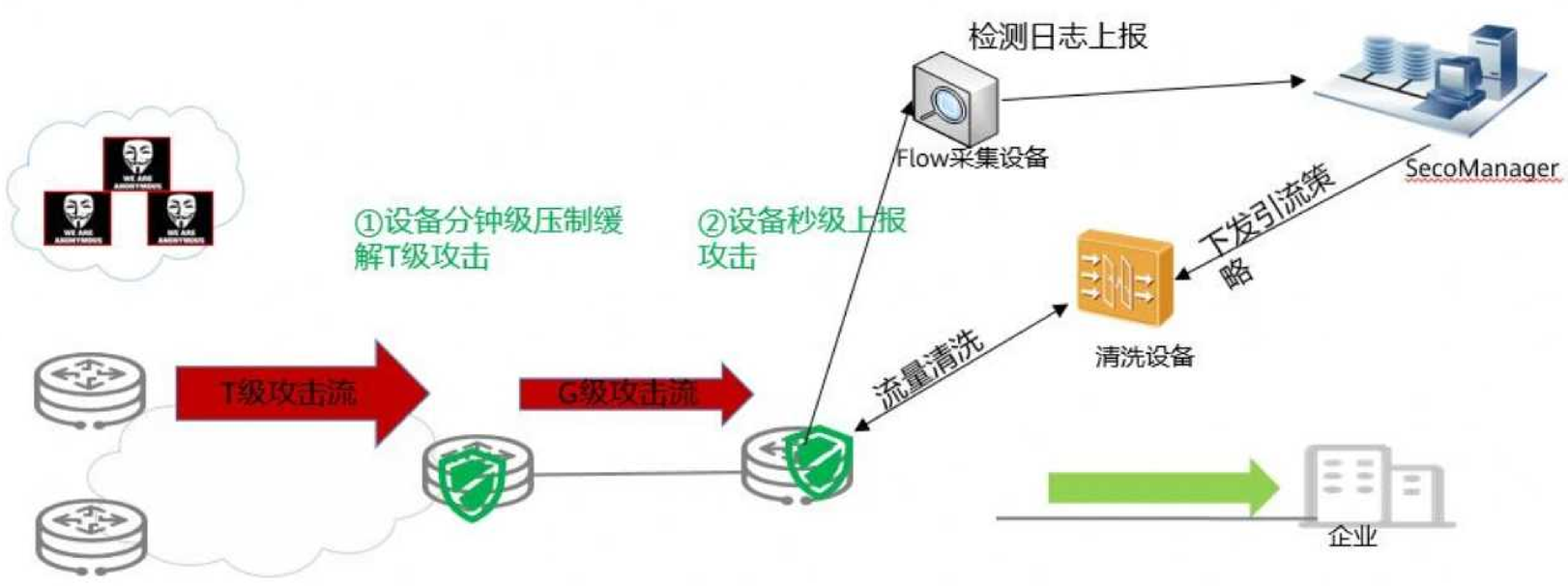

图 14 AI-DDoS 秒级闪防机制

目前，AI-DDoS 秒级闪防技术已在运营商现网完成部署与实战验证，彻底解决了传统防御响应滞后、漏检率高、防护低效等痛点。该闪防技术现网试运行一个月期间，4 块业务单板累计上报安全攻击告警 2.5 万次，覆盖被攻击 IP 共计 70 个，经 IP 地址聚合统计后，累计识别有效攻击超 2000 次。其中，1900 余次短时突发攻击无法被传统检测机制识别，实战数据证明，AI-DDoS 秒级闪防技术大幅提升了网络攻防对抗能力，实现了 DDoS 攻击“早发现、快处置、零漏检、低影响”的防护目标。

六、总结与展望

本白皮书系统阐释了韧性互联网的核心目标与技术体系，围绕常态化运营痛点、新兴业务需求、极限场景挑战，明确了网络韧性建设的必要性与核心价值。面向全生命周期风险治理，构建“固本御危、承压稳运、应急存续、迭代优化”四维核心目标，搭建三阶段闭环韧性能力架构，依托五大技术底座协同赋能，形成拓扑硬防护、协议快自愈、管控智自治、安全内生、知识迭代的全方位韧性保障格局，有效补齐传统网络故障易扩散、故障恢复慢、极限场景存续弱、能力难以迭代等短板，形成可落地、可演进的韧性网络技术体系与实践范式。

面向未来，随着算网融合、AI 大模型、天地一体化网络深度发展，网络运行场景与攻防环境将更趋复杂。后续韧性互联网将持续深化技术迭代，推动网络感知、自愈、调度能力向全域自主、智能自适应升级；持续完善分层分级的韧性标准体系与量化评估机制，夯实行业落地规范；深化产学研用协同创新，加速韧性技术在政务、金融、算力网络等关键行业规模化落地。通过技术、标准、产业多维协同，持续提升网络复杂扰动适配能力与极限场景生存能力，持续夯实关键信息基础设施韧性底座，助力数字经济安全、稳定、高质量发展。

中国联通研究院根植于联通集团（中国联通直属二级机构）作为中国联通科技创新专业子公司，自 2022 年起，挂牌成立中国网络安全研究院、下一代互联网宽带业务应用国家工程研究中心及首个国家级网络安全产业知识产权运营中心，形成“两院两中心”发展格局，开创了研究院高质量发展的新局面。中国联通研究院作为服务于国家战略、行业发展、企业生产的战略决策参谋者、技术发展的引领者、产业发展的助推者，坚持以高水平科技自立自强为使命担当，聚焦网络强国、数字中国主责，拓展联网通信、算网数智业务，形成“态度、速度、气度、有情怀、有格局、有担当”的企业文化，以下一代互联网、光网络、5G-A/6G、网络安全、数智网优、低空智能网联和新型智库研究七个领域为主攻方向，坚持“四个聚焦”，开展关键核心技术攻关、科创力量建设、专业技术人才队伍建设、创新成果转化等工作，着力实现价值创造提升、战略科技力量提升、专精特新能力成色提升，争做通信行业科技创新主力军，努力建设成为“国家信赖、行业领先、集团倚重、员工自豪”现代化一流研究院。

战略决策的参谋者
技术发展的引领者
产业发展的助推者

态度、速度、气度

有情怀、有格局、有担当

中国联合网络通信有限公司研究院
地址：北京市亦庄经济技术开发区北环东路 1 号
电话：010-87926100
邮编：100176

中国联通研究院

中国联通泛终端技术