

通信世界

COMMUNICATIONS WORLD

总第917期 2023年4月10日 第7期

中国标准连续出版物号: ISSN 1009-1564
CN 11-4405/TP



工业和信息化部主管
人民邮电出版社有限公司主办



中国通信企业协会会刊

问“网”哪得清如许

打造网络安全新活力

IPv6流量首超IPv4

万物互联时代迎来拐点/P4

中国信通院副院长魏亮

以技管网，开创行业反诈新格局/P9

中国移动李男：5G小基站规模化发展

夯实新一代边缘算力底座/P33

ISSN 1009-1564



9 771009 156234

“深”

见未来

新时代·新通信·新世界



通 信 世 界 全 媒 体

运营商转型科技创新公司是时代的选择

半月谈

刘启诚

有媒体报道称，国资委科技创新局负责人日前表示，中央企业已成立数字科技类公司近500家，主要集中于新一代信息技术、人工智能等战略性新兴产业。此前，笔者在参加某一行交流时，与会的电信运营商高层也表示，国内电信运营商都在向科技公司转型，转型的标志之一是设立数字科技类子公司。近两年，三大基础电信运营商成立了众多专业科技子公司，重点布局“云大物智安”，紧盯行业领域开展创新业务。看来在这500家数字科技类公司中，电信运营商应该贡献了不少。

当下，为何中央企业如此密集地成立数字科技类公司？业界普遍观点认为，作为数字化转型的主力军，中央企业竞相成立数字科技公司的目的在于数字化转型。

全力发展数字经济，已成为国家重要战略部署。近两年，国家出台了多项数字经济建设政策，从国务院印发《“十四五”数字经济发展规划》，到中共中央、国务院出台《数字中国建设整体布局规划》，都预示着我国数字经济建设已到新阶段。作为数字化建设的主力军，中央企业定要担纲。如何实现数字化？成立数字科技公司无疑是最直接、有效的解决办法。

中央企业数字化发展研究院院长、华润数科控股总经理董坤磊认为，中央企业成立数字科技公司带来4个方面的收获。一是引领及带动更多国有企业加快数字化转型发展，服务数字中国战略；二是充分参与市场竞争，形成更具市场竞争力的业务能力；三是以外促内，更好地服务集团产业智能化发展和数字化转型；四是以内促外，带动上下游产业链、供应链，助推数字经济高质量发展。

但对于运营商来讲，要转型成为科技公司，成立专业科技子公司只不过是“万里长征的第一步”。要成为真正的科技创新公司，运营商还需要走很长的路。

首先，在思维上彻底改变。通信是一个高科技领域，通信技术发明百余年来，一直处于科技前沿。因此，在许多眼中，电信运营商应该是高科技公司。但实际上，电信运营商的科技创新能力一般。电信运营商的本质是服务公司，通过提供电信接

入服务来获取用户和市场。多年以来，大概也就是当年没有拆分的美国AT&T还算得上一家科技创新公司，其旗下的贝尔实验室研发了许多对后世影响很大的通信技术。如今全球有影响力的运营商多数为营销服务公司，国内三大运营商也是如此。如今提出要转型为科技公司，更多出于响应国家数字经济发展战略的需要。

当然，运营商喊出转型科技创新公司的口号，另一个主要原因是行业数字化转型的市场要求。5G时代，从面向to C市场转向to B市场，对运营商的技术能力提出了新要求。三大运营商纷纷加码数字科技领域的投入，显然也是看中了这一领域的重要战略价值。

所以说，运营商或者中央企业向科技型企业转型，是政策和市场的双重推动，是一种“箭在弦上不得不发”的结果。在这种情况下，要实现向科技型企业转型，就要在思维上彻底地转变。

其次，体制机制的转变。运营商要成为科技创新型公司，不是成立几家数字科技公司就万事大吉，挑战还在后头呢。作为科技创新公司，就要承担失败的风险。现有的体制机制是否适应这一要求？此外，管理数字科技子公司也需要灵活的机制。

最后，研发投入的问题。科技创新需要资金的支持。从研发投入来看，尽管这两年三大运营商逐步加大了研发投入，但与互联网企业和通信设备厂商相比，还有很大的差距。从2022年年报数据看，阿里巴巴的研发支出为443亿元，腾讯的研发支出为614亿元，百度的研发支出为233亿元，华为的研发投入达到1615亿元。而中国电信的研发投入为134亿元，中国联通的研发投入为109亿元，中国移动的研发投入为217亿元。从研发投入占营收比数据看，华为达到了25.1%，而运营商几乎是最低的。没有投入的创新是产不出成果的。

对于运营商来讲，从定位于“创新型科技公司”，到成为“创新型科技公司”，还需要更多的努力。当然，在数字经济成为产业主旋律的背景下，运营商转型成为科技公司，是必须也是必然的结果，这是时代的选择，也是唯一的出路。

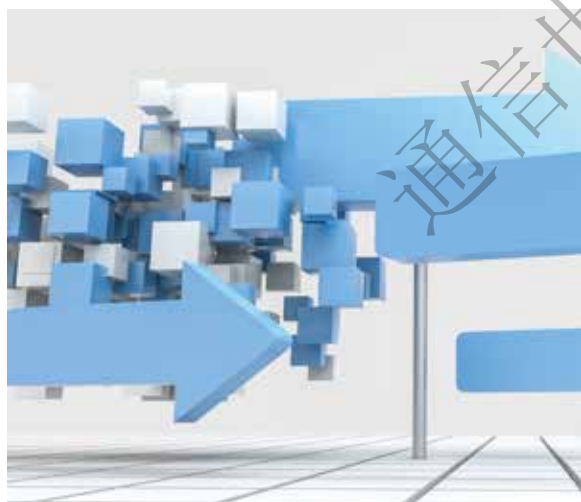
CONTENTS 目录

述评 Review

- 4 IPv6流量首超IPv4, 万物互联时代迎来拐点
- 5 鸿蒙从0到8%: 着眼泛化终端, 实现长远发展

专题 Topic 网络安全

- 6 活力彰显, 我国网络安全产业驶入“快车道”
- 9 中国信通院副院长魏亮
以技管网, 开创行业反诈新格局
- 11 新形势下的车联网安全风险及应对
- 14 跨境电信网络诈骗形势特点分析与治理路径研究
- 16 电信和互联网行业数据安全人才发展洞察与思考



P18 2022年运营商业绩亮点及趋势展望

广告目录

- 封二 通信世界形象广告
- 封底 科技创新为节能减碳助力公益广告



P27 全球2G/3G网络关闭潮加速到来

产业 Industry

- 18 2022年运营商业绩亮点及趋势展望
- 21 财报解读: 穿越周期 运营商绘就“第二曲线”
- 23 根深叶茂 广州“AI+算力”深度赋能幸福民生
- 24 探寻智慧城市发展新路径 智慧“龙江”三步走
- 27 全球2G/3G网络关闭潮加速到来
- 29 城市管网基础设施智能化问题研究
- 31 小基站能否登上大舞台?
- 33 中国移动李男: 5G小基站规模化发展
夯实新一代边缘算力底座
- 35 中国联通李福昌: 不仅拓展覆盖
5G小基站将创造更多价值
- 36 精耕细作, VIAVI测试方案助推5G小基站产业腾飞
- 37 恩智浦O-RAN 5G小基站为垂直行业“量体裁衣”

技术 Technology

- 38 针对5G车载通信模组的模拟网测试方案研究
- 42 事理认知图谱在电信运营商
潜在不满预测分析中的应用研究
- 46 工业互联网领域商用密码应用安全性评估研究



主管：工业和信息化部

主办：人民邮电出版社有限公司

出版：北京信通传媒有限责任公司

编辑：《通信世界》编辑部

总 编 辑：刘启诚

副 总 经 理：张 鹏

执行主编：舒文琼

执行副主编：程琳琳

采 编 部：王 涛 甄清岚 梅雅鑫 王禹蓉 孙 天

朱文凤 王鹤迦 包建羽 盖贝贝

美 术 编 辑：杨斯涵 李 曼 张 航

持 证 记 者：刁兴玲 程琳琳 甄清岚

刘华鲁 梁海滨 牛晓敏

（国家新闻出版署 举报电话：010-83138953）

市 场 部：申 晴 孟 月 姜蓓蓓 沈新竹 刘适之

工 联 网：郑勇志 刘艳玲 胡锦明

视 频 编 辑：林 嵩 刘 江 黄杨洋

技 术 支 持：伍朝晖

通信地址：北京市丰台区顺八条1号院2号楼北阳晨光大厦3层

邮 编：100079

编辑部：+86-10-52266521

营销部：+86-10-52266541

+86-10-52265997

发行部：+86-10-52265707

通信世界网网址

Website：www.cww.net.cn

投 稿 邮 箱：cww@bjxintong.com.cn

中国标准连续出版物号：ISSN 1009-1564
CN 11-4405/TP

出版日期：2023年4月10日

承印单位：涿州市荣升新创印刷有限公司

定 价：20.00元

编委会

编委会名誉主任

郭 浩 中国通信企业协会会长

编委会主任

顾 翀 中国工信出版传媒集团总经理、总编辑

编委会副主任

赵中新 中国通信企业协会副会长兼秘书长

刘华鲁 中国工信出版传媒集团副总经理

编委会委员

蒋林涛 中国信息通信研究院科技委主任

余晓晖 中国信息通信研究院院长

鲁春丛 中国工业互联网研究院院长

胡坚波 中国信息通信研究院副院长

李长海 中国工信出版传媒集团原总经理助理

沈少艾 中国电信科技创新部顾问

张成良 中国电信研究院院长

张同须 中国移动研究院党委书记

马红兵 中国联通科技创新部总经理

黄宇红 中国移动研究院院长

唐雄燕 中国联通研究院副院长

高 鹏 中国移动设计院副院长兼总工

窦 笠 中国铁塔股份有限公司技术部总经理

杨 骅 TD产业联盟秘书长

吕廷杰 北京邮电大学教授

梁海滨 北京信通传媒有限责任公司副总经理

刘启诚 通信世界全媒体总编辑

陈山枝 中国信科集团副总经理

彭俊江 爱立信东北亚区研发中心总经理

发行范围：公开发行

国内发行：中国邮政集团公司北京市报刊发行局

订购处：全国各地邮局 **邮发代号：**82-659

国外发行：中国国际图书贸易集团有限公司（北京399信箱）

国外发行代号：T1663

广告发布登记：京东市监广登字20170149号

本刊声明

- 《通信世界》授权信通传媒旗下通信世界网为本刊唯一网络发布平台，本刊所有内容将在通信世界网上同时刊登，本刊文章可能由通信世界网向其他合作网站免费提供。向本刊投稿的作者，均应同意上述条件，如不同意请在来稿中特别注明。
- 本刊寄发给作者的稿酬，已含其作品发表在本刊网站及电子版上的稿酬。
- 向本刊投稿的作者应同意授权本刊可以依法维护其著作权等权利。
- 未经本刊书面同意，不得以任何形式转载、使用本刊所刊登的文章及图片。

IPv6流量首超IPv4 “万物互联”时代迎来拐点

马继华

相关统计数据显示,2023年2月我国移动网IPv6流量占比达到50.08%,实现移动网络IPv6流量超过IPv4的历史性突破,标志着我国推进IPv6规模部署及应用工作迎来了新的里程碑。

不仅如此,据中国信息通信研究院监测,全国已有超过95%的CDN节点支持IPv6;国内主要13家云服务企业54个可用域的云主机中,IPv6访问质量优于IPv4的有40个,占比为74.07%。我国IPv6互联网活跃用户数达7.424亿,占比70.64%。

根据《关于加快推进互联网协议第六版(IPv6)规模部署和应用工作的通知》,到2025年全面建成领先的IPv6技术、产业、设施、应用和安全体系,中国IPv6网络规模、用户规模、流量规模位居世界第一。从目前的进展来看,这一目标的实现将水到渠成。

在世界互联网发展史上,中国曾经是一个跟随者,各种原因导致IPv4互联网协议时代IP地址资源稀少,且缺乏根服务器,对整个互联网的业务发展和网络安全形成了很大压力。而IPv6协议的加快落地并形成规模优势,对于数字中国建设将起到关键性的支撑作用。

IPv4构成现今互联网技术的“基石”协议,但资源有限,从理论上讲,可用的网络地址和主机地址的数目总量只有43亿个,根本无法满足万物互联时代终端和机器接入网络的巨大需求。

此前,在互联网时代,还可以通过局域网等技术进行适应性“变通”以化解难题。而目前的智慧城市、智慧园区建设涉及各种传感器,必须依靠可公开路由的IP地址进行监视和数据收集。在制造领域,工业互联网需要大量工业传感器,需要对每个生产设备上的装置甚至是生产线上的每个零件进行生产自动化监控,需要大量的IP地址。

IPv6地址由128位二进制数组成,地址空间中大约有 2^{128} 个地址,被形象地比喻为“地球上的每一粒沙子都能分配一

个IP地址”,可以认为是取之不尽、用之不竭的。

我国移动物联网用户规模快速增长,截至2022年底,连接数达18.45亿,比2021年底净增4.47亿,占全球总数的70%。如此庞大的网络用户规模和快速增长的设备接入数量,只有IPv6才能够满足。

相比IPv4,IPv6的数据转发路径更短,极大地提高了转发效率,也消除了IPv4中常见的地址冲突问题,为设备提供了更多简化的连接。这些特点让IPv6成为了“万物互联”时代低时延应用的基础设施。

IPv6不仅IP地址数量多,而且安全性也很高,其采用的IPSec安全体系架构可以“无缝”地为网络层数据传输提供各种安全服务,解决了网络层端到端数据传输的安全问题。

目前,由下一代互联网国家工程中心牵头发起的“雪人计划”,已在全球完成25台IPv6 DNS根服务器架设,中国部署了其中的4台,由1台主根服务器和3台辅根服务器组成,我国的网络安全有了更坚实的保障。

IPv6规模部署的不断深化,推动IPv6网络实现从“能用”走向“好用”,而向“爱用”的跨越将成为下一阶段我国IPv6发展的重要目标。

从现实来看,虽然IPv6优势明显,但由于网络建设的惯性、新老设备的兼容性以及迁移成本等限制,IPv6的下一步推进还存在很大压力,需要各方采取有力措施加以推动。当然,IPv6也要继续强化健壮性、可靠性、安全性,让用户安心实现平滑过渡。

总之,IPv6是互联网演进升级的大势所趋,是数字中国、网络强国建设的关键支撑,也能给用户带来更快的网络速率、更安全的数据传输和更好的隐私保护。IPv6流量已经超过IPv4,而“万物互联”的美好才刚刚开始。(作者为通信行业资深分析师)

鸿蒙从0到8% 着眼泛化终端,实现长远发展

金峰

2012年,鸿蒙系统启动开发;2019年,鸿蒙系统商用,并搭载于智慧屏上;2021年,搭载鸿蒙系统的手机推出;2022年底,Counterpoint数据显示,在智能手机市场中,鸿蒙系统全球份额占比为2%,国内份额占比为8%,稳坐“第三大操作系统”交椅。

笔者认为,鸿蒙系统的发展具有5个方面的启示。

一是知识产权“避雷”:解决可持续发展的问题。

近年来,一些自主终端操作系统或多或少以Android作为基础,以期实现快速生成。由于Android系统在组成上包括开源部分(如AOSP)和知识产权部分(如谷歌的GMS),且二者边界模糊,这就导致一些国产系统,陷入了“Android换皮”的“口水战”中,或被谷歌告上法庭。

于2012年启动开发的鸿蒙系统,虽然也站在Android的肩膀上,但仅使用了完全开源的AOSP部分,并且时刻具有危机意识,防范来自法律诉讼、行政制裁等方面的威胁,确保知识产权合规,构筑发展基石。

二是自有终端规模:促进系统规模发展。

一款全新操作系统能否被广泛应用,取决于终端厂商的接受程度。将系统安装在自有终端中,不仅能够促进系统快速规模发展,同时也能为其他终端厂商提供示范样板。参考国际案例,苹果采用终端与系统一体化发展方式;谷歌在Android系统推出的早期,也定制手机,为行业提供范例。

现阶段,华为的鸿蒙系统参考了苹果的模式。虽然受到制裁导致5G手机停产,但在2022年依然占有国内手机市场7.9%的份额;同时鸿蒙系统支持多终端,以智能手表为例,2022年华为国内市场占有率达到27%,位居第一。这推动了鸿蒙系统装机量快速上升。

三是兼容Android生态:可用性快速到位。

在智能终端时代,各类应用须保证“智能”的实现。在鸿蒙系统诞生之时,移动应用生态分属苹果的iOS和谷歌的

Android,两大阵营各自拥有数百万开发者和应用。

由于鸿蒙使用了AOSP,百万级Android应用基本上能够正常运行。差异在于运行的效率,如部分谷歌所提供专有能力的调用、部分终端权限的调取等方面。通过“借力”,鸿蒙应用生态直接从百万级起步,而非从“零”起步,使得终端可用性“一步到位”。

在发展后期,谷歌逐步开始调整应用格式,限制鸿蒙兼容Android应用,但鸿蒙此时已经通过自有生态建设,形成了一批鸿蒙原生应用,可独立发展。

四是自主生态发展:实现发展的可持续。

开发操作系统并不难,难的是建立相应的生态。鸿蒙系统在生态化发展方面,已经取得显著成效。一方面,在终端生态上,除了华为自有终端外,已有WIKO等其他品牌手机使用鸿蒙系统,一些发烧友在小米等其他手机品牌上适配鸿蒙;此外,由于鸿蒙是多终端系统,在智能家居、可穿戴设备等方面应用空间广阔。

另一方面,在应用生态上,华为以“开发者计划”扶持,以方舟编译器等技术手段赋能(从Android移植较快),截至2022年末,鸿蒙的注册开发者数量达到600万人,贡献了数十万个原生型的鸿蒙应用,与Android生态逐步实现脱钩。

五是系统通用赋能:着眼泛化终端空间。

华为鸿蒙在立项时,以开发物联网轻量系统为目标;2019年商用时,成为智慧大屏的系统之一;2021年,落地于智能手机;2023年,鸿蒙PC系统亦在测试中……而根据华为计划,鸿蒙系统将是“1+8+N”的全场景战略基石,可应用在各类终端上。

这也意味着,鸿蒙系统在开发过程中,未将应用方向“锁死”,而且不断强化通用底座特征,为后期开放式泛终端拓展奠定基础。而这种泛终端方式,也在苹果以及微软的新系统中得到体现。(作者为ICT行业资深分析师) 

编者按

党的二十大报告提出构建全域联动、立体高效的国家安全防护体系，以新安全格局保障新发展格局，为推进网络安全能力建设提供根本遵循。在第八个全民国家安全教育日（2023年4月15日）来临之际，《通信世界》特别策划，广邀行业专家共商共议，构筑网络安全产业新局面，服务经济社会高质量发展。

活力彰显 我国网络安全产业驶入“快车道”

■ 中国信息通信研究院 焦贝贝 黄媛媛 周杨

在政策扶持、需求扩张、应用创新的共同驱动下，我国网络安全产业发展活力凸显，技术和产业综合实力稳步提升，为应对新形势下网络安全挑战提供了坚实基础。同时，在需求释放、创新能力、协同效应方面仍有较大发展空间，

应加强政策引导、市场监管和产业协同，构筑产业高质量发展支撑力。

国家统筹谋划网络安全 产业发展新格局

随着数字化、网络化、智能化在更

广范围、更深层次上推进，网络安全形势愈发严峻复杂，网络安全的“压舱石”和基础保障作用日益凸显。党的二十大报告提出构建全域联动、立体高效的国家安全防护体系，以新安全格局保障新发展格局，为推进网络安



全能力建设提供根本遵循。

在党中央关于网络安全工作部署要求的指引下，网络安全“四梁八柱”逐步确立，顶层设计和总体布局不断优化，形成以国家政策为指引，以行业为抓手，以地区为牵引的多层次网络安全政策体系。在国家层面，2021年以来，我国充分发挥立法引领作用，《中华人民共和国数据安全法》《关键信息基础设施安全保护条例》《中华人民共和国个人信息保护法》等法律法规陆续出台，《网络产品安全漏洞管理规定》《网络安全审查办法》等重要规章制度加紧落地。在行业层面，电信、互联网、医疗、金融等重要行业的“十四五”规划、管理办法、指导意见集

中释放，网络安全成为各方关注焦点。在地区层面，网络和数据安全成为江苏、江西及广州等省市数字经济发展的重要着力点，湖南、河南及武汉等省市密集出台基础设施保护、人才培养的相关政策，推动网络安全产业高质量发展。

我国网络安全产业发展活力彰显

在国家、行业及地区多层次网络安全政策体系协同发力作用下，我国网络安全产业发展进入“快车道”，区域网络安全市场逐步成型，重要行业网络安全能力建设稳步推进，网络安全技术、产品和服务迭代升级，为应对新形势下网

络安全挑战提供了坚实基础。

产业规模快速增长 软硬产品部署逐渐优化

当前，我国网络安全产业处于快速成长期，根据中国信息通信研究院预测，2022年我国网络安全产业规模接近2200亿元；从长期发展趋势来看，近5年我国产业规模平均增速高出全球约4~5个百分点，产业发展活力显著增强。部署的产品形态结构正在发生渐进式调整，以终端安全、身份管理与访问控制等为代表的软件产品在网络安全销售中的占比快速增加，2022年调研数据显示，软件占比超四成，表明行业用户安全产品部署从“重硬轻软”到“软硬结合”逐步优化。

区域市场格局初现 网络安全与信息化建设同频共振

我国各地区网络安全市场稳步发展,基本形成“三强四促”的市场格局。其中,华北、华东和华南地区成为网络安全发展前三强,市场份额占比分别达到30.7%、27.7%和13.5%,较高的数字经济产值和信息化建设水平为上述区域网络安全市场提供先发优势。此外,华中、西南、西北和东北四大区域正在蓄力赶超,多地政府出台促进网络安全产业发展的规划举措。如河南省自2016年起先后出台70余项网络安全政策规定,不断加快网络安全体制机制建设;四川省于2022年5月获批建设国家网络安全产业园区(成渝地区),将打造引领西部网络安全产业的创新发展高地。

重要行业增加网络安全投入 全面强化安全能力建设

随着数字化、网络化、智能化的深入推进,网络安全对各行各业的保障和赋能作用愈加凸显,成为行业平稳发展的基础和底线。政府、金融、电信、能源等关乎国计民生的重要领域面临的网络威胁持续升级,遭受的攻击长期位居前列。在此背景下,重要领域的安全能力构建正在加速推进,拉动相关安全建设投资增长,根据2022年调研数据,来自政府、金融和电信三大领域的营收合计占网络安全企业营收的六成左右。

紧跟演进升级前沿 网络安全新技术新理念蓬勃发展

随着ICT环境创新变革,攻击技术和安全威胁演进升级,促使安全技术和防御思路适应性发展,以“零信任”、云原生安全、安全自动编排为代表的新技术新理念受到业界高度关注,安全技术向着动态边界、协同联动、安全云化等趋势演进。其中,以“零信任”技术为代表的动态边界,可较好地应对边界泛化带来的身份与访问风险;以云原生安全

技术为代表的安全云化,能够助力提升云化基础设施和平台安全防护能力;以安全自动编排为代表的协同联动,提高了多源系统设备的协同和响应效率。

新兴领域成发力重点 网安企业打造场景化安全能力

当前,随着数字经济向深向实发展,新兴领域对于安全保障的需求与日俱增。网络安全企业把握新兴领域安全产品及服务需求增长机遇,2022年调研数据显示,超过六成企业深化布局在工业互联网、物联网等领域的产品。在工业互联网安全方面,面向智慧生产、智能制造等IT和OT深度融合的场景,着力构建一体化纵深防御体系;在物联网安全方面,针对多协议及海量异构设备接入场景,综合利用态势感知、入侵检测与防御等技术,实现对复杂威胁的预判和抵御。未来,新兴领域有望迎来一批综合保障能力强、业务场景融合深的安全产品、专业服务和解决方案。

对网络安全产业发展的 思考与建议

在政策扶持、技术引领、市场催化的共同驱动下,我国网络安全技术和产业综合实力稳步提升,但距离实现需求释放足、创新能力强、协同效应高的目标仍有较大提升空间,行业应加强政策引导、市场监管和产业协同,构筑产业高质量发展支撑力。

改善需求投入和采购秩序 营造产业发展新环境

近年来,网络安全下游行业数字化转型加速,对于安全保障的重视程度日益提升,但总体来看,仍存在网络安全预算少、招标采购不规范等问题。因此,行业应多措并举,激励用户增加安全投入,形成良好采购秩序,助力产业健康发展。一方面,对基础信息网络和重要

信息系统制定明确的安全评估保障要求和安全投入占比标准;另一方面,规范相关采购行为,政府和重点行业采购向应用效果突出的安全产品服务倾斜,坚决遏制“唯价格”“唯品牌”论,避免因安全市场“劣币驱逐良币”后果。

聚焦差异化技术优势 构建市场竞争新格局

近年来,网络安全企业研发投入高速增长,头部企业研发费用平均增速超过30%。然而网络安全产品高达上百种,加之调研发现多数企业采取“优化现有产品”“研发新产品”并重的策略,“撒胡椒面式”的研发资金配置方式不仅导致产品创新性差,也造成低水平同质化竞争。为减少重复研发和恶性竞争,一方面,应推动形成以技术先进性、应用效果等为尺度的评估认证机制,引导形成以产品服务能力为导向的竞争环境,促使企业聚焦先进技术产品研发;另一方面,结合当前国家、行业和细分领域安全需求特征,着力打造层次分明、重点突出的多类型市场主体,实现企业间有序竞合、共赢发展。

优化产业协同 激发网络安全市场新动力

我国网络安全产业链涉及企业众多,覆盖网络安全设备、软件、服务、集成等各环节,为促进产业有序发展,应进一步提升协同效能。一方面,鼓励国家智库、行业组织、联盟等发挥网络安全创新枢纽和平台优势,支撑技术研发、示范应用、人才培养、论坛交流等活动开展,形成良好的创新生态;另一方面,倡导企业间通过联合研发、协同建设、资源整合等形式进行技术创新合作,加强网络安全技术、最佳实践和威胁应对等方面协同联动和信息共享,持续激发创新活力。CWV

中国信通院副院长魏亮 以技管网，开创行业反诈新格局

■ 本刊记者 甄清岚（整理）

随着我国信息技术快速发展，电信网络诈骗已成为当前社会面临的重大安全威胁之一。公安部发布的最新数据显示，2022年我国共破获电信网络诈骗案件46.4万起。电信网络诈骗的手段千变万化，包括虚假中奖信息、冒充公检法部门进行电话诈骗、冒充亲戚朋友求助等，这些诈骗行为通常以虚假名义骗取受害人的个人信息和财产，给个人和社会带来极大的损失。

2023年4月15日是我国第八个“全民国家安全教育日”。对此，中国信息通信研究院副院长魏亮受邀参与通信世界全媒体采访，探讨中国信息通信研究院在助推电信网络诈骗防范治理方面取得的成果、我国电信网络诈骗治理面临的困难与挑战，以及中国信息通信研究院对此的工作部署。

《通信世界》：近两年，中国信息通信研究院在推动电信网络诈骗治理工作方面做了哪些重点工作？取得了哪些成效？

魏亮：中国信息通信研究院深入贯彻落实党的二十大精神，坚决贯彻党中央、国务院决策部署，坚持以人民为中心，在工信部网安局的指导下，聚焦突出问题，狠抓工作落实，初心如磐，奋楫笃行，创新推出多项反诈利器，扎实推进



中国信息通信研究院副院长 魏亮

行业反诈工作取得历史性突破。

一是聚焦突出问题，深化行业源头治理。针对号卡、“黑灰产”设备涉诈高发问题，中国信息通信研究院支撑开展“断卡行动2.0”“打猫（猫池、GOIP设备）”等专项行动，全面清理涉诈高风险卡1亿多张、互联网账号9600万个、“涉猫”设备超2万个，强力压缩了不法分子的犯罪空间。

二是强化预警预防，大幅提升预警实效。中国信息通信研究院先后上线全国移动电话卡和互联网账号“一证通查”便民服务，创新推出12381涉诈预警劝阻短信系统，累计发送预警信息近6亿条，直接避免约900万用户受骗；推出“反诈名片”服务，大幅提升公安机关预警劝阻电话接通率。

三是坚持创新引领，筑牢反诈技术

屏障。中国信息通信研究院高效建成信息通信行业反诈大平台，对接百余家单位的反诈能力，首次实现了行业反诈工作的集中指挥调度、统一资源整合、“秒级”响应处置能力，用心、用情、用力守好群众“钱袋子”。

《通信世界》：当前我国在电信网络诈骗治理中还面临哪些困难与挑战？

魏亮：众所周知，电信网络诈骗不是简单的社会治安问题，而是复杂的社会治理难题。在超常规的严打、严防、严控高压态势下，防范打击电信网络诈骗工作的长期性、复杂性日益凸显，犯罪手法不断翻新，呈现出以下新趋势及新特点。

一是翻新迭代，诈骗迷惑性持续增强。当今时代，在新一轮科技革命推动下，人民群众的生产生活方式加速向网上转移，涉诈网络犯罪案件数量也持续高发。虚拟现实、增强现实等新兴技术迅速发展，元宇宙等虚拟世界概念越发普及，这些新技术和新概念将成为网络诈骗“新阵地”，进一步增加了诈骗的迷惑性。

二是跨境跨网，打击治理难度升级。涉诈资源及传播渠道跨境趋势明显，2022年境外接入的涉诈网站占比

达九成以上,涉诈APP主要由境外接入,涉诈资源的跨境化严重阻碍了溯源打击难度。与此同时,随着近几年持续有力打击,传统电话诈骗高发势头得到明显遏制,作案途径主要向互联网蔓延,明显提高了诈骗手段的隐蔽性,加大了打击治理难度。

三是敌暗我明,攻防对抗烈度加剧。当下,在与诈骗分子技术博弈的过程中,反制技术的研发往往滞后于诈骗手段的更新迭代。如诈骗分子借助呼叫转移、开发新型“简易组网GOIP”等投入小、成本低的方式,想方设法规避已有的反制技术。此外,电信和互联网业务规模庞大,风险评估和管理任务重,稍有不慎,诈骗分子就会发现利用新漏洞、更新诈骗方法,并在短时间内大量作案。

《通信世界》:下一步中国信息通信研究院将采取哪些措施或手段,加强电信网络诈骗的治理工作?

魏亮:2023年是全面贯彻落实党

的二十大精神的开局之年,是《反电信网络诈骗法》施行的开篇之年,也是承上启下、巩固提升反诈治理成效的关键之年。下一步,中国信息通信研究院要以党的二十大精神为指引,按照党中央、国务院以及工信部的工作部署,聚焦《反电信网络诈骗法》落实工作,坚持系统观念、问题导向,加大工作力度,以新气象、新担当、新作为开创行业反诈新局面,为有效遏制全国电信网络诈骗高发多发态势作出新的更大贡献。

一是提高政治站位,推进依法治理。中国信息通信研究院将深入贯彻党的二十大精神,坚持以人民为中心,围绕《反电信网络诈骗法》有关要求,全力支持工信部制定相关配套政策措施,进一步深化、细化、实化法律规定,督促指导相关企业落实落细《反电信网络诈骗法》各项要求,推动《反电信网络诈骗法》迅速落实见效,坚决遏制电信网络诈骗案件多发高发态势。

二是聚焦重点难点,强化源头治

理。持续深化“断卡行动2.0”“打猫”等专项行动,强化电话卡、物联网卡、宽带、短信端口等基础业务风险防范,支撑开展互联网领域、跨境电信业务、涉诈移动应用程序等专项治理,稳步推进失信惩戒工作,巩固提升工作成效。

三是强化以技管网,提升技防能力。不断完善信息通信行业反诈大平台功能,做好“部一省一企”反诈系统平台联通、能力联动、数据共享,积极推动跨行业涉诈数据共享、协同联动,加快建立统一的行业涉诈资源库,加大“一证通查”、12381预警系统、“反诈名片”等应用推广力度,切实提升技术反制能力,全链条挤压涉诈犯罪空间。

四是加大宣传力度,增强防范意识。加强专业队伍建设,健全反诈工作保障体系,支撑开展多轮次、全覆盖的《反电信网络诈骗法》宣贯培训工作,在全行业范围内强化普法宣传和防诈教育,建立全方位、广覆盖的反诈宣传体系,营造全民反诈的浓厚氛围,坚决遏制电信网络诈骗案件多发高发态势。 





新形势下的车联网 安全风险及应对

■ 中国信息通信研究院 张宁 李文 赵爽 柯皓仁

车联网作为新一代网络通信技术与汽车、电子、道路交通运输等领域深度融合的新型产业形态,已成为推动汽车制造业高质量发展的重要引擎。目前,发展车联网已成为多国重要战略选择。欧美以自动驾驶和智能交通为切入点,强化政策导向驱动车联网快速发展。我国主导单车智能和网联赋能并行

发展的路线,车联网无线通信技术装备不断普及、政策体系不断完善,车联网迎来产业发展黄金期、布局关键期。然而,伴随车联网的快速发展,网络攻击方式也不断升级,网络入侵、数据窃取、非法控车等攻击影响不断扩大,汽车、平台、网络、数据等要素安全风险交织叠加,威胁隐患不容忽视。业界亟需加

强车联网安全风险防范应对能力,推动车联网产业高质量发展。

车联网安全风险

一是汽车及核心部件风险隐患突出。智能网联汽车系统运行上亿行代码量,软件和网络存在的安全漏洞威胁车辆运行安全。其中,车载信息交互系



统、智能网关等核心部件存在的缓存溢出、代码注入等安全漏洞，易被攻击者利用，以此构建控车攻击链，实现远程操控车窗车门、控制车辆启动转向等。2023年1月，近20家汽车制造商曝出API安全漏洞，这些漏洞可以被黑客利用进行各种恶意活动，包括解锁、启动和跟踪汽车，甚至可访问企业内部门户网站，窃取大量车主详细信息。

二是车联网服务平台频繁遭受攻击。车联网服务平台提供信息交互、车辆控制、软件升级等服务，攻击者可通过互联网直接入侵渗透，对车辆实施远程操控，并通过篡改无人驾驶车辆的自动驾驶路线或恶意派发软件升级任务，危害车辆行驶安全。监测数据显示，近年来针对我国车联网服务平台的攻击频发，2022年累计达620.7万次，同比增长74.26%。2022年9月，俄罗斯本土网约车巨头Yandex的服务平台被入侵，黑客伪造车辆调度信息并通过平台下发虚假订单，大量汽车在莫斯科市中心集聚，造成严重交通堵塞。

三是车联网通信安全防护极为薄弱。当前，联网汽车数量和通信需求不

断增长，据统计，具备组合驾驶辅助功能（L2级）的乘用车渗透率达33.6%，预计2025年各级别自动驾驶渗透率将合计达到80%。车联网通信连接对象多样，应用场景丰富，通信协议、网络接入等普遍存在身份伪造、未加密传输、会话劫持等安全风险，易造成通信数据泄露，干扰汽车自动驾驶判断，进而引发交通事故。2022年5月，特斯拉的“无钥匙进入系统”曝出重大安全漏洞，攻击者可以通过对BLE低功耗蓝牙通信的中继攻击，在10秒内解锁一辆特斯拉Model 3或Model Y。

四是数据泄露和违规跨境流动风险日趋严峻。车联网数据安全贯穿智能网联汽车、通信网络、手机APP以及服务平台之间的各个互联互通过程，数据安全防护目标复杂多样。近年来，随着产业规模和价值急剧提升，车联网数据已成为黑客的重点攻击目标，任一过程管理不严或者数据防护不当，都将导致数据被不法分子窃取或篡改，造成用户数据泄露，个人隐私、企业权益受到侵害。2022年10月，意大利汽车制造商法拉利遭到勒索，包括企业内部文档在

内的总计6.99GB商业文档被窃取。此外，随着全球车联网行业的高度融合以及数据黑色产业链的不断发展，出境数据被滥用和售卖的现象频频发生，势必产生数据跨境流动安全隐患。

车联网安全应对措施

首先，车联网安全政策密集出台，体系逐步健全完善。近年来，我国先后发布《新能源汽车产业发展规划（2021—2025年）》《智能汽车创新发展战略》《车联网（智能网联汽车）产业发展行动计划》等多项政策措施，要求车联网企业健全安全管理体系、强化安全技术能力。自2021年起，相继发布《网络产品安全漏洞管理规定的通知》《关于加强智能网联汽车生产企业及产品准入管理的意见》《汽车数据安全若干规定（试行）》《关于加强车联网网络安全和数据安全工作的通知》等文件，紧抓车联网安全多项重点工作任务，加强智能网联汽车企业和产品准入、车联网安全防护、汽车数据安全、汽车产品安全漏洞管理、车联网卡实名登记等重点领域部署。近期，

《道路机动车辆生产准入许可管理条例（征求意见稿）》《关于开展智能网联汽车准入和上路通行试点工作的通知》（拟征求意见，还未施行）向社会公开征求意见，就智能网联汽车企业和产品准入提出行驶安全、功能安全、预期功能安全、网络和数据安全方面的原则性要求。

其次，发布车联网安全标准框架，强化标准体系布局。2022年2月，工业和信息化部发布《车联网网络安全和数据安全标准体系建设指南》，强化标准体系化建设，覆盖总体与基础共性标准、终端与设施网络安全标准、网联通信安全标准、数据安全标准、应用服务安全标准、安全保障与支撑标准六大重点领域及方向，布局103项标准项目。中国通信标准化协会（CCSA）在TC8下正式成立“车联网安全任务组（TF2）”，汇聚汽车生产企业、基础电信企业、互联网企业、零部件制造商、网络安全企业、科研单位、高校等百余产业链重点单位，聚焦车联网平台防护、数据安全、个人信息保护、供应链风险管理、能力成熟度评价等重点领域，高效推进车联网安全标准的研制和应用，目前已发布国家标准、行业标准、团体标准共16项，同步推进OTA安全技术要求、平台安全防护监测、数据安全保护要求、安全管理接口规范、车联网卡实名登记等55项标准。

最后，搭建产业合作交流平台，促进综合安全能力提升。一是搭建产业界合作交流平台。2021年3月，在工业和信息化部指导下，中国信通院牵头成立了车联网安全工作专班，为产业界提供深度交流和技术创新的引领性、先导性平台。目前，专班已成功召开7次会议，成员单位共108家，覆盖整车企业、零部件企业、服务平台企业、安全企业、科研机构及高校等，从政策研究、标准

研制、人才培养和产业孵化等方面，加快推进车联网网络与数据安全落地，护航车联网产业安全健康发展。二是产业各方积极开展实践。汽车生产企业开始建立整车开发安全流程管理体系，将网络安全贯穿车辆设计整个生命周期，网络安全架构设计逐步深入。产业链上下游企业协同共建，积极探索实践入侵检测、安全防御等技术整合，联合打造网络安全实验室、靶场等，安全技术不断创新、人才队伍日益壮大。第三方专业机构等积极发布车联网安全检测工具箱及安全测试能力，车联网产业安全能力逐渐提升。

基于车联网安全风险的思考和建议

一是加快车联网安全管理制度体系构建。坚决落实《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《关键信息基础设施管理条例》，以及车联网网络安全分级防护、汽车产品安全漏洞管理、数据分类分级管理、重要数据识别备案、车联网卡实名登记等规定要求。加快出台《道路机动车辆生产准入许可管理条例》，纳入汽车网络安全、数据安全等相关要求，改善汽车安全“基因”，对于重要车联网服务平台实施更加严格的安全管理。着力推动企业安全责任落实，部署车联网安全能力提升专项行动，组织汽车生产企业、车联网服务平台企业、基础电信企业、零部件供应商、网络安全机构等，围绕车辆、平台、通信、数据等安全风险点，开展安全自查互检，联动处置安全隐患，促进安全能力协同建设。

二是提升车联网安全防护能力。加快推进车联网安全防护建设，深入实施车联网网络安全定级备案，落实车联网网络安全分级防护措施，加强车辆设

计、制造、测试验证等全过程安全能力，开展整车及关键部件、服务平台、车路协同系统网络安全检测，完善风险监测技术手段，提升监测预警和应急处置能力。强化整车安全漏洞管理，加大整车安全漏洞收集、研判、通报、处罚力度，有效督促漏洞风险的修补处置。增强车路协同通信安全保障，推动建立全国统一的车车、车路、车云、车设备安全互认通信机制。

三是强化车联网安全标准研制。以车联网安全标准体系框架为指引，有序开展车联网安全领域重点急需标准的研制和发布，同步推进其他标准的研制进程，加快车联网安全标准体系建设。加快推进车联网平台防护、安全检测、在线升级、重要数据识别、数据安全保护等政策配套性、技术指引性标准的立项研制，对车辆远程监控、软件在线升级等车联网服务实施强制性安全要求，开展标准宣贯、安全体检、评估评优等活动，为行业企业提供可用、好用、管用的安全管理、建设和实施依据。加大国际车联网网络安全标准化工作力度，支持国内标准的国际转化，提升国际标准影响力。

四是加快构建车联网安全产业生态体系。推动安全技术产品创新，充分发挥车联网安全专班、车联网安全任务组等行业组织作用，整合技术优势和资源优势，开展整车网络安全能力评价、攻防演练、技术竞赛等活动，提升产业安全保障能力。加快建立并完善车联网安全测试评价体系，推动建设综合性、全链条安全测试场，覆盖智能网联汽车、网络基础设施、路侧设施、车联网服务平台等核心要素场景，完善安全测评方法，搭建车联网安全测试和公共服务平台，不断升级完善安全测试评价能力，提升车联网安全产业保障水平。



跨境电信网络诈骗 形势特点分析与治理路径研究

■ 中国信息通信研究院 王玉环 常雯 崔现东 马宁宁

近年来,随着我国信息网络技术快速发展,传统犯罪持续下降,以电信网络诈骗为代表的新型网络犯罪持续高发多发。为坚决遏制我国电信网络诈骗犯罪快速上升势头,各地区相关部门多措并举,“打防管控”齐发力,我国电信网络诈骗治理工作取得实效。据公安部统计,截至2022年11月底,我国共破

获电信网络诈骗案件39.1万起,同比上升5.7%,抓获犯罪嫌疑人同比上升64.4%,立案数同比下降17.3%,造成财产损失总价值同比下降1.3%。受国内高压治理影响,境内诈骗分子纷纷转向境外,频频通过在境外拨打诈骗电话、发送诈骗短信、租用服务器搭建诈骗网站,对境内用户实施诈骗犯罪行为,人

民群众的生命财产安全受到严重威胁,正常生活受到严重干扰。

跨境电信网络诈骗当前的形势与特点

随着我国对电信网络诈骗犯罪打击力度的持续加大,境内电信网络诈骗活动空间被明显压缩,诈骗分子“走出国

门”，逐步向境外转移，形成组织严密、分工明确、境内外衔接紧密的诈骗团伙，屡屡对我国公民实施诈骗行为。公安部2022年披露的数据显示，我国电信网络诈骗犯罪境外作案占比已高达80%，跨境诈骗形势愈发严峻。据统计，2022年我国境外呼入的诈骗电话超半数，境外接入的诈骗网站超九成。目前，境外电信网络诈骗呈现以下特点与趋势。

一是境外诈骗电话多为虚拟电话且资费低。在境外，诈骗分子一般采用网络电话APP，使用手机号+短信/语音验证或邮箱账号完成注册后，按照国家、省份/州、区号等筛选条件，购买不同国家的电话号码，拨打诈骗电话。同时，由于网络电话APP不安装手机卡也可使用，注册成功后还赠送一部分话费，在接码平台、云控平台、一次性邮箱平台助力下，可批量注册免费境外号码和购买收费号码，甚至可以实现批量外呼。

二是境外诈骗短信套路多变且多含有链接。境外短信诈骗案件特点之一是紧跟社会热点，内容不断更新，短信内容以贷款、刷单、网络赌博等为主。但诈骗分子无论是以贷款为由，还是以刷单兼职的名义，他们的诈骗方式万变不离其宗，都是在短信内带有引诱性的链接，引导人们点击后填写个人信息，从而转走钱财。

三是诈骗网站多为境外接入与境外注册。由于境外对域名注册、IP服务器使用的监管较为宽松，诈骗分子大量租用境外服务器搭建诈骗网站，以躲避有关部门的监管和治理。据统计，2022年我国有超九成的诈骗网站在境外接入。从注册特征看，归属于境外域名注册服务机构和域名注册管理机构的诈骗网站占比持续增多。

四是有组织特征的跨国电信网络诈骗日趋明显。藏匿在境外的诈骗团伙，或打着高薪招聘的幌子，诱骗涉世

未深的年轻人赴境外从事诈骗活动；或通过拨打诈骗电话、发送诈骗短信实施诈骗犯罪活动；或通过境外聊天软件，指挥境内人员从事APP制作开发、引流推广、贩卖个人信息、转账洗钱等各类违法犯罪行为。诈骗套路层出不穷，诈骗技术不断迭代升级，让人防不胜防。

跨境电信网络诈骗治理难点分析

当前，跨境诈骗手法套路多变、境内外衔接紧密、跨国有组织的犯罪愈发猖獗，为电信网络诈骗治理工作带来了巨大的挑战。

一是诈骗套路更新迭代迅速，识别难度大。诈骗分子利用人们不熟悉境外电话号码有关特征，编造各类诈骗“话术”，同时利用区块链、元宇宙、虚拟货币、AI、GOIP等新技术，不断更新犯罪工具和诈骗手法，使其更具隐蔽性和迷惑性，难以监测识别，人民群众很容易上当受骗。如近日有网友反馈，自己遭到了境外诈骗电话“围剿”，不到5分钟接到6个境外来电，这些号码涉及泰国、新加坡、菲律宾、美国、挪威甚至斐济。

二是跨国有组织犯罪愈发猖獗，打击治理更加困难。境外诈骗集团组织严密、分工明确，且呈现多行业支撑、产业化分布、集团化运作、精细化分工等跨国有组织犯罪特征，为打击治理工作带来较大挑战。以境外诈骗电话为例，藏匿在境外的诈骗分子利用远程控制软件，操控境内人员搭建GOIP等非法集群设备，借以拨打诈骗电话、群发诈骗短信，这极大地增加了涉诈风险预警、阻断和线索分析难度，也对公安机关落地查人、实施精准打击带来较大挑战。

三是诈骗网站资源多在境外，难以及时处置。目前，互联网已成为实施电信网络诈骗的主要渠道，案件占比超80%。在互联网领域，诈骗分子多通过

境外的域名注册管理机构、域名注册服务机构获取域名资源，通过租用境外网络资源建立诈骗APP或虚假投资理财网站。在境内外诈骗团伙相互勾结以及“黑灰产”推波助澜下，现有技防能力难以发挥应有作用，架设于境外资源上的诈骗APP、诈骗网站等呈“井喷式”增长，而位于境外的诈骗网络资源也很难溯源核查并及时处置。

四是各国治理情况参差不齐，国际合作需强化。当前，电信网络诈骗已成为全球性治理难题，但各国治理侧重点不同，强度不一，特别是各国对于电话用户实名制、互联网账号实名、GOIP设备管理等相关要求不同，为境外诈骗分子实施犯罪行为提供了便利。如柬埔寨于2023年3月9日发布通告，要求所有电话卡必须实名，但对于境内逗留少于60日的人可以免除实名；而菲律宾亦是于2022年12月27日，才对新入网用户实施实名管理，对于预付卡要求在6个月内完成实名注册。此外，各国警方合作打击此类犯罪的框架性协议有待完善，因此难以及时启动侦查程序，跨境打击和调查取证难度大。

举措建议

为严厉打击跨境电信网络诈骗犯罪这一顽疾，响应国际社会共同呼声，我国相关部门应积极行动：一方面要主动参与反诈领域相关的国际会议、国际论坛，参与国际有关标准与策略制定，吸纳先进治理经验，贡献我国治理方案；另一方面要利用线上线下、主流媒体与新型媒体，加强普法宣传与反诈宣传，特别是境外诈骗方面的相关防范技巧以及《反电信网络诈骗法》中对帮信人员的惩戒措施，进而提升人民群众防范意识，教育劝返赴境外作案人员，不断破坏跨境诈骗滋生土壤，最大限度压缩境外诈骗分子生存空间。

电信和互联网行业数据安全人才发展洞察与思考

■ 中国信息通信研究院 姜宇泽 沈怡欣 庞妹 寇金锋

人才是“第一资源”，培养数据安全人才是护航数字中国建设的重要任务，是推动数据安全产业健康发展的前提条件。当前，随着数字经济进入专业化、具体化推进阶段，数据安全市场引起广泛关注，数据安全人才供需矛盾日益凸显，培育、强化、壮大数据安全人才队伍刻不容缓。本文基于数据安全人才供需调研，梳理数据安全人才现状，展望未来发展趋势，并提出针对性建议。

行业数据安全人才发展现状

数据安全人才队伍初具规模

抽样调研结果显示，我国数据安全人才队伍已初步建立，71.28%的基础电信企业形成5人左右数据安全团队，头部互联网企业大多成立虚拟数据安全委员会或工作组，形成跨部门的数据安全工作团队。此外，从业人员学历水平普遍较高，七成以上从业人员具有硕士研究生及以上学历；约80%的从业人员具有信息通信或计算机软件相关专业背景。信息通信企业数据安全团队成员专业分布如图1所示。

数据安全分岗定责模式已逐步确立

数据安全与业务深度耦合的特点导致其无法通过传统网络安全的边界防护模式实现安全保护目标。在抽样调研中发现，当前行业内组织机构已形成

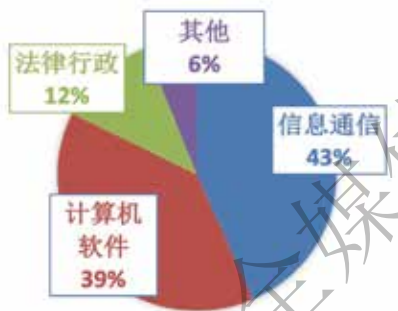


图1 信息通信企业数据安全团队成员专业分布

普遍共识，构建“统筹管理+分岗实施”体系，既延续了网络与信息安全管理系的格局，由数据安全管理部门统筹协调；又结合数据安全多层面防护需求，将数据安全工作“触角”由管理部门延伸至各业务及职能部门，由“单兵作战”向“团队作战”模式转变，树立总体一致目标，畅通绿色沟通渠道。

从业人员积极适应新职能、新角色

在我国，从政府部门、国有企事业单位到私营企业，数据安全大多带有传统信息安全保护、信息内容治理基因。当前阶段，“职业赛道”初步完成划分，职责细化逐渐明晰。随着所在岗位职能的转变及新岗位的增加，相关从业人员大多经历了“职业赛道”转换，并能够积极适应新职能、新角色。抽样调研结果显示，在现有从业人员中，70.68%经历过岗位转换，41.35%目前仍兼任其他岗位。

与此同时，组织机构积极组织在岗学习，帮助从业人员尽早适应全新岗位职责。抽样调研显示，80%以上的企业自主开展数据安全培训，57%的企业通过外聘讲师提升数据安全培训质量。然而，有63%的企业每年仅开展一次数据安全培训，表明培训频次亟待提升、培训形式亟待丰富、培训内容亟需扩展。

数据安全人才发展趋势

数据安全岗位数量持续走高

招聘平台数据显示，自2021年1月起，数据安全岗位数量稳步提升，在2022年第一季度达到高点，岗位数量增长率达73%，2022年1—9月，数据安全招聘岗位总量同比增长26%。此外，信息化领域作为数字产业化和产业数字化的前沿阵地，成为数据安全人才的主要聚集领域，IT、通信、电子、互联网行业岗位数量占比达87%左右。各行业数据安全岗位数量占比如图2所示。

数据安全人才供给多点发力

高等院校、社会培训组织齐发力，加速构建数据安全人才“蓄水池”。在长期专业人才培养方面，北京邮电大学等高校已逐步开启数据安全教学活动，开设数据安全相关专业方向及课程，同时采用产教融合新模式，通过召开数据安全相关研讨会及开展大数据安全分析竞

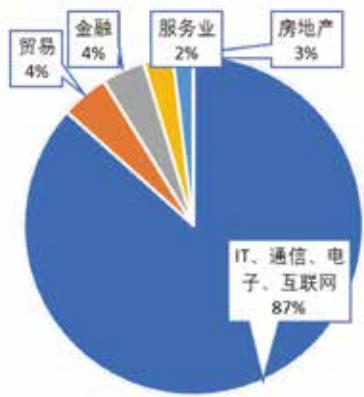


图2 各行业数据安全岗位数量占比

赛等方式,强化人才供需对接。在短期能力提升方面,数据安全社会培训掀起热潮。CISAW、CISP等知名安全培训品牌及中国信息通信研究院等科研机构率先推出数据安全培训课程,快速、高效、灵活提升在岗人员职业技能。

数据安全工作对人才能力提出更高要求

在专业技能方面,数据安全工作的高度复合性,要求从业人员将合规能力、技术能力及管理能力融会贯通。在实践经验方面,数据追踪溯源难度大、数据安全技术迭代迅速、数据安全保护与业务工作结合紧密,使得工程和实践经验成为用人单位选才的重要标准。招聘平台数据显示,55%以上的数据安全岗位要求从事相关专业3年及以上,用人单位普遍通过丰厚薪资吸引从

业经验丰富的求职者,具有10年以上从业经历的人员薪资中位数超过3万元。用人单位对数据安全人才从业年限要求的统计如图3所示。

行业数据安全人才发展建议

形成人才顶层设计“大格局”

持续强化全社会

对人才培养工作的重视程度,做好数据安全人才培养工作顶层设计,是突破数据安全人才紧缺困境、直面数据安全人才培养挑战的首要选择。一是加快数据安全学科专业建设。推动高等院校、职业院校加强数据安全相关学科专业建设,发挥学科引领和带动作用,深化课程体系、师资队伍、实习实训等配套资源建设。二是推进高水平数据安全人才培养。鼓励高等院校、职业院校、科研机构、优质企业等创新人才培养方式,深化产教融合、协同育人,加快培养一批实用型、复合型的数据安全专业技术人才和优秀管理人才。三是完善数据安全人才培养配套机制。健全以创新能力、质量、实效、贡献为导向的科技人才评价体系,构建充分体现知识、技术等创新要素价值的激励和保障机制,遴选并

推广一批产业发展急需的数据安全人才培养项目。四是加强全民数据安全意识与技能培养。充分利用网络、广播、电影电视、报刊杂志等媒体平台,面向大众宣传数据安全常识,传播数据安全知识,培育数据安全文化。

构建人才供给“多渠道”

大力推动多方主体共同创新人才培养格局,丰富人才培养方式,畅通人才供给渠道,为数字经济发展提供源源不断的数据安全人才保障。充分发挥高校在培养数据安全基础型人才方面的主力军作用,加快推进设立数据安全专业学科,全方位谋划数据安全教育课程,集中优势力量在重点高校建设数据安全国家级重点实验室,加大政策支持和资金投入力度。培训机构要充分发挥自身灵活高效的特点,在深入调研数据安全人才培养需求的基础上,定制具备典型数据安全特色的培训课程,严格按照数据安全人才培养工作顶层部署,规范开展专业培训及能力认证工作。用人单位要严格落实相关法律法规及行业监管要求,建立健全本单位数据安全人才培养制度,定期组织内部培训,规范开展培训考核和评定工作。

涵养人才发展“生态圈”

要不断释放发展效能,持续激发人才驱动力,就要持续不断营造数据安全人才成长良好环境,深耕数据安全人才“成长沃土”,打造数据安全产业高质量发展“硬支撑”。一是加强“产学研用”合作,企业、院校、专业机构等各方协同互补,逐步形成并完善“输送、培养、历练、保障”四位一体的人才发展完整产业链条。二是搭建人才交流平台,建立健全人才共享、职称互认、人才交流等机制,精准助力供需对接,破除人才流动壁垒,逐渐形成数据安全人才培养的规模效应。三是营造数据安全人才发展良好环境,加大数据安全人才培养工作宣传力度,提升全行业数据安全人才培养意识,营造数据安全领域爱才、识才、惜才、用才的良好氛围,建设可持续的人才成长生态,助力数据安全产业高质量发展。CWW

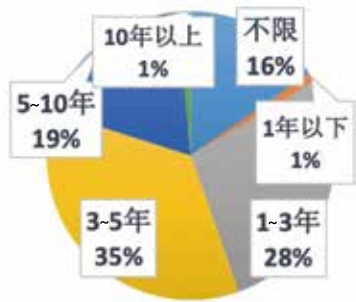
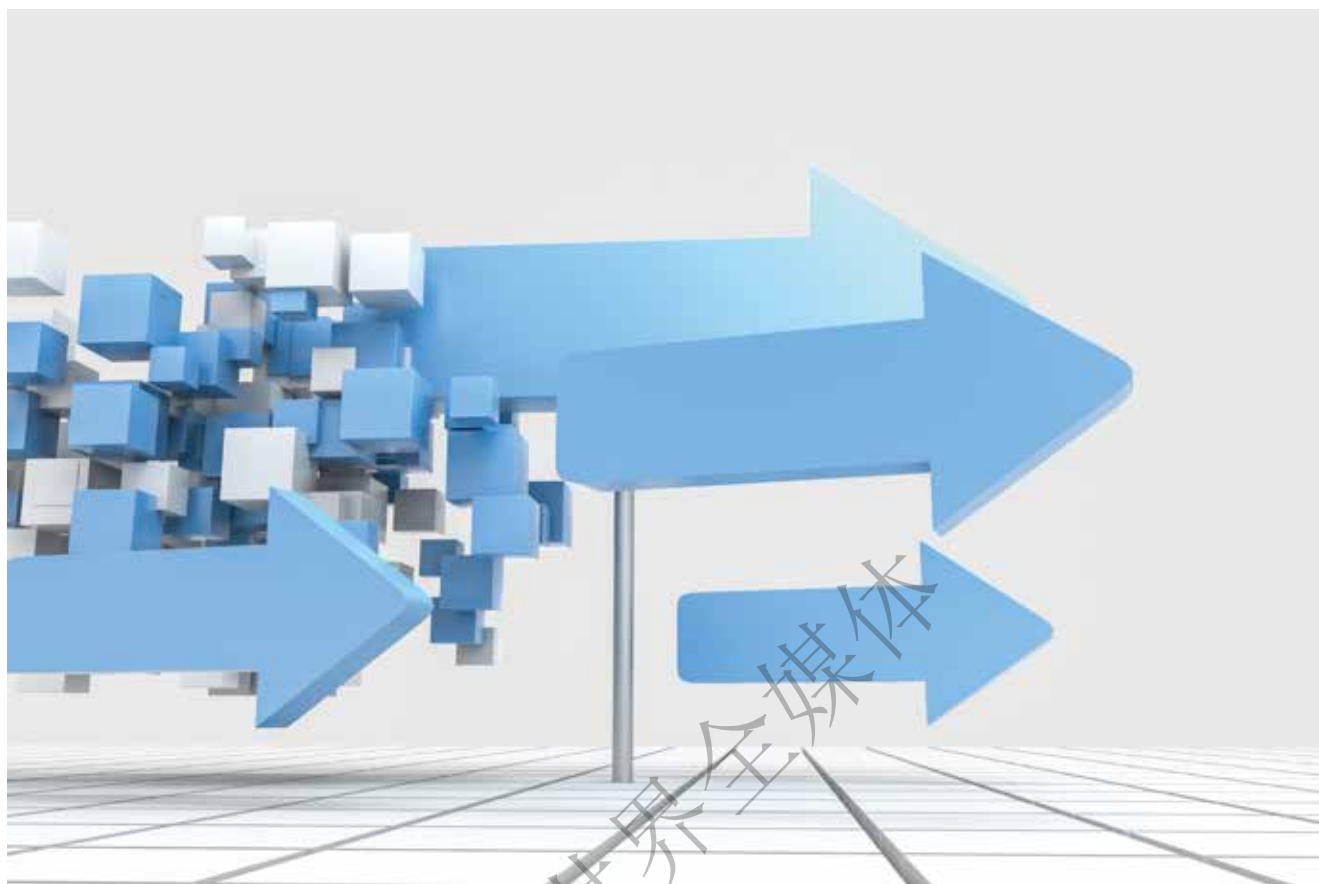


图3 用人单位对数据安全人才从业年限要求的统计



2022年 运营商业绩亮点及趋势展望

■ 中国电信研究院 胡世良

2023年3月，我国三大运营商陆续公布了2022年财报。

2022年是党的二十大召开之年，是实施“十四五”规划关键之年，也是我国踏上全面建设社会主义现代化新征程、向第二个百年奋斗目标进军的重要一年。从三大运营商2022年财报来看，其业绩继续保持稳健增长的发展势头，

亮点特征明显，在促进我国经济实现恢复性增长中发挥了重要作用。

2022年运营商业绩亮点

收入利润实现“双增长”，资本市场表现良好

2022年，面对疫情反复等国内外多重超预期因素的冲击，运营商坚持战

略定力，统筹疫情防控和经营发展工作，推动业务高质量发展，实现收入利润“双增长”。

2022年，中国电信实现经营收入4814亿元，同比增长9.5%，通信服务收入4349亿元，同比增长8.0%，净利润276亿元，同比增长6.3%；中国移动营收达到9373亿元，同比增长10.5%，

通信服务收入达到8121亿元,同比增长8.1%,净利润达到1255亿元,同比增长8.0%;中国联通实现营业收入3549亿元,同比增长8.3%,增速创近9年新高,通信服务收入达到3193亿元,同比增长7.8%,利润总额达到204亿元,同比增长14.4%。

从收入和利润来看,2022年三大运营商经营业绩表现出色,收入保持稳健增长,盈利能力持续提升。特别是数字化业务的快速发展,推动其从“传统管道运营商”向“数字化科技型企业”转变,良好的经营业绩也得到资本市场的认可。

持续推进价值经营,用户价值持续提升

巩固和发展基础业务、持续推进基于规模的价值经营成为三大运营商共同的经营策略,价值经营取得成效。

2022年,中国电信移动用户达到3.91亿户,移动用户ARPU达到45.2元,增长0.4%;宽带用户达到1.81亿户,千兆宽带渗透率达到16.8%,全屋Wi-Fi、天翼看家用户分别增长45.8%、52.7%,宽带综合ARPU达到46.3元,增长0.9%。

2022年,中国移动深化“连接+应用+权益”融合运营,移动ARPU达到49.0元,同比增长0.4%;家庭市场保持快速增长,家庭市场收入达到1166亿元,同比增长16.0%,家庭宽带用户达到2.44亿户,继续保持行业领先,千兆家庭宽带用户达到3833万户;智慧家庭增值业务对家庭市场收入增量贡献上升到55.9%,有效拉动用户价值提升,家庭用户综合ARPU达到42.1元,同比增长5.8%。

2022年,中国联通实现基础业务规模和价值双提升。移动出账用户达到3.2亿户,移动用户ARPU达到44.3元,同比增长0.91%。固网宽带出账用户超

过1亿户,融合渗透率达到75%,融合ARPU首破百元,进一步打开了家庭市场的广阔发展空间。

“第二曲线”增长加快,成为推动收入增长“第一动力”

2022年,三大运营商克服疫情及经济下行压力的影响,把握产业数字化发展机遇,全面发力政企市场,大力拓展5G融合应用,加快数字技术与实体经济深度融合,产业数字化快速发展,成为推动企业收入增长的“第一动力”。

中国电信积极把握经济社会数字化、智能化转型机遇,坚持以融云、融AI、融安全、融平台为驱动,推进“云网能力底座+行业应用平台”深度融合的产业数字化发展模式,为千行百业提供数字化整体解决方案,产业数字化发展迅速,天翼云收入实现翻番。2022年,中国电信产业数字化收入达到1178亿元,同比增长19.7%，“产数”收入占比达到27.1%，对收入增长的贡献率达到58.9%，成为拉动企业收入增长的“第一动力”。其中,天翼云收入达到579亿元,同比增长107.5%;网络安全服务收入达到47亿元,同比增长23.5%。

中国移动牢牢把握产业数字化发展机遇,积极拓展政企市场,强化“网+云+DICT”一体化拓展,云、5G“双引擎”拉动行业数字化快速发展。2022年,中国移动包括DICT在内的数字化转型收入达到2076亿元,同比增长30.3%,对收入增长的贡献率达到79.5%;其中DICT收入达到864亿元,同比增长38.8%;移动云收入达到503亿元,同比增长108.1%,综合实力迈入国内业界“第一阵营”。

中国联通按下产业互联网发展“快捷键”,2022年产业互联网业务收入达到705亿元,同比增长28.6%,收入占比达到22.1%,对收入增长的贡

献率达到67.7%,成为推动联通收入增长的“第一引擎”。其中,联通云实现收入361亿元,同比增速达到121%;物联网实现收入86亿元,同比增速达到42%;大数据收入达到40亿元,同比增长58%。

拓展5G融合应用,5G规模化发展取得突破

2022年,三大运营商积极贯彻国家5G发展战略,稳步推进5G网络建设,不断拓展5G融合应用。5G规模发展取得突破,成为推动运营商收入持续增长的新引擎。

5G网络覆盖能力持续提升。2022年,中国电信持续推进与中国联通网络共建共享,双方累计共建共享5G基站超过100万个,为全球通信行业贡献了共建共享关键技术和运营经验。中国移动深入推进与中国广电5G网络共建共享,实现全国城区、县城、乡镇连续覆盖,建成全球最大5G SA网络;2022年累计开通5G基站达到128.5万个,其中700MHz 5G基站达48万个。2022年,中国联通加快5G精品网建设,深入推进与中国电信共建共享,5G共享基站达到100万个,行政村覆盖率达到96%,5G中频规模和覆盖水平与行业相当。

面向个人市场,三大运营商加快5G用户规模发展。2022年,中国电信5G套餐用户达到2.68亿户,套餐渗透率达到68.5%;中国移动5G套餐用户达到6.14亿户,保持行业领先,套餐渗透率达到63%;中国联通5G套餐用户达到2.13亿户,套餐渗透率达到66%。

面向垂直行业市场,三大运营商加快5G融合应用规模化发展。2022年,中国电信推动5G行业应用及数字平台的业务能力和服务水平向纵深发展,丰富应用场景,推动模式升级,打造5G示范标杆,5G to B商用项目累计达1.5万

余个。中国移动持续推动5G专网实现全面产品化,推进9 one平台核心能力突破提升。2022年,中国移动累计签约5G行业商用案例超1.8万个,在智慧矿山、智慧工厂、智慧电力、智慧医院、智慧城市、自动驾驶等多个细分行业实现领先。2022年,中国联通持续升级5G专网产品体系,5G行业专网达到3800余个,5G规模化应用项目超过1.6万个,打造1600多个5G全连接工厂,铸就“5G+工业互联网”第一品牌。

强化创新驱动,科技创新实力不断增强

2022年,三大运营商强化创新驱动,坚持科技自立自强,加大研发投入,强化核心技术攻关,扩大科研队伍,科研实力不断增强,助力企业高质量发展、打造世界一流企业。

中国电信坚持“科技是第一生产力”,全力打造科技型企业。2022年,中国电信研发费用达到106亿元,较上年增长52.3%,研发费用占主营收入的比例达到2.43%,科技和产品研发人员达到2.23万人;R&D科技创新研发体系布局全面完成,实现核心技术自主掌控,天翼云4.0、5G边缘网络、新一代云网运营系统、AI、量子密话等技术创新取得明显成效;2022年国内发明专利和PCT专利申请数分别为2021年的1.4倍和2倍。

2022年,中国移动持续加大研发投入,深化研发机制创新和研发体系创新。2022年中国移动研发费用达到181亿元,同比增长16.1%,研发费用占主营收入比例达到2.22%,研发人员达到3.97万人。移动云、基础芯片、物联网操作系统等领域核心技术攻关取得突破,形成多项国产化自主产品;专利、标准化能力行业领先,累计牵头5G国际标准197个,申请5G专利超4100件,稳居全球运营商“第一阵营”。

中国联通以打造科技创新型企业为目标,实施创新驱动战略,加大核心技术攻关,高水平科技自立自强取得“里程碑式”进展。2022年,中国联通科协正式成立,聘任16名院士作为科技委特聘专家,研发投入强度不断加大。2022年中国联通研发费用达到68亿元,同比增长42.7%,研发费用占主营收入比例达到2.14%,研发人员数量达到1.88万人,授权专利数达到1666件,自主研发产品收入同比增长超过70%。

发展趋势展望

2023年是全面贯彻落实党的二十大精神开局之年,是实施“十四五”规划承上启下的关键之年。面对复杂的国际环境和各种不确定因素,运营商需要坚定信心,把握机遇,勇毅前行。

一是数字经济快速发展为我国电信业创造更大的发展空间。党的二十大报告指出,加快发展数字经济,促进数字经济和实体经济深度融合;2022年12月,中央经济工作会议提出,大力发展数字经济;2023年政府工作报告提出,“大力发展数字经济”“加快传统产业和中小企业数字化转型,着力提升高端化、智能化、绿色化水平”。这预示着我国数字经济必将迎来更大的发展机遇,为运营商转型发展创造更大的空间,运营商应牢牢把握机遇加快发展,转变发展模式,在助力我国经济“企稳回升”中发挥更大作用。

二是对2023年面临的困难、风险和挑战要有充分认识。2023年1-2月,我国工业生产恢复加快,服务业明显回升,市场销售由降转增,稳经济政策效果持续显现,经济运行整体呈现“企稳回升”的态势。但当前经济发展仍然面临诸多困难挑战,外部环境不确定性加大,需求收缩、供给冲击、预期转弱的三

重压力仍然存在。经济恢复的基础仍不牢固,实现2023年经济增长5%左右的目标既有希望,也有挑战。

经过综合研判,2023年我国电信业务收入增长将达到7.6%左右,较2022年略有下降。从2023年1-2月数据来看,我国电信业务收入同比增长7.9%,较2022年下降0.1个百分点,说明2023年我国电信业保持高速增长有压力、有挑战。因此,运营商要对发展面临的困难、风险和不确定性有充分准备,以确定性应对各种不确定性,重点从“供需”两端发力,促进电信业企稳发展。

三是锚定“打造世界一流企业”目标,真抓实干。从2022年三大运营商财报来看,经营业绩表现亮丽。三大运营商虽然连续多年进入“世界500强”,但应清醒地认识到运营商与“世界一流企业”尚有较大差距,主要表现在:科技创新实力不强,在操作系统、芯片等底层技术、共性技术、关键技术上缺乏话语权;品牌战略不够清晰,品牌影响力不高,品牌内涵缺乏科技感、现代感和时尚感;产品供给不能有效满足日益增长的数字化需求,真正叫得响、广受欢迎用户欢迎的数字化平台和应用服务不多,产品品质和附加值较低;企业治理尚不适应企业转型发展的需要,现代企业治理能力有待进一步提升。

对于我国电信运营商来说,企业发展不仅要追求收入规模和资本市场的良好表现,还要向打造世界一流企业的目标迈进,从转变发展方式、强化科技创新、打造高品质数字化产品、打造卓越企业品牌和产品品牌、提升企业现代化治理能力、建立健全创新体系等方面系统推进、攻坚克难、勇于创新、综合施策,这才是企业转型发展的重中之重。 

财报解读

穿越周期 运营商绘就“第二曲线”

■ 山东工商学院法学系 于宗平

随着3月23日中国移动发布2022年财报，三大运营商2022年“成绩单”悉数公布。在宏观经济承压前行、“人口红利”增长见顶、传统业务疲态渐显的背景下，三大运营商能够取得8%以上的营收增长率和6%以上的净利润增长率，可谓是“逆势而上、殊为不易”。如此亮丽的“成绩单”，也为业界带来了融融暖意。

能够突破大环境限制，实现主要指标强劲增长，三大运营商深耕“第二曲线”功不可没。当作为“第一曲线”的传统业务增长乏力之时，运营商迎接数字经济浪潮，畅通连接“大动脉”，穿越成长周期，打造“第二曲线”。三大运营商在此次披露的财报中纷纷提及：“第二曲线”加速发展、打造“第二曲线”取得积极成效……

蝶变“第二曲线”

财报数据显示，2022年中国电信实现营收4814.48亿元，同比增长9.5%；中国移动实现营收9372.59亿元，同比增长10.5%；中国联通实现营收3549.44亿元，同比增长8.3%。中国电信净利润为275.93亿元，同比增长6.3%；中国移动净利润为1254.59亿元，同比增长8.0%；中国联通净利润为

167.45亿元，同比增长16.5%。无论从营收还是净利润来看，三大运营商的财务数据均令业界倍感振奋。

在总体呈现快速增长的态势下，不同业务的发展却快慢不一。以中国电信为例，其2022年实现基础业务收入3096亿元，同比增长4.0%，拉动收入增长2.9个百分点；实现产业数字化收入1178亿元，同比增长19.7%，拉动收入增长4.7个百分点。“基础业务作为基本盘、产业数字化业务作为新引擎”的格局清晰可见，这里的产业数字化即“第二曲线”。

在信息通信行业，“第二曲线”的首位提出者是中国移动董事长杨杰。在2021年世界移动通信大会上，杨杰表示：“运营商把握数字经济机遇，关键就是要通过数智化转型，形成以网络为基础、

信息技术和数据要素为驱动的新增长模式，打造自身发展的‘第二曲线’，在助力经济社会发展中发挥更大作用。”

目前，发展“第二曲线”已经成为三大运营商的共识。运营商积极探索“第二曲线”，并赋予其不同内涵，比如中国移动称之为数字化转型，中国电信称之为产业数字化，中国联通称之为产业互联网。

从2022年财报看，三大运营商的“第二曲线”增势强劲，成为拉动收入增长的重要力量。除上述的中国电信外，中国移动2022年实现数字化转型收入2076亿元，同比增长30.3%；中国联通实现产业互联网收入705亿元，同比增长28.6%。三大运营商“第二曲线”具体规模和通信服务收入中的占比见表1。

表1 三大运营商“第二曲线”相关业务规模及占比

类别		2020年	2021年	2022年
中国电信 产业数字化	收入(亿元)	840	984	1178
	在通信服务收入中的占比	22.5%	24.4%	27.1%
中国移动 数字化转型	收入(亿元)	1262	1594	2076
	在通信服务收入中的占比	18.1%	21.2%	25.6%
中国联通 产业互联网	收入(亿元)	427	548	705
	在通信服务收入中的占比	15.5%	18.5%	22.1%

当传统业务增长触顶时，三大运营商正穿越“第一曲线”的成长周期，以数据中心、云计算、大数据、物联网等为着力点，打造数字化转型的“第二曲线”，赋能数字经济高质量发展，开辟新“蓝海”空间。

“花开”多个领域

虽然三大运营商对于“第二曲线”的定义不尽相同，但是云计算、物联网、5G专网、网络安全等已成为共同选项。运营商在这些细分领域表现亮眼，近年来增长速度非常可观。

作为“第二曲线”的核心，三大运营商的云业务跑出了新速度。2022年，中国电信天翼云实现营收579亿元，同比增长108%；中国移动云业务实现营收503亿元，同比增长108%；中国联通云业务实现营收361亿元，同比增长121%。这是继2021年大幅增长后，运营商云业务再度实现快速增长，成为“第二曲线”的重要组成部分。表2为三大运营商近年来的云业务收入规模及增速。

2022年，三大运营商均实现了“物超人”，物联网也因此成为运营商收入增长的重要支柱。中国电信物联网收入达40.1亿元，同比增长40.2%，连接规模超4亿个；中国联通物联网收入达86亿元，同比增长42%，物联网连接数约为3.9亿，在5G连接新增市

场中的份额接近七成；中国移动物联网收入达154.4亿元，同比增长35.5%，物联网连接数达16.9亿，总连接规模全球第一。

以5G网络为依托，三大运营商聚焦行业应用市场，构建数字化平台底座，持续沉淀原子能力，推动5G行业应用及数字平台纵深发展，充分释放5G网络价值。中国电信聚焦5G行业应用场景，累计发展近1.5万个5G to B商用项目，其中2022年新增项目超过8000个；中国移动累计签约5G行业商用案例超过1.8万个，2022年带动DICT项目签约金额达到365亿元，5G专网收入达到25.5亿元，同比增长107.4%；中国联通累计打造1.6万多个5G规模化应用项目，规模复制到国民经济52个大类，打造了1600余个5G全连接工厂。

此外，运营商在网络安全、大数据、AI等板块多点发力，实现了多个领域业绩的快速增长，推动运营商“第二曲线”持续上扬。

重构估值模型

英国管理大师查尔斯·汉迪在《第二曲线：跨越“S型曲线”的二次增长》中写道：“在第一曲线达到巅峰之前，找到驱动企业二次腾飞的第二曲线，且第二曲线必须在第一曲线达到顶点之前开始增长，企业永续增长的

愿景才能实现。”

目前，三大运营商正穿越“第一曲线”的成长周期，绘就持续增长的“第二曲线”，着力打造新的差异化竞争优势，迸发出全新的增长活力。这也证明，运营商把握数字经济时代网络化、数字化、智能化的综合信息服务需求，探索高质量发展道路的尝试已取得初步成效。

随着“第二曲线”的出现，运营商的估值模型也需重新架构。正如中国联通董事长刘烈宏所言：“今天的中国联通，正在从传统‘管道’运营商向数字科技领军企业加速转型，联接规模和联接结构、核心功能、服务和赋能水平、发展理念都实现了转型升级，打破了传统运营商连接‘管道’、恶性竞争和创新不足的三大估值‘天花板’。仅用衡量联接价值的‘一把直尺’，已经量不出五大赛道价值的‘多维空间’，至少需要‘五把尺子’甚至更多的模型来测算。”

展望2023年，数字中国建设走向深入，数字经济空间无可限量，为行业发展带来前所未有的机遇。因此，打造“第二曲线”、奋楫数字经济“主航道”仍将是三大运营商的必然选择。

在发布财报的同时，三大运营商也披露了2023年投资方向。据悉，中国电信将把38.4%的资本开支投向产业互联网，较2022年29.3%的占比大幅增长；中国移动将加大对算力和能力的投资，减少对连接的投资；中国联通虽然没有公布具体投资方向，但是提出要进一步加强数字化转型，提升数字化赋能生产经营能力。

相信未来，随着投资力度的持续加大，运营商转型的步伐将更加稳健，“第二曲线”也将不断上扬、愈加清晰。 

表2 三大运营商云业务收入规模及增速

类别		2020年	2021年	2022年
天翼云	收入(亿元)	138	279	579
	增速		102%	108%
移动云	收入(亿元)	113	242	503
	增速		114%	108%
联通云	收入(亿元)	112	163	361
	增速		46%	121%

根深叶茂 广州“AI+算力” 深度赋能幸福民生

■ 本刊记者 孟月

近年来，数字经济的领跑作用不断显现，成为稳增长、促转型的重要引擎。作为数字经济时代的重要基础设施，人工智能将在“十四五”期间为我国产业转型升级和数字经济发展提供核心驱动力。

3月28—29日，通信世界全媒体记者“从叶到根”实地探访了广州人工智能优秀企业，聚焦智慧医疗、智慧农业、智慧城市、智慧制造等领域，见证羊城智慧化新成果，梳理广州“AI+算力”的发展脉络，探究算力如何深度赋能数字经济高质量发展。

“叶茂”：人工智能应用 百花齐放，赋能幸福民生

在政策的推动下，人工智能越来越多地与行业、场景深度融合。记者在参观广州极飞科技股份有限公司时，通过采访交流发现，科技可以让种田像“游戏”一样简单。“基于昇思MindSpore AI框架、结合昇腾AI硬件和华为云服务等，极飞科技在数字化农业管理的全面感知、智能决策和精准执行等方向发力，让种田像‘游戏’一样简单。通过神经网络模型训练，让多源遥感影像数据、气候数据的获取变得更加便捷、高效，并能适用于图像分类分割、作物分类和目标检测等多种不同的应用场景。”极飞科技工作人员介绍道。

在广州安必平医药科技股份有限公司，记者发现AI病理辅助诊断系统可

运用于病理诊断，极大地助推了智慧医疗的发展。在云从科技股份有限公司，记者与技术人员探讨人机协同操作系统如何助力城市数字化转型。在广州港南沙港区四期码头，记者发现广州知行机器人科技有限公司联合广州人工智能公共算力中心开发的“天空地一张图智能决策平台”，已成为无人码头的“眼、手、脑”，为码头的无人化和智能化提供了系统化感知与决策底座。

“根深”：算力深度赋能 让人工智能用得上、用得起、 用得好

经过十几年的发展，人工智能已步入大模型时代，而这背后离不开算力的推动作用。此次，记者也来到了广州人工智能公共算力中心，探看算力如何深度赋能人工智能。基于自主创新且全球领先的昇腾基础软硬件平台，广州人工智能公共算力中心对外提供99PB规模的AI算力服务，为广州市智能经济发展和产业数字化转型提供底层支撑，形成新一代信息基础设施核心能力。

“广州人工智能公共算力中心围绕人工智能产业五大要素——场景、数据、算力、算法、应用，构建人工智能创新应用服务体系，打造五大赋能平台——算力服务平台、应用创新孵化平台、产业融合赋能平台、科研合作平台、人才培养平台，通过多平台、多维度赋能并服务人工智能企事业单位，集聚企

业、人才、技术、政策、资本等产业生态资源，为整个产业构建扁平化的共生价值网，从而实现与人工智能生态伙伴的合作共赢。”广州人工智能公共算力中心主任梁添才表示。

基于“一中心五平台”的建设理念，广州人工智能公共算力中心与华为合作组建专业团队，开展国产化人工智能生态建设工作，服务广州以及粤港澳大湾区的人工智能产业，从源头上推进人工智能自主创新、原始创新，支持一批技术研发及成果转化项目。

“在广州人工智能公共算力中心的建设过程中，华为作为深度参与者，一是提供先进的全栈解决方案；二是利用我们的实践经验和专业技术能力，为人工智能公共算力中心提供运营支持。”华为广东产业发展与生态部总经理阎刚表示。

值得注意的是，广州人工智能公共算力中心于2022年6月8日正式建成，12月正式对外提供算力服务。仅3个月，该中心就初步对接150余家企业，其中“专精特新”企业占45%，赋能广州11条重点产业链，打造80多个解决方案，并为50多家企业和高校培育170多位人工智能领域人才。

人工智能产业链的高质量发展不止于当下，更关乎未来；不止于产业本身，更关乎千行百业和全社会的高质量发展。期待产业链上下游进一步精诚合作，齐心协力营造良好的产业生态，推动人工智能产业高质量发展。CWW

探寻智慧城市发展新路径 智慧“龙江”三步走

■ 本刊记者 孙天 文 / 摄影

“智慧城市”概念于2008年提出，随后在国际社会引起广泛关注，并引发了全球智慧城市的发展热潮。智慧城市发展大致经历了探索期、调整期、突破期、融合期。我国智慧城市在经历了约10年的发展后，逐渐走向精细治理、全面融合阶段。2022年由国家工业互联网发展联盟等联合发布的《依托智慧服务共创新型智慧城市——2022智慧城市白皮书》指出，“5G、人工智能、物联网等多种新技术的应用，带动城市数字基础能力的跃升，智慧城市建设获得全新的‘智慧支持能力’。新能力催生新要求，创新协同成为智慧城市发展的新要求。”

3月21—23日，通信世界全媒体记者先后走访了大庆、鸡西、哈尔滨，探寻黑龙江智慧城市发展新模式，解密黑龙江省内城市如何通过“数智”技术使老城焕发新生。

第一步：打造“数智”新名片，建设数字中心

60多年前勘探队在松辽盆地发现了新中国第一个大油田，该油田后被正式命名为“大庆油田”，在此后的发展大潮中，“大庆”因“石油城”这个名字

火遍了中国。

如今，随着信息技术的快速发展，信息资源也日益成为新的生产要素，各地区、城市都在积极开展数字化转型升级，为城市发展赋能，而大庆这座“石油城”也迎来了新的发展机遇。大庆联通助力政府打造的“数字大庆”中心，作为大庆智慧城市的“大脑”，目前已涵盖公共服务、城市管理、应急指挥、社会治安、道路交通、企业运行等多个领域。

据大庆联通的工作人员介绍，“数字大庆”智慧城市运营管理指挥中心涵盖了城市概览、城市治理、经济运行、民生服务、城市安全、生态农业、应急管理、旅游发展、智慧电力九大领域。

“数字大庆”项目的建设可以概括为“八个一”，即依托一朵云、建好一套库、整合一张图、打通一张网、集成一中台、汇聚一个“脑”、展示一组屏、管好一座城。其中，“一朵云”“一套库”“一张图”由核心算力

数据支撑，以“一张网”“一中台”为核心传输承接纽带，“一个‘脑’”“一组屏”是城市数字化治理的载体，最终实现“管好一座城”的目标。

指挥中心涵盖众多领域，通过感知设备获取了大量数据。那么如何将这些数据统一统筹利用，真正为管理者、老百姓提供便利？

大庆联通工作人员表示：“‘数字大庆’项目中的联动指挥模块，采用‘一盘棋’的信息化系统，提供全市应急通信网、业务应用体系、基础硬件设施和安全运维保障等服务内容，进一步筑牢了城市安全防线，更加适应‘全场景、大应急’的广义应急理念，也是东北首个、全国领先的地市级多级联动



中国联通数智大庆中心

应急指挥体系。”

在“12345政务服务中心”，大庆联通工作人员介绍说，自2016年起，大庆联通便承接了政务服务热线运营工作，目前已平稳有序运行了6年，搭建起政府与百姓沟通的桥梁。2022年“数字大庆”全面升级，系统重建，整体迁至“数字大庆”中心新址，全力保障了疫情期间百姓诉求的渠道畅通。

依靠政务服务中心，大庆联通工作人员发挥“铁人”精神，在新冠肺炎疫情期间，“12345政务服务中心”发挥了重要作用。据工作人员介绍，作为大庆300万市民与政府沟通的平台和桥梁，政务服务中心依托线上线下相结合的方式，7×24小时为广大市民提供服务。

大庆联通正在将“铁人精神”转化为“铁人智慧”，赋能大庆这座城市，“数智”城市也正在成为大庆的新名片。

第二步：推出便民、利民的智慧社区新样板

智慧社区是智慧城市的重要组成部分，是居民能够切实感受得到的。智慧社区的发展早在20世纪80年代就开始了，大致经历了智能化、数字化、智慧化、人文化几个发展阶段。近些年，国家通过各种政策支持智慧社区建设，国家发展改革委、科技部、住建部、公安部等发布相关政策规划，全力推进智慧社区建设。《黑龙江省国民经济和社会发展规划第十四个五年规划和二〇三五年远景目标纲要》中也明确指出，运用数字技术推动城市管理手段、管理模式、管理观念创新，精准高效满足群众需求。

2020年，鸡西联通认真执行省公司要求，在全市全面开展智慧社区推广工作。在推广过程中针对网格化管理、



鸡冠区智慧社区服务平台小程序

智慧社区标准化管理相关业务与鸡冠区政府进行了深入研讨，并多次深入社区现场考查，了解用户痛点，精心打造了鸡冠区智慧社区平台，并成为全省智慧社区新样板。

鸡冠区智慧社区服务平台具备诸多功能，包括文明城市献言、鸡冠区“12345”、网格化事件管理、民政救助、司法援助、供求信息、证明办理、志愿者招募、新冠疫苗登记、商铺推荐等……

记者了解到，鸡冠区智慧社区服务平台自上线以来，累计开通7个街道、2个乡所属的32个社区、14个村、800余个网格，网格员共计660名，累计录入实有人口37万余人、建筑3000余栋、实有住宅21万套，企业商户4千余个，数据覆盖占比达到96%以上，实现数据“一次采集，多方共享”，确保社区数据的动态更新和精准管理。

在智慧社区内，居民微信注册用户数207824，实名认证人数184629，绑定住宅人数127043，系统自上线以来已经受理事件共4830件，彻底解决老百姓上报难、基层治理人员权责不清晰、监管难度大等问题，百姓满意度逐月攀升。

特别是在疫情防控期间，实时统计

居民的健康、居家隔离、疫苗接种、核酸检测等情况，提供了数字化支持，社区人员通过APP采集的数据能够随时办公，有效提高社区在疫情防控中的工作效率，平台月均采集数据1700万次。同时，依据“人防关联”的基础数据，基于居家隔离功能，实现对中高风险地区返回人员、密切接触者隔离人员的居家隔离管理，为社区工作者的有效管理提供数字化支撑75442次。

鸡冠区智慧社区服务平台为社区管理带来了极大帮助，也为老百姓提供了高效率的办事途径，已经成为了便民、利民的新样板。

第三步：数据赋能，实现城市现代化治理

随着物联网、云计算等新技术的出现，我国智慧城市加速发展，如何利用新技术赋能现代化城市的治理？中国联通（黑龙江）产业互联网有限公司（以下简称联通黑龙江产互公司）给出了答案。

联通黑龙江产互公司研发并大力推广智慧社区产品，公司党委书记、总经理王全新表示：“社区是社会的基本单元，是连接城市、小区、家庭的重要桥梁。从老百姓的衣食住行，到政府的公共服务、社会治理，无不与社区的管理服务能力紧密相关。根据集团公司和黑龙江省公司统一部署，联通黑龙江产互公司基于集团统一研发平台，有根生长，依托自身强大的研发能力，结合社会各级需求，倾力打造了智慧社区产品。公司在智慧城市领域深耕多年，具有丰富的项目经验、成熟解决方案和实施能力。通过多年的经验积累，意识到新型智慧城市是‘长’出来的，而不是一次性‘建’出来的，需要长期的治理和运营。”

传统的政务服务存在一些问题，



七台河市域社会治理

如政务服务、城市治理等数据更新频次低、汇总难；各部门之间的数据对接、整合缓慢等。随着技术和城市的进一步融合，联通黑龙江产互公司基于社区政务的痛点打造了智慧社区服务平台。

谈及数据要素充分流通对城市综合治理能力的提升有多大帮助，联通黑龙江产互公司数字化业务部总经理

仲光锐对记者说道：“数据要素向基层下沉是现在城市数字化转型发展的趋势，相对于自然资源、地理区位等传统要素，数据要素更易跨时空流通，在这样的背景下，智慧社区平台的建设

能够更顺利地进行，基层获取和利用数据要素的渠道更加多样、方式更加便捷，有利于更加充分地发挥数据和信息等生产要素在基层治理体系中的作用。”

联通黑龙江产互公司所打造的智慧社区平台是将“天、地、人、事、物、情、组织、家庭、时间”九大要素全部数字化，并落入单元网格，以网格化管理

模式、根系化巡查模式、脉络化信息传导模式，将各职能部门力量“拧成一股绳”，互联互通、协同管理、高效处置，推动“多网融合、一网统筹”，可融合城管、交通、教育、政法、医疗多个领域，形成“上面千条线、下面一张网”，不断提升社会治理水平，提高人民群众幸福指数。

王全新总经理表示：“放眼未来，联通黑龙江产互公司将坚持以人为本，积极运用智慧社区运营理念，深入探索智慧社区新工作模式，为提高人民幸福感、不断实现人民对美好生活的向往贡献‘联通智慧’。”

党的二十大报告提出，要“加强城市基础设施建设，打造宜居、韧性、智慧城市”。联通黑龙江产互公司正是从居民的需求出发，将“居民-城市-管理者”以数据连接起来，为城市的现代化管理赋能，打造更加智慧的城市。📶





全球2G/3G网络关闭潮加速到来

■ 云晴

2022年底，全球移动供应商协会（GSA）称：在其调查的68个国家和地区中，已经有135张2G/3G网络被关闭，因为运营商希望将频谱资源用于建设4G/5G网络。2G/3G网络关闭已经成为全球运营商面临的重要课题之一。

关闭2G/3G网络成必然趋势

2G/3G网络占据着优质的无线电频谱资源，但频谱利用效率却远低于4G/5G网络。在速率、容量、安全等方面，2G/3G网络已经难以满足数字化转型中许多场景的要求。此外，伴随着网络升级换代，网络规模不断减小，维护升级成本持续增加，运营商通过规模获利的模式也面临威胁。而多张网络并存导致运维成本居高不下、频谱资源受

限、站点资源不足等,也是运营商亟需解决的问题。因此,在数字化转型需求日益增长、5G网络逐渐成熟的背景下,全球运营商对于关闭2G/3G网络具有强烈意愿。

尽管关闭2G/3G网络能够带来节省多网运营成本、腾出宝贵频谱资源、升级应用能力等好处，然而运营商对于关闭网络依然非常谨慎。其中，确保物联网应用的平滑过渡是重要考虑因素。物联网应用的不断发展形成了巨大的连接规模，其中有不少是基于2G/3G网络。而且越是基于2G/3G网络的应用，其业务敏感度和重要程度就越高——毕竟早期选择用无线方式实现连接的业务大概率是重点业务。在NB-IoT和LTE Cat.1规模化发展之前，物联网终

端的无线接入承载主要依靠2G/3G网络, 其中2G网络又是重中之重, 这些网络连接在短时间内难以全部向NB-IoT、LTE Cat.1迁移。

从技术角度来看，2G/3G网络的替代产品是非常成熟的。GSMA数据显示，截至2020年9月，全球NB-IoT、LTE Cat.1网络达到112张，规模效应已经非常明显。在面向低速场景的NB-IoT方面，运营商连接规模不断扩大；在面向中低速应用场景的LTE Cat.1方面，模组成本也在快速下降。NB-IoT和LTE Cat.1的成熟将能够满足大部分物联网的连接需求。此外，关闭2G/3G网络可以降低能耗，节省运营维护费用，有助于实现绿色低碳。在安全方面，关停可以解决2G/3G基站认证机制不

完备的问题，杜绝黑客窃听和利用伪基站实施诈骗等犯罪行为，消除部分危害用户信息安全和公共治安的隐患。

存在业务中断、成本分摊不合理等挑战

然而，网络关闭并非仅是成本和技术层面的问题。如上所述，与针对个人市场的普通业务不同，物联网广泛应用于行业用户市场，特别是一些关键的流程。如果在网络关闭之前没有充分梳理，就有可能出现严重的后果。

例如，美国国家公共安全电信委员会、安防产业通信委员会等就向FCC发出申请，要求延迟2G/3G网络关停。其理由包括：网络关闭可能影响到安装在美国家庭和企业中的数百万个报警器；用于追踪一些特殊人群或物品的连接设备，在未完成替换的情况下中断服务，可能引发公共安全事件。

在医疗设备、公共安全、特定人群追踪等领域的行业用户看来，网络关闭的业务梳理、替代工作是先决条件，能否平滑地实现“业务迁移转网”是关停2G/3G网络的关键因素。为此，美国主流运营商进行了相应的资源准备，并与FCC进行了沟通，主要是预估网络关停可能涉及的用户规模及相关应用。AT&T在2022年提交给FCC的报告中预测，大约有270万用户将受到3G网络关闭的影响。

在此过程中，如何消除物联网行业用户对替换可能带来业务中断风险的担忧，以提升其替换意愿尤为重要。如果能够为行业用户梳理出更有价值的使用场景，用户或许才愿意配合开展业务迁移工作。

例如，英国频谱政策指导委员会曾预测英国的2G网络至少要维持服务到21世纪30年代，因为除了少量to C用户之外，智能电表和欧盟主导的救援系统

都依赖2G网络支撑。而在预先设定的服役时间结束之前，用户并没有强烈的意愿或是相应的成本预算来实施迁移替换工作。在这种情况下，运营商需要投入力量做好业务梳理和迁移准备工作。

另外，在网络关闭过程中如何分摊成本也是个问题。因为网络迁移并非完全由用户侧业务驱动，用户的支付意愿取决于业务价值；而从运营商角度看，关闭网络涉及大量的历史资产问题，包括现有通信模组、生产类设备升级等费用，如果最终受益用户不承担任何成本，似乎也不太说得过去。因此，在行业用户市场，如何引导用户发掘相关业务价值、找好投资方、建立合理的回报模式，也是需要解决的难题。在此过程中，发挥好市场之“手”的作用，而非采取行政强制手段迫使用户退网是非常重要的。运营商以更优质服务、更低廉价格，辅以产业发展趋势的宣传，并处理好用户关系、引导用户停止旧服务，或许能够借此发现更多商机。

2G/3G网络关停热潮已至

从实际情况看，不同运营商所面临的外部环境千差万别，并没有统一的网络关闭计划。运营商会根据本地需求、自身目标及能力情况制订关闭时间表，并且将依据实践情况动态调整时间表。

但总体而言，2022年是关闭2G/3G网络的重要一年。如上所述，截至2022年底，全球已有135张2G/3G网络被关闭。此后，2G/3G网络关闭的比例将继续增加，尤其是3G网络关闭速度将超过2G网络。2G/3G网络关闭潮将在2025年达到高峰。

从区域来看，欧洲地区的2G/3G网络关闭数量最多，占据关闭总量的63%；亚洲地区占比为21%；北美地区、中东及非洲地区、大洋洲地区则分别占

比为5%左右。

具体到国家来看，欧洲各国出现分化，2G/3G网络关闭时间从2021年到2025年不等。例如。英国3家主流运营商3 UK (Three UK)、EE (Everything Everywhere) 和 Vodafone 将关闭时间确定在2023—2024年。德国已经关闭了3G网络，但到2025年底才会关闭2G网络；法国的2G网络甚至计划要使用到2028年底。德国Vodafone在2021年6月就彻底关闭了3G网络，并将之前用于3G网络的2.1GHz频段上20MHz的带宽全部重新分配给LTE网络。从Vodafone的角度看，一方面3G流量占总流量的比例已经低至不足2%；另一方面，3G网络耗电量是4G的7倍左右，非常不经济。因此Vodafone的3G网络关闭推进得非常迅速。而T-Mobile和O2两个主流运营商，也在2021年7月关闭了3G网络。

美国主流移动运营商Verizon、AT&T和T-Mobile将3G网络关闭时间确定在2022年。AT&T在2022年2月宣布关闭3G网络；T-Mobile分两步完成了关停动作，先是在2022年3月关闭原Sprint的CDMA网络（T-Mobile于2020年收购Sprint），然后于同年7月关闭了自己的3G UMTS网络；最后一个完成的是Verizon，它在2022年底关闭了3G网络。

从各国关闭2G/3G网络的经验来看，除了针对个人用户做好宣传沟通之外，工作重点需要集中在物联网业务替代、迁移等问题上。在此方面，运营商做好网络整体演进规划、论证好应用平滑过渡方案非常重要。在具体实施过程中，按需新增NB-IoT基站、推动产业链成熟、关注网络能力和垂直行业能力深度融合、形成与用户协调的行动节奏，是未来2G/3G网络关闭能够顺利推进的关键。📶

城市管网基础设施 智慧化问题研究

■ 中国信息通信研究院 王晨 王文跃
国家石油天然气管网集团有限公司 于浩
博鼎实华(北京)技术有限公司 葛妍 柯桢

城市管网基础设施被喻为城市的“神经”和“血管”，是保障城市运行的“生命线”，是消除“马路拉链”“空中蜘蛛网”、提高城市承载力的有效形式。在国家高度重视“新型智慧城市”“新型基础设施”建设的大背景下，推进城市管网基础设施智慧化已势在必行；但在此过程中依然面临多重困难，亟需从智慧化的标准、技术瓶颈与智慧城市统筹建设等方面发力解决。

我国城市管网基础设施发展历程

城市管网是分布于城市地上、地下的通信管道、给排水管道、燃气管道、热力管道等基础设施的总称，支撑着城市居民日常生活的正常运转。

我国城市管网基础设施建设始于1958年的北京天安门广场地下管廊，历经了概念探讨阶段、争议阶段、快速发展阶段、赶超和创新阶段。2018年以来，我国相关政策要求各城市根据实际情况编制合理规划，制订切实可行的建设计划，有序推进城市管网基础设施建设。

在当前国家提振经济、去产能加快供给侧改革的政策推动下，我国城市管网基础设施建设逐步进入有序发展阶段，且呈现智慧化发展态势，从建设规模和建设水平来看，我国已成为城市管网建设的“超级大国”。

传统城市管网基础设施管理模式存在的问题

随着智慧城市建设的不断深化，我国城市管网基础设施规模越来越庞大。管网基础设施由于空间断面设计复杂、纳入管线种类多，建设过程中具有施工组织复杂、工程量大、项目工程管理难度大等特点，在工程进度、成本、安全、质量等精细化管理方面均存在困难，传统管理模式已无法满足综合管廊快速发展的需求，诸多问题已经显现出来。

首先，传统的运维模式导致管理水平落后，运营成本高、应急响应速度慢、责任不清等问题频频发生。其次，数据不统一，形成“信息孤岛”。由于参与单位多、数据种类多，众多子系统形成数据分割，使数据无法整合利用。最后，运维管理智能化水平低下、巡检手段落后、工作效率低下、应急处置能力薄弱、

监控维护漏洞百出，导致管廊运营成本居高不下、管廊管线安全无法保障、事故发生概率增加。

为解决上述问题，我国自2000年起大规模开展城市管网信息化建设，北京、上海、广州、厦门、杭州、南京等城市虽已建立城市管网信息化系统，但大多是在各行业内部分散建立专业管理系统，缺乏统一规划与协调，各系统间信息不能交换与共享。同时，城市管网资源信息数据缺乏规范标准，信息数据动态更新程度低。通过总结我国城市管网资源智能化建设实践经验可以看出，城市管网资源数据应用依然是对单一、局部数据的利用，智能化平台设施对时空数据融合挖掘不够，只是通过集成初步实现了城市管网资源管理监控的智能化，远未达到智慧化的程度，与利用静态数据、动态数据实现智能应用服务尚存在较大差距。



城市管网基础设施智慧化建设的效益分析

当前,发达国家已开始将城市管网智慧化建设升级为一项重要的新型基础设施建设加以推进。不同规模、不同用途的城市管网智慧化管理系统、平台及设备进入了商品化生产和专业化应用阶段,智慧化管网基础设施的运营投入具有显著的社会和经济效益。

一是可提高管网运行监管的能力,切实保障管廊长期安全运行。一方面,通过管廊智能化建设,组建管廊监控物联网系统,可实现管廊实时在线监管,形成人与物、物与物相连,实现信息化、智能化和远程管理控制。另一方面,将智能监管与人工巡查相结合,可切实提高管廊安全运行管理能力,有效保障管廊运行安全和廊内管线运行安全,第一时间提供危险预警并及时处置事故,有力保障城市安全运行和人民群众生命财产安全。

二是可转变管理模式,突破传统管理局限,提升管理工作水平。一方面,通过与业务系统融合,实现对地下管线工程档案的接收、整理、鉴定、统计、保管和利用,提高政府工作效率。另一方面,应用创新设计、创新建设和创新运营,打造城市综合管廊运营服务平台,逐步健全城市综合管廊运营管理体系,为电力、燃气、热力、通信、广播电视等行业提供优质、稳定的服务,从而提高城市综合管廊建设水平,形成智能、先进的城市综合管廊运营服务能力。此外,可优化管廊运行方式,降低运行维护费用,提高经济效益。还可优化管廊运行管理方式,用信息化、智能化管理方法代替传统的人工管理方式,将有效提高管理效率、节约管理资源,在保障管廊安全运行的同时,实现高效运营,避免资源浪费,减少运营管理费用。

三是可形成合作互惠机制,加强管

线入廊管理,发挥管廊作用。一方面,通过城市管廊创新运营,可助力传统建设企业转型为“城市综合管廊运营服务商”,并为地方政府财政带来持续性运营收入,形成政府和企业的多方共赢。另一方面,通过建立政府与企业间的合作互惠机制,实现管廊内部数据信息共享、信息化建设成果共享,促进地方管线入廊等工作,使城市综合管廊切实发挥作用。

推动城市管网基础设施智慧化建设的策略与建议

当前,我国城市管网基础设施智慧化建设推进工作依然存在薄弱环节,具体表现在以下4个方面。

一是现有智慧化解决方案存在局限性。我国主流城市管网基础设施智慧化管理解决方案存在着管线空间信息不准确、管线运行状态监测手段匮乏、管网事故预警手段不足、管网数据兼容性差等突出问题,且目前研发工作热点主要集中于数字化层面,以期实现管廊信息数字化表达和管理,依然属于智慧化最基本的层次,未来需要融入物联网、云计算等先进的技术手段,突破技术瓶颈,进行集成化、智慧化层面提升,实现综合管廊的全面感知、智能监测、灾害预警、仿真模拟等智慧化管理。

二是缺乏智慧化建设的技术标准体系。目前,我国城市管网基础设施智能化工程建设解决方案主要体现在现代信息技术的集成上,但是解决方案实现智慧化的程度存在差异,大部分解决方案侧重于综合管网全生命周期管理以及系统的自动感知与监控,目前尚未形成城市管网基础设施智慧化的技术标准体系。

三是尚未形成健康可持续发展的产业生态。城市管网基础设施智能化建设跨多个领域,涉及多专业、多技

术,而目前的解决方案大多专注于某个环节,国内尚无企事业单位具备单独提供城市管网智能化建设完整解决方案的能力,且产业链相关企事业单位合作的案例极少。

四是智慧化运维还未得到重视。目前我国城市管网基础设施智慧化运维在一站式运维服务、全生命周期管理、快速精准的运维支撑等方面尚处于初级阶段,运营模式、建设模式仍在探索期,与智慧城市其他系统间互联互通的实践经验有待积累。

通过分析我国城市管网基础设施建设现状和传统管理模式存在的短板,结合推动城市管网基础设施智慧化建设面临的问题,建议从3个方面发力突破。

一是解决智慧化建设的标准问题。城市管网基础设施从信息化向智能化演进,并最终实现智慧化,是技术发展与社会进步的必然,但需要国标、行标、团标、地标相互配合的标准体系支撑实现,以标准形式明确智慧化需要达到何种程度、包括哪些内容等。

二是解决智慧化实现的技术瓶颈。一方面,需要针对管理需求,研究实现的技术与方法,提供实用、科学、可靠的管理运维工具,同时要注重地上地下一体化,兼顾软硬件的有机结合,在梳理管理运维流程基础上,研究如何“让数据说话”,实现动态服务。另一方面,引导形成以政府为主导、以需求为导向、“政产学研用”共建共享产业生态。

三是解决与智慧城市相互统筹的问题。作为重要基础设施,城市管网信息是智慧城市时空信息的重要组成,是城市空间信息管理的内容,在城市规划和建设过程中,应提前统筹数据互联互通、信息系统对接等工作。



小基站 能否登上大舞台？

■ Omdia 资深首席分析师 杨光

随着在线教育、远程医疗、远程办公等应用快速发展，5G室内应用场景增多。在5G覆盖行业更广、应用走深向实的当下，能够弥补宏基站技术上不足的小基站悄然兴起。具备小体积、低成本、高性能、低功耗、易部署等特性的5G小基站成为业内公认的网络基础设施建设重点之一。

小基站的春天？

在今年世界移动通信大会（MWC2023）召开前不久，沃达丰（Vodafone）发布了基于树莓派平台和Lime Microsystems软件定义无线电（SDR）板卡的小基站原型机，其外壳由3D打印制造，外形尺寸与普通家用路由器相当。沃达丰希望能够利用这样一款以Open RAN标准打造的低成本

小基站原型产品，为产业界树立样板，促进创新型小基站产品的开发，满足企业用户对移动专网服务的需求，尤其是帮助运营商开辟面向欧洲2200万家中小企业的5G专网市场。2023年世界移动通信大会期间，这一产品受到了参展观众的极大关注，充分显示出市场对低成本、创新型小基站产品的强烈需求。

无独有偶，在2023年世界移动通信大会前几周，中国电信北京研究院也宣布，成功研发出5G扩展型小基站pRRU产品。该产品将主要部署于室内场景，用于解决小型封闭空间的无线覆盖问题。难能可贵的是，此款5G小基站产品的射频收发和数字前端等芯片均来自中国厂商，成功实现了产品整机国产化芯片器件的集成应用，做到了芯片和器件的100%国产化。中国移动研究院和设计院也在2022年完成了基于国

产飞腾CPU的5G云小站研发，并成功中标中国移动集团2022—2023年扩展型皮站集采。

重量级运营商对小基站研发的大力投入，令产业界再次泛起对“小基站春天”的期待，但回顾小基站发展的历史，产业界又不免心生疑虑。确实，自3G时代出现飞蜂窝（Femtocell）产品之后，每当宏网络覆盖达到相当程度，小基站都会成为产业界的热点话题，担负起以较低成本帮助运营商完善网络覆盖的重任。然而，在过去的3G和4G时代，广为期待的“小基站春天”并未真正来临，这样的情况能否在5G时代被改写呢？

5G时代的新需求

完善室内环境的网络覆盖一直是

电信运营商的一项重点工作。移动互联网时代,约70%~80%的数据流量产生于室内环境,移动网络在室内环境的服务质量将显著影响用户的使用体验。小基站是运营商完善室内网络覆盖的一个重要工具,但同时也面临着来自不同方向的竞争。无论是Wi-Fi无线局域网还是已经发展多年的分布式天线系统(DAS),在某些情况下都更具成本优势,且也能提供较好的业务体验。成本与收益的综合考虑使小基站在3G、4G时代陷入“叫好不叫座”的尴尬局面。

而这一局面在5G时代似乎正在改变。一方面,5G系统工作频率更高,穿透损耗的影响更为明显。中国移动的测试结果显示,在其部署于2.6 GHz频段的5G网络中,室内用户平均下载速率仅为室外用户平均下载速率的1/4~1/3,而上行速率的差距更可能高达百倍量级。对于主流的部署于3.5 GHz频段的5G网络来说,这一差异可能更为显著。同时,3.5 GHz频段往往超出了既有DAS系统的工作频率范围,使运营商无法重用既有DAS系统。这些都提升了市场对5G小基站的需求量。

5G行业应用的发展更是为小基站打开了新的应用空间。大多数行业(例如制造、医疗、仓储乃至矿山)的应用场景处于“室内”环境之中,而且对网络服务质量有较高要求,现有Wi-Fi系统不能完全满足这样的市场需求。正如中国移动研究院无线与终端技术研究所副所长李男在行业研讨会上所指出的,“小基站也是行业网市场端到端解决方案的关键入口,工厂、矿山、医院等行业用户对5G小基站灵活组网的需求十分强烈。整个to B市场空间可能达百万级BBU、千万级RRU量级,行业网产品利润预计高于公网。”

正因如此,小基站在5G时代可能迎来全新的发展机遇。为抓住这些机

遇,产业界还需要付出持续的努力。

何谓“小”基站?

根据行业传统观念,小基站的“小”主要体现于较小的发射功率和覆盖范围。然而随着市场需求的发展,业界有必要从更多元的角度看待小基站的定义。

在大多数行业专网的部署场景,行业用户不但需要5G网络提供有保证的服务质量,还需要整个解决方案具有较“小”的成本压力。这也正是沃达丰推出基于树莓派平台和Open RAN架构的小基站原型机的原因。相比基于专用硬件的传统小基站产品,这种基于商用低成本通用硬件平台的小基站有望显著降低设备成本。更重要的是,软硬件解耦的系统架构和商用通用硬件平台可以降低通信设备的开发门槛,从而促进更多厂商进入市场,提高市场竞争水平,刺激技术和商业模式创新。

中国移动研究院研发的5G云小站参考设计以及相关的产业化推广,也已证明此类开放性架构确实有利于产业生态的多元化发展。在中国移动2022年的5G扩展型小站集采中,不仅有京信、中信科移动等传统厂商入围,还有赛特斯、联想等非传统基站厂商中标,为市场注入了新鲜活力。这必将提升小基站市场的商业竞争和技术创新水平,促进5G行业专网的部署推广。

但是,也需要辩证看待小基站的参数配置。行业应用虽然多发生于室内环境,但仍可能面临较为复杂的无线电传播场景,比如重工业生产车间或井下巷道,往往有较多的厚重遮挡物,需要基站既具有较大的发射功率以保证完善的网络覆盖,又无需很大的系统容量,这样就产生了一个介于传统小基站与宏基站之间的细分市场空间。在某些偏远地区的广域覆盖场景也存在类似情

况,虽然需要基站具有较大发射功率但对容量的需求却较低。在这些情况下,小基站的“小”就更多体现于较小的容量配置而非较小的发射功率。对此,高通公司近期发布的紧凑型毫米波“宏”基站平台就瞄准“大功率而小容量”的细分市场,其思路值得产业界借鉴。

小基站成为算力网络的有机组成部分

无论是在消费市场还是行业应用市场,小基站均部署于贴近用户生产生活之处。作为真正的网络边缘节点,小基站可为电信运营商的创新型业务提供有力支持。尤其在算网融合的背景之下,无论是利用云化小基站中通用处理器的计算能力,还是在传统型小基站上增加相应的计算资源,都可使小基站成为贴近用户的算网融合平台,成为服务行业数字化转型的新型基础设施。

同时,由于小基站贴近用户部署、站间距远小于宏基站,其在对用户的定位、感知等方面较宏基站具有天然优势。尤其在室内环境,宏基站往往无法获得导航卫星信号。如果室内蜂窝系统能够集成精准的感知定位能力,必然可以为行业数字化应用提供更好的服务。目前,3GPP已为5G系统定义了室内精准定位能力,通信与感知融合的讨论也在进行之中,并有望成为5G-Advanced系统的重要组成部分。在获得这样的感知定位能力加持之后,小基站应能在算网融合体系中扮演更为重要的角色。

综上所述,业界有理由期待,5G时代的市场演进,尤其是行业数字化应用发展,将促使小基站登上更大的“舞台”,迎来真正的发展“春天”。当然,为了达到这一目标,产业界上下游仍需携手努力,共同打造更加开放、更加多元的小基站产业生态。CW

中国移动李男：5G小基站规模化发展 夯实新一代边缘算力底座

■ 本刊记者 舒文琼（整理）

随着5G步入高质量发展的新阶段，小基站也迎来了广阔发展空间。5G小基站可以完善和补充大网覆盖，提供连续一致的5G体验，并为垂直行业提供个性化的服务能力。2022年三大运营商启动了5G小基站集采，标志着5G小基站正式登场。

为探讨小基站如何助力千行百业数字化转型、赋能5G高质量发展，近日通信世界全媒体记者采访了中国移动研究院无线与终端技术研究所副所长李男。

5G小基站需求将持续增长

《通信世界》：目前5G小基站商用已经正式开启。展望未来，您认为5G小基站发展态势如何，应用重点何在？

李男：随着近年来5G网络的加速建设，截至2月末，我国5G基站总数达238.4万，5G用户数达5.9亿，已完成城区、绝大部分县城及部分乡镇的5G网络覆盖。随着5G网络基础覆盖的逐步完成，运营商后续将聚焦细分场景网络建设。5G的频谱资源频段普遍偏高，从室外穿透室内的能力较弱，同时考虑到数据业务80%的流量发生在室内，特别是未来随着AR/VR、云游戏、高清视频等对传输和时延要求极高的业务不断发展，未来几年室内覆盖将成为5G网络建设的重要方向。

与传统室分相比，5G小基站在吞



中国移动研究院无线与终端技术研究所副所长 李男

吐量、服务用户数和频段选择灵活性上优势明显，可提供更佳的小区覆盖性能和更好的用户体验。除为公网覆盖提供重要补充外，5G小基站还具有支持云化、智能化及与边缘计算等技术结合的能力，可为工业互联网等垂直行业提供整体解决方案，在行业5G专网建设中将扮演重要角色。随着后续室内网络建设的不断深入和行业市场的快速发展，5G小基站的需求也将持续增长。未来3年，5G小基站市场有望迎来规模增长。

为垂直行业提供低成本、一体化服务

《通信世界》：垂直行业用户对于5G专网需求呈现何种特点，中国移动在5G专网方面进展如何，在5G小基站融入垂直行业方面有何尝试？

李男：中国移动非常重视5G专网发展，大力推动5G专网实现全面产品化。截至2022年底，中国移动累计签约5G行业商用案例超1.8万个，全年带动DICT项目签约金额达365亿元，5G专网收入达25.5亿元，同比增长107.4%。基于大量专网建设实践工作，中国移动整理归纳了垂直行业用户对5G专网的几个主要需求。

能力定制：千行百业对5G网络的需求多、差异大，从网络容量、连接可靠性到业务时延、增值服务扩展等，定制化要求几乎“一行业一网络”，甚至“一项目一网络”，要求网络能力极致且可灵活定制。

成本可控：行业用户的信息化改造项目预算普遍有限，用户对价格敏感，高度关注方案性价比，低成本建设方案成为开拓5G专网市场的关键因素。

部署敏捷：网络建设需匹配用户生产节奏，专网系统的打包交付、快速配置、简易维护已成为行业用户的基础需求。

使用简便：用户要求专网产品互联网化、销售全流程线上化、业务开通敏捷化、使用简便化。

基于通用硬件平台研发的5G小基站产品，可依托云原生架构及软件定义技术，将5G网络接入、能力开放、无线AI及行业应用保障等多种服务能力有机结合，根据项目需求统一部署于行业

用户的通用服务器平台,提供低成本的云、网、算、智、业一体化服务。

中国移动2022年在安徽马鞍山华孚工厂部署了基于无线智能控制器(RIC)的5G小基站网业协同智能化方案,可有效提升视频监控、AGV控制等业务的时延、吞吐量、抖动等关键性能指标的保障能力,满足行业用户的SLA需求。除了工业互联网场景,5G小基站在煤矿、野外勘测和城市物联网等业务场景中也有着广泛的应用需求。

依托小基站打造新一代边缘算力底座

《通信世界》:边缘计算是5G领域非常重要的一项技术,算力是运营商的重要发力点,当边缘计算、算力与小基站结合,将迸发出怎样的火花?

李男:随着数字化转型的深入,业务上云呈现多样性爆发式增长。云服务除对计算能力提出较高要求外,在服务时延、数据安全性、服务连接可靠性等方面也有较高要求,集中建设大型IDC已无法完全满足未来云服务的需求。如果说“东数西算”是算力网络的“中枢神经”,建设具有连接与服务能力的边缘云节点就是算力网络的重要“神经末梢”,解决算力网络“最后一公里”的确定性服务能力问题,也是算力网络服务更多经济实体、走进千行百业的关键。

边缘计算、算力网络与5G小基站深度融合打造的无线算力网络,是以无线算力和无线通信能力为基础,涵盖云计算、人工智能、大数据、泛在感知等新一代信息技术领域,面向业务最优体验实施无线算力、无线通信及多样化业务的协同调度,实现业务质量保障、算力与通信的最优匹配,是算力网络在无线接入层面的具象化体现。无线算力网络将推动无线通信基础设施底层设计发生革命性变革,打造面向

5G-Advanced和6G多业务、多量纲、高效能的边缘算力承载底座。

无线算力网络将催生以云、网、算、智、业一体交付、一体服务为需求特征的无线边缘云服务细分市场新机遇。在中小微专网应用场景,传统的网络、云平台、行业系统独立采购,现场定制集成,各系统独立运营。这种模式成本高、运维复杂,市场推广难度大,而基于5G小基站的无线算力网络有望依托通用平台的成本优势、云化架构的灵活定制、应用快速上线、全业务一站式敏捷交付、IT化统一智能运维等能力,改变中小微专网的生产模式,激发无线边缘云服务市场活力。

中国移动研究院在集团算力网络顶层设计下,积极推进无线接入网向算力化方向演进,在中国通信标准化协会主导无线算力网络标准立项,提出无线算力网络架构设计方案,开发面向行业用户、本地多云编排能力组件和无线智能化应用,并将于年内在自研云化5G小基站中集成交付。通过底层核心技术创新,中国移动实现5G无线通信业务与企业云服务基于通用服务平台的一体化部署和一体化算力编排,助力行业合作伙伴基础设施统一投资、统一管理、统一维护,降低行业用户5G连接及信息化升级的基础投资和运维成本,大幅提升垂直行业的基础设施利用效能,打造新一代的边缘算力底座。

推动5G小基站的规模落地和可持续发展

《通信世界》:对于保障小基站的规模化落地性能和小基站产业的可持续发展,您有何建议?

李男:5G小基站是一款新的无线设备站型。为了保障小基站规模化落地性能,一方面,小基站厂商需要构建规模化生产和交付能力,以及覆盖全国的

敏捷运维体系,建立与运营商省、市公司之间的业务深度连接及信任关系,形成“研产交维用”的生态闭环,不断迭代优化小基站的性能和成本;另一方面,运营商省、市公司需要尽快熟悉5G小基站的能力特点,找准5G小基站的适配部署场景,积累小基站与宏基站之间多场景互操作配置和网络协同优化经验,保障5G小基站的规模化落地性能。

现阶段促进小基站产业的可持续发展,核心是全力保障已采购的5G小基站落地并推进持续性采购,让新站型引入带来的成本、性能等方面改善效果得以显现和持续,得到方方面面客户的认同,也让小基站厂商多年的研发投入获得合理回报,使其能够生存下去并保持迭代研发的能力。在此基础上,产业需要持续挖掘小基站在大网和细分行业的部署场景,进一步拓展小基站的服务能力,例如,提高支持的天线数/小区数、提升智能化业务保障能力、增强业务集成能力,甚至防爆、防辐射等特殊行业应用能力等,同时进一步拓展小基站的种类,满足千行百业的定制需求。

《通信世界》:据报道,中国移动2022年完成了“扩皮”小基站招标,请问具体进展如何?2023年在小基站建设和行业市场拓展方面有何规划?

李男:2022年5G小基站招标后,在集团公司的统一规划和全程指导下,中国移动各省公司正与中标厂商合作,积极开展5G小基站的试商用部署,中国移动研究院也在全力支撑,解决新站型在落地部署中出现的技术问题。待试商用结束后,5G小基站将进入全面铺开阶段。2023年中国移动将全力保障小基站的规模落地并积极推进行业市场拓展,适时开展新站型的产业化验证,不断创造价值点,增强产业信心,推动小基站产业可持续发展。CW

中国联通李福昌：不仅拓展覆盖 5G小基站将创造更多价值

■ 本刊记者 舒文琼

随着5G宏基站规模的不断扩大，5G小基站开始登上5G建设的大舞台。2022年，三大运营商陆续开启了5G小基站的常态化测试和集采，标志着5G小基站已经正式具备商用条件。进入2023年，5G小基站建设继续紧锣密鼓地推进。

“预计未来几年小基站将迎来集中部署阶段，随着经济社会数字化转型持续深入、5G渗透到生活的方方面面，小基站将迎来更大的发展机遇。”中国联通研究院无线技术研究中心总监李福昌在接受通信世界全媒体记者采访时表示。

迎来“5G+数字化应用”的广阔“蓝海”

截至2月底，我国已经建成238.4万个5G基站，基本实现了乡镇及以上地区的连续覆盖。随着5G网络规模的扩大，5G室外网络建设告一段落，进一步拓展广度覆盖、增强深度覆盖成为下一阶段的重点。在加强室内网络覆盖方面，与宏基站互补的小基站将大显身手，释放巨大潜力。

“室内场景环境复杂，业务量分布不均衡，导致覆盖需求多样化。5G小基站具有造价低、建设方式灵活等特点，可作为室内中低价值、小微区域覆盖的有益补充，在精品网络建设中发挥重要作用。”李福昌认为。

不仅室内覆盖，在“5G+数字化



中国联通研究院无线技术研究中心总监 李福昌

应用”方面，小基站也将迎来广阔“蓝海”。李福昌表示，经济社会数字化转型升级，推动5G网络向各行各业渗透，产业用户已经成为5G需求新的增长点。而5G小基站具有定制化、灵活性高等特点，易于与垂直行业深度融合，能够满足中小型行业应用的碎片化需求。

此外，基于云化技术，小基站、MEC可全部部署在通用服务器上，形成“云算网业”一体化设备，还可融合云计算、大数据、AI等技术，形成MEC能力开放、数据可本地卸载的弹性、敏捷、安全、高效的定制化多维能力融合网络，为垂直行业提供端到端个性化解决方案。

在拓展垂直行业的过程中，小基站将获得连接之外的价值增益。李福昌分析，丰富的应用场景对通信服务提出了数据本地化、场景小型化、业务融合化等要求，也希望网络具备差异化和定制化等特征。小基站具备良好的本地卸载能力，可轻松叠加本地轻量核心网，满

足小型园区、楼宇等场景的灵活部署需求，支撑传统toC业务、新兴视频类业务、数据采集业务、实时控制业务、高精度定位业务、感知类业务等。

商用部署和国产化双管齐下

在规模部署5G宏基站的同时，中国联通也在积极推进5G小基站的建设。

李福昌介绍，中国联通着力打造产业链生态，在2019年牵头成立产业联盟，并于年内完成了小基站原型机开发；2020年继续推动产业链成熟，率先在业内实现了11个厂家设备的NG接口解耦、5个厂家设备与统一网管南向接口对接，以及9个厂家4款设备的功能/性能验证，满足了预商用条件；2021年推进产业链升级，在7个省分公司进行外场试点验证，为商用落地做准备；2021—2022年，完成近20个厂家60余款产品的常态化测试，助力5G室内建网。

中国联通还致力于推动5G小基站国产化。2021年完成中频段自主可控微站开发和毫米波高国产化率微站开发，中频段自主可控微站国产化率达99%；2022年发布业内首个“国产化CPU+全国产化pRRU”的自主可控微站设备，其中BBU设备采用全国产化CPU芯片，实现微基站“设备大脑”自主可控，首次实现pRRU数字中频、射频收发器芯片、时钟芯片和射频器件等关键器件国产化。CWW

精耕细作

VIAVI测试方案助推5G小基站产业腾飞

■ 本刊记者 朱文凤

截至今年2月末,我国5G基站总数达238.4万个,5G建设已经步入深水区,然而千行百业对5G网络的需求多、差异大,很难用统一的网络部署方式满足所有的差异化需求。5G小基站凭借造价低、建设方式灵活、可定制等优势,与垂直行业深度融合,正在成为5G行业应用生态的“新基石”,其需求量持续走高。

2022年国内三大运营商启动5G小基站集采,5G小基站建设全面提速。VIAVI大中华区无线业务部高级总监王兴扬表示,VIAVI的小基站测试方案覆盖从实验室产品开发生产到大规模网络部署的所有阶段,可全力助推5G小基站高效部署,持续赋能行业数字化转型。

乘势而上! 2028年5G小基站数量将超过4G

“目前运营的5G基站有70%在中国,中国已实现5G网络的广度覆盖。下一步,5G小基站将精准‘补盲’,助力中国实现5G网络的深度覆盖。”王兴扬讲道。

ABI Research预测,5G小基站大规模部署将于2025年开始,到2027年室外5G小基站数将达到1300万,到2028年5G小基站总数将超过4G。

5G小基站的蓬勃发展将带动行业专网的应用,但由于垂直行业对5G网络的需求各不相同,5G专网要按需定制,在确保网络高质量运营的基础上,



VIAVI大中华区无线业务部高级总监 王兴扬

满足垂直行业对时延、灵活性和可靠性提出的特殊需求。

另外,5G专网对安全风险容忍度低,厂商需要积极主动地进行检测以保障5G专网系统安全。5G小基站具有部署灵活、敏捷高效、性价比高和适配性强等特点,可按行业专网的需求做深入定制并提供安全保障。“小基站厂商在4G时代积累了大量经验,从5G建设初期就有计划地缩短与宏基站部署的时间差,此时已开始发挥巨大作用。”王兴扬表示。

与时俱进! VIAVI助推5G小基站高效部署

测试作为5G专网规模部署的重要一环,对支撑5G融入垂直行业尤为重要。王兴扬表示,在5G小基站建设中,VIAVI可提供端到端网络测试、核心网元测试以及云安全测试方案,协助厂商检测5G小基站是否可靠(如能否以期望的QoS稳定可靠地传输数据,能否保障吞

吐量、时延、抖动、丢包率等指标),助推5G小基站大规模高效部署。

作为基站性能测试的领先企业,VIAVI的小基站测试方案覆盖从实验室产品开发生产到大规模网络部署的所有阶段。其中,实验室测试解决方案可用于验证开放RAN基站组件,包括芯片、物理层和协议栈软件;小基站保障解决方案满足了小区回程服务激活、性能保证、监控和优化等小基站建设的全流程需求。

并且,VIAVI的测试方案与5G网络同步发展。据王兴扬介绍,业内正在探索如何部署云原生的智能化网络,在当前阶段,O-RAN测试和核心网测试为运营商和制造商带来了新的挑战,而VIAVI能够对云部署中的公有云、私有云以及边缘云的O-RU、O-DU、O-CU、RIC和核心网,进行功能测试、安全测试和端到端性能测试。

具体来看,VIAVI RIC测试方案能够复现大规模且复杂的真实接入网场景,帮助用户训练网络人工智能模型。VIAVI虚拟化的云原生测试方案允许用户使用弹性的测试平台,通过集中管理和分配资源,帮助用户在不同地点进行协同测试,降低测试硬件成本,提高测试效率。王兴扬表示,VIAVI将紧随网络云化、智能化的发展趋势,在测试工具智能化、云化方向上积极进取,不断创新,助力运营商和制造商使用云原生环境测试5G网络。

恩智浦O-RAN 5G小基站 为垂直行业“量体裁衣”

■ 本刊记者 程琳琳 王鹤迦

随着5G网络建设的不断推进,移动运营商开始调整现有的基础设施,并增加相关配置,以支持未来5G应用所需的更高吞吐量、更密集设备和更低时延。

“考虑到5G运行在高频段,基站密度将是前所未有的大,小基站的市场空间将非常巨大。”恩智浦高级客户经理樊枫在接受通信世界全媒体记者专访时讲道,小基站可以根据需要灵活地扩展或者裁剪容量,十分契合垂直行业需求。恩智浦5G接入边缘技术基于开放O-RAN架构,让设计人员可以更快地部署量身定制的5G解决方案,毫米波小基站将是恩智浦2023年的布局重点。

定制化小基站使5G部署更高效

随着5G不断普及,当前业内发展重点聚焦在5G覆盖与5G容量之间达到优化平衡。以前主要由大功率宏蜂窝基站构成的网络,现在变成各种技术的复杂组合,并根​​据需要提供容量。基于多样化的应用需求,樊枫认为小基站的形态多样化是其最显著的特点。

垂直行业对于无线网络的需求也趋于多样化。3GPP在定义5G标准时就将垂直行业的网络需求放在了前所未有的重要位置,5G可以有效提



恩智浦高级客户经理 樊枫

高工业生产效率,驱动数字化转型。

“面对不同行业的特殊要求,使用定制化小基站会更加方便和高效。”樊枫介绍道。小基站可以根据需要灵活地扩展或者裁剪容量,根据地形的不同进行灵活组网和“补盲”,根据不同的数据类别进行优先级和加密等级的排序,甚至可以根据不同时段的不同业务需求进行灵活调度。

与此同时,小基站还可以与边缘计算结合,更充分地发挥数据的作用。

“使用5G小基站配合边缘计算可以降低网络延迟。”樊枫介绍道,个人用户和企业用户的大量隐私数据通过边缘计算进行本地处理、本地加密、本地存储,只将必要的实时性数据上传到云端,极大地提高了数据安全性。

毫米波小基站是2023年布局重点

多年来,恩智浦在5G小基站产品

领域持续深耕。恩智浦5G接入边缘技术基于开放O-RAN架构,让设计人员可以更快地部署量身定制的5G解决方案,同时以更轻松、低成本的方式来维护、升级和扩展其5G功能,但毫米波技术用于5G,其信号具备不易穿透的特性,需要更多的5G小基站部署,建设5G毫米波小基站将是恩智浦2023年的布局重点。

恩智浦的5G接入边缘解决方案能够满足不同应用的多样化网络需求,其核心技术能够大幅降低业务时延,减轻对传输网的带宽压力,降低传输成本,进一步提高内容分发效率,提升用户体验。

恩智浦提供了从处理器到射频功放的完整5G解决方案,其中包括:Layerscape多核通信处理器、Layerscape Access LA1200系列可编程基带处理器、Airfast射频功率多芯片模块。其中,Airfast系列模块可满足多种5G小基站的频段或功率需求。

“恩智浦5G小基站方案的另一个特点是平台的开放性。”樊枫介绍道,多家国内外优秀合作企业已基于恩智浦Layerscape Access平台开发了5G小基站的物理层和协议栈软件。同时又有多家著名厂商基于恩智浦平台开发了形态多样化、灵活可扩展的5G小基站产品,这些产品已经陆续在市场上亮相。

针对5G车载通信模组的 模拟网测试方案研究

■ 中国信息通信研究院新一代移动通信测试验证国家工程研究中心高级工程师 陈凯

当前全球5G规模商用部署已进入“快车道”，在网络条件日趋成熟的背景下，车联网产业迅速发展，已经开始改变普通大众的驾驶体验和日常生活。完整的车联网业务需要人、车、路协同，基于蜂窝移动通信、V2X等基础设施，与大数据、人工智能网络协同，提供包括自动驾驶、高级辅助驾驶、智慧交通等全新业务体验。现阶段V2X相关路侧设施产业尚处于技术示范阶段，车企为了打造初级辅助驾驶、智能座舱、车载信息娱乐等可以直接提升驾驶体验的方案，越来越关注车载通信模组尤其是5G通信模组的通信质量。同时5G商用网络经过多年与手机、行业终端的协同发展和优化，条件较为成熟，发挥了车联网产业第一阶段基础设施的作用。

随着汽车制造行业越来越关注车载通信系统在5G网络中的表现，车企也开始自建模拟网实验室用于实现更细化的5G车载通信模组测试。本文介绍了针对5G多模通信模组进行模拟网测试的技术挑战和基本方案，涵盖功能测试、性能测试和稳定性测试等，并分享了实践经验。

5G多模模拟网实验室测试发展现状

模拟网测试是指利用商用设备在实验室或可控小规模外场区域，建设与商用网同样架构的端到端测试环境，用于验证被测产品在实际网络中的功能、性能和兼容性。在2G、3G和4G产品测试中，模拟网测试一般作为进入外场测试前的最后“门槛”，避免故障进入外场测试阶段。到了5G阶段，各大终端、芯片和模组厂家开始自建大规模模拟网测试环境，将模拟网测试向研发阶段前移，其重要程度也显著提升，主要原因在以下方面。

一是商用网络“四代同堂”，测试不仅要解决5G单模问

题，还需要解决5G与4G、3G甚至2G的互操作问题，测试难度提升，测试用例增加，测试周期必然大幅拉长。

二是为了获得最佳用户体验，基础性的功能、兼容性、互操作测试已经无法满足终端厂家对通信性能的极致追求，将模拟网作为信号源，利用空口信道模型完成针对基带芯片、射频前端和天线的测试及优化成为主流终端厂家的重要研发环节。

三是设备稳定性不断提升，传统的“外场测试出现问题后回到实验室复现解决”的模式已经非常低效，企业利用自建模拟网实验室引入大量的稳定性、自动化测试方案，可以在产品商用前将可能出现的问题提前暴露在实验室。

基于上述目的，近3年来基于模拟网的测试方案普遍应用于终端研发阶段的测试中，从基本的功能性、兼容性测试逐渐演进到性能、稳定性测试。形成了如下几类典型实践。

(1) 功能和互联互通测试

作为最传统的模拟网测试类型，功能和互联互通类测试是在产品商用前，在最接近运营商真实网络的环境中对各类业务的功能和互联互通能力进行验证，通过业务拉通各网元间信令流程，对通信协议层面可能存在的问题进行最终验证。该类型测试对模拟网环境配置要求较低，针对重点关注的商用市场，配置对应模式、厂家和频段的小区，接入业务平台，测试工程师通过手动或自动化的方式操作被测终端完成业务流程，配合信令分析软件或路测软件定位并分析故障。

(2) 网络兼容性测试

在通信芯片和终端开发初期，协议一致性测试主要是通过综测仪完成，理论上综测仪、系统设备、终端和芯片都是根据标准化的协议开发，但在实际测试中却出现各类兼容性问题，其主要原因是各厂商对协议理解不一致。为保障自家产品



图1 模拟网稳定性测试系统方案架构

与各系统设备均能兼容，终端厂家需要与各基站、核心网设备厂家完成兼容性测试。另外，实际商用的核心网和基站配置参数量巨大，在运营商网络中的具体配置千差万别，由于配置差异而导致的外场问题需要在实验室内复现解决，这也属于兼容性测试的范畴。

(3) 无线性能优化

在功能和兼容性较为成熟后，终端进入性能的差异化竞争阶段。终端性能表现不仅受限于基带算法，天线设计和优化也起到关键性作用，因此，需要在确定的空口信道条件下，开展针对性的基带和天线优化。相比综测仪等网络模拟仪表而言，模拟网系统使用与运营商商用网络相同的设备，其容量和处理能力也与运营商商用网络相同，不存在上下行网络能力受限的情况。只有将模拟网作为信号源，配合信道模拟器和空口信道模型，才能构建出最接近真实商用环境的性能测试系统。业界主流终端厂家已经着手建立自有典型无线空口信道场景库，以此作为全系列机型的精准性能优化手段。

(4) 稳定性测试

终端稳定性测试是从终端MTBF (Mean Time Between Failure) 测试的基础上发展而来。为了保证终端内置软件长期运行的稳定性和可靠性，在保证网络通畅的前提下进行软件系统的大容量、高负荷、长时间测试以发现系统故障。考虑到通信质量本身就是影响终端业务表现的关键因素，终端厂家在MTBF测试中引入了蜂窝移动通信网络，将信号强度、信号变化、切换、重配、干扰等因素作为测试条件，大幅提升了终端稳定性测试完整度。部分终端厂家已将网络损伤因素引

入MTBF测试条件中，完成之后就能模拟现网全部测试条件，形成完整的模拟网稳定性测试系统，如图1所示。

经过多年探索和应用，5G多模智能手机的模拟网测试方案已非常成熟。该测试方案持续帮助企业提升产品质量、优化产品性能，同时在模拟网基础上实现不断探索创新，为车载通信引入模拟网测试打下了坚实基础。

5G车载通信模组测试的需求和挑战

近两年，越来越多的车企意识到通信系统对整车的重要性，因此加大了通信系统研发和测试方向的团队建设力度和资源投入，部分车企已经具备自研车载通信模组能力，可以预见，移动通信和汽车制造之间的行业融合将越来越紧密。车载通信模组的测试可以借鉴大量传统终端成熟测试方案，而对于典型的车载场景，需要针对性地开发测试系统或进行现有测试方法的定制化升级，表1为传统终端与车载通信模组测试需求差异对比。

针对模拟网相关的测试方向，5G车载通信模组的需求和挑战主要包括以下3个方面。

一是多类型业务并发。车载通信模组需要完成整车运行数据、辅助驾驶数据、信息娱乐数据等多类型业务，对通信性能要求更高。在模拟网测试系统设计的过程中，需要配套对应的各类业务模型，在核心网和业务平台侧的建设规模将比智能手机测试更大。

二是天线模组的差异化设计。车载通信天线不断升级，传统的鲨鱼鳍天线、最新应用的前置板状天线以及未来整车布放的天线系统都会带来不同的通信性能影响。天线的尺寸直接影响模拟网测试线屏蔽室的建设规划，新测试系统的建设需要提前考虑后续整车天线方案的需求。

表1 传统终端与车载通信模组测试需求差异对比

主要指标	传统终端	车载通信模组
移动性	80%以上为静态或低速移动场景	● 大量高速移动场景 ● 小区间切换频繁
业务	个人通信和娱乐	● 驾驶信息、定位信息 ● 车载娱乐系统
产品设计	● 天线布放空间局促，但方案成熟 ● 功耗敏感	天线设计形态千差万别，需要单独优化
典型场景	传统的室外和室内场景	高速、隧道、地库等典型场景
使用环境	高低温、生活防水、掉落等	更严格的高低温、防水、雷电、振动、冲击等

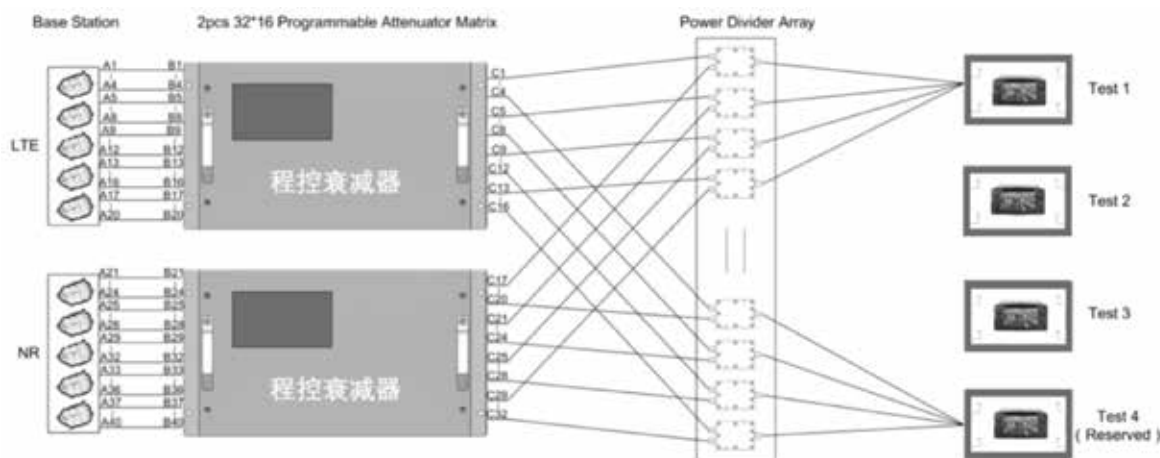


图2 程控衰减系统示意

三是大量高速移动场景和复杂特殊场景需求。大量高速移动场景主要带来多普勒效应和频繁小区间切换的挑战,使得模拟网测试方案从初期就不能只考虑功能测试,需要引入集成了信道模拟器的性能测试模块。同时,面临隧道、地库、高架桥等复杂特殊场景和恶劣气候环境影响,车载通信测试方案与传统测试方案的差别主要是空口多径传播和小尺度衰落的变化,这就更依赖空口信道模型的引入。

5G车载通信模组的模拟网测试方案设计

5G车载通信模组的模拟网测试方案设计统筹需考虑功能测试、性能测试和稳定性测试需求,针对特定应用场景和无线性能需求,兼顾成本和收益,以实现较完整的模拟网基础平台和可扩展的各类测试系统。

模拟网基础平台方案

面对日益全球化的汽车市场,国内外车企均面临“出海”需求,模拟网建设应考虑对全球运营商网络的模拟,平台设计须考虑现存移动通信制式和全球主要频段的要求。

(1) 核心网

运营商级的商用核心网建设和维护成本极高,且2G、3G、4G和5G的核心网需要全部配置,而全球有4家主流核心网设备提供商,对于模拟网平台建设都是必选。采购4套运营商级核心网对于企业自建模拟网来说投入极高,目前的最优方案是与现有多厂家大型核心网的实验室合作通过远程方式接入,同时在本地架设核心网用户面网元设备,既保证了用户面业务性能,又保障了测试数据安全,极大节省了投入。

(2) 接入网

基站采购是模拟网平台建设的主要投入,应针对全球重点市场确定制式和频段,选择当地运营商主要宏基站供应商的设备。5G基站有AAU和RRU两类站型,如果选择AAU站型则需要配置对应的工装转接板,才能将射频信号以传导方式引出,便于后续各测试系统建设。

(3) 射频信号控制

模拟网基站数量多且覆盖多制式,要实现对信号强度的控制、小区间切换和模式间切换,比较高效的方式是通过软件

控制将射频信号配置到所需测试线。这就需要引入程控衰减系统,将射频信号从基站天线口通过程控衰减器,经过多跳射频线缆及连接器,最终到达被测通信模组的天线口或屏蔽室中,程控衰减系统如图2所示。

基于模拟网的测试系统

基于5G多模车载通信模组的模拟网测试系统主要分为3

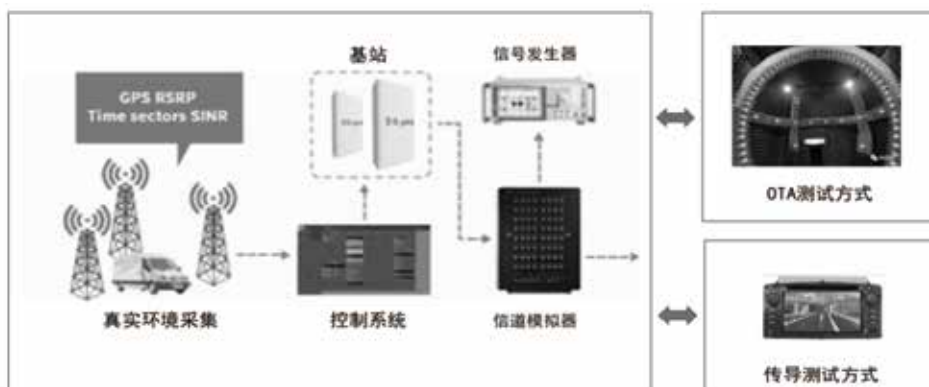


图3 性能测试系统架构

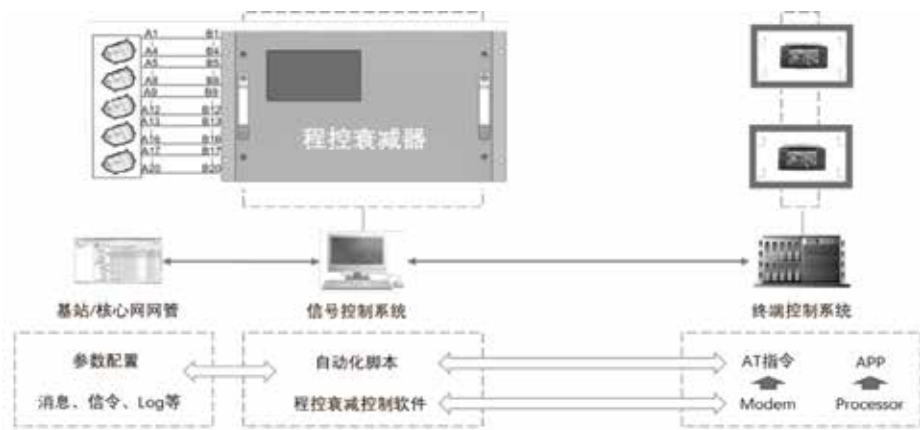


图4 稳定性测试系统架构

类，现阶段各种针对性的测试能力都可以归纳在这3类之中。

(1) 功能测试系统

主要是完成基本功能和接口协议类相关测试，包括L1/L2/L3协议的NVIOT测试、外场问题复现测试、基本业务测试等。测试系统可以是传导方式或OTA方式，测试工程师根据测试用例预置核心网和基站配置，控制信号强度，完成终端拨测并记录和分析测试结果，功能测试系统的典型测试用例见表2。

(2) 性能测试系统

主要完成空口性能相关测试，需要在测试环境中配置信道模拟器，将3GPP标准信道模型（如EVA、ETU、EPA、SCME、IMT-A、38.901 CDL等）或外场录制的真实信道模型（如密集城区、高架桥、隧道、地库等）导入，用于性能优化和问题定位。以传导方式构建的性能测试系统主要针对通信芯片算法进行性能优化和评估；以OTA方式构建的性能测试系统可以完成整机和天线性能优化测试，测试环境则需要引入多探头微波暗室。性能测试系统架构如图3所示。

(3) 稳定性测试系统

稳定性测试系统需要模拟在不同网络配置和条件下，车载通信模组各类用户行为的长时间烤机测试。

该测试系统重点要求3个方面的自动化控制：一是被测车载通信模组的自动化拨测，可以通过模组厂家自研或第三方

表2 功能测试系统的典型测试用例

序号	测试类别	典型用例
1	基本业务	接入、语音、数据等
2	移动性	切换、重定向、漫游等
3	通信质量	吞吐量、MOS等
4	多模互操作	多模切换、回落、小区重选等
5	物理层协议	频段、带宽、功控、多天线的等
6	重要功能	C-DRX、HPUE、URLLC等

APP实现模拟用户行为的控制；二是射频信号的自动化控制，通过设计和编制脚本控制程控衰减矩阵系统实现小区信号强弱、小区间切换、制式间切换、干扰信号开关等的控制；三是基站的自动化配置，通过基站网管的控制接口实现小区组网控制和参数的配置修改。上述3个方面通过统一管理软件协同控制，并且能将模组侧和基站侧的Log进行自动

化比对分析，最终实现完整的稳定性测试能力。稳定性测试系统架构如图4所示。

测试线规划设计原则

(1) 需求优先原则

在模拟网测试系统建设时，车企需要提前考虑现阶段和未来一段时间内的全球出货地，根据当地运营商和系统厂家设备配置对应的基站站型和频段，在基站设备资源池预留足够的未来扩容空间。根据对自身产品和测试量的考虑，对功能测试线、性能测试线和稳定性测试线数量进行合理规划和配比，其中稳定性测试线需要考虑并行测试的方式和数量，选择建设多条测试线还是可容纳更多被测物的大型测试间。

(2) 最低路损原则

基站资源池放置地应设计在与各测试线均靠近的位置，以满足最低路损要求。对信号路损敏感程度从高到低依次为：性能测试系统、稳定性测试系统和功能测试系统。性能测试系统在未加载空口信道模型时须保证峰值，因此一般需要独占小区资源，对性能测试需求较多时可以考虑专门配置基站资源。

结束语

车载通信模组的模拟网测试仍处于起步阶段，且目前以5G多模蜂窝移动通信系统作为主要测试内容，相应场景、模型、脚本的积累刚刚开始。

随着车载通信系统的不断发展和完善，未来针对车载通信模组的模拟网测试将向着蜂窝移动通信与短距通信结合、蜂窝移动通信与V2X结合、车载模组测试与整车测试结合的方向进行技术演进，为提升车内、车外通信质量和广大车主驾驶体验作出更大贡献。

事理认知图谱在电信运营商潜在不满预测分析中的应用研究

■ 中国移动通信集团天津有限公司 赵东明 田雷 刘静

以前,电信运营商多借助机器学习分类算法和构造分类器来衡量用户体验满意度,其不足之处在于无法得出用户不满意的原因。本文拟使用事理认知图谱技术进行电信运营商网络及业务数据的满意度认知分析,从而挖掘事件之间的演化规律与模式。具体通过引入以事件为形态的知识资源,描述实体间的关联关系,以及动态化、结构化的语义信息,最终通过事件抽取及关联将各类源数据进行串联,从而实现更精准的潜在不满预测。

用户潜在不满预测分析现状

当前,AI技术驱动满意度提升,持续提升用户体验成为中国移动重点关注的课题。回归到市场,电信行业的市场竞争主要表现为存量竞争,用户服务质量是用户归属的关键。中国移动目前积累了大量用户服务数据(10086语音、外呼语音、在线服务记录、服务标签等),每日全网内产生的语音条数可高达百万,并且可以借助语音转写引擎将语音转换为文本信息。但是目前大部分语音数据仅做短暂存储并未对潜在投诉进行回溯,对投诉语音数据的价值挖掘还存在不足之处。挖掘投诉语音数据价值,识别出的用户情绪、语义信息等可为电信运营商提供决策支持,而且提前获知用户的潜在不满意倾向甚至离网倾向,也有助于持续提升用户使用体验。

对用户潜在不满进行预测是中国移动用户服务分析的重要内容,主要用于挖掘潜在不满用户,并且给予精准维系和服务,从而提升用户服务感知。中国移动各服务领域应用呈现日趋复杂的特性,比如数据来源众多、系统逻辑复杂、应用需求繁杂等,因此中国移动潜在不满预测系统在构建中也面临“多而杂”的场景。具体来看,包括智能应答侧提供的投诉

工单、在线服务记录、需求文档、业务管理规定、语音转写文本等,以及存量运营侧需要获取的用户特征、用户标签、场景化行为、DPI解析数据等。因此构建一种服务预警的认知概念网络,针对不同场景定制模型,将对中国移动服务提升产生重要作用。不可否认的是,在相关模型构建过程中数据处理、模型学习等工作也面临巨大挑战。

就目前来看,既有衡量用户体验满意度的方法无法定位出用户不满意的原因,即便是通过统计方法,也只能定位出可能影响满意度的指标,缺少语义进行具体分析,而且业务人员在后期精准运营和业务推荐时可参考的资料较少。

因此,本文提出一种面向用户潜在不满预测的事理认知图谱分析方法,意在实现更有效的信息沉淀,即事理认知图谱可以通过数据进行自动构建,快速抽取关系,沉淀经验;更清晰地呈现,即事理认知图谱通过语义网络将基于时间线的用户事件知识进行关联,使知识关系更清晰;更有效地判别潜在不满,即事理认知图谱可以展现用户不满意的置信度以及语义原因,使业务人员在维护时能够有更好的参照。

事理认知图谱功能架构

本方案通过事理认知图谱进行以无线、家庭宽带、资费数据为基础的事理逻辑分析,从而对负面事件(用户不满、升级投诉、离网预警等)进行演化规律预测。该方案设计了一种面向用户满意度预测事件实体、事理逻辑关系(如顺承、因果、条件、上下位等)的事件知识表示方法,并通过事理认知图谱可视化地呈现单个用户的发展趋势,最终融合业务事件和事实事件,将单个用户生命周期内的事件进行时间序列串



图1 面向用户潜在不满预测的事理认知图谱技术架构

联，从而形成清晰、有逻辑的事件时间线，输出潜在不满用户列表，并将时间线关联的事件信息输出。

技术架构

该方案技术架构主要由数据层、构建层、计算层、应用层构成，如图1所示。具体来看，该方案在数据层的基础上设计事件图谱构建层及事件图谱计算层，通过事件抽取及事件关系预测从业务数据中构建事件图谱，通过事件图谱计算层补充事件关系并对事件属性及演化趋势进行计算，最终以接口及文本同步方式对上层应用赋能，实现潜在不满用户列表输出。

● 事件抽取

事件抽取主要包括事件类型判断、触发词管理、业务实体管理、事件名生成，即通过人工设定的触发词对业务数据进行筛选，将包含触发词的数据初筛出来，下一步进行事件类型及业务实体判断，进而根据事件类型、触发词及业务实体进行事件名的预测输出。

● 事件关系预测

事件关系预测主要对抽取出的多个事件进行关系判断，其中可能包括时序关系、共指关系、从属关系、因果关系等。

● 事件计算

事件计算主要对抽取出的海量事件进行相似度计算及统计，对事件进行权重、质量、热度等维度的标签划分，用以辅助后续图谱的关系推理及计算。

● 事件推理

根据上述已有的图谱信息，对事件进行关系推理及补充，并计算演化趋势。

构建方法

本文涉及的用户满意度预测本质上是一个分类任务，即通过分析带有时间线的用户事件序列，将用户分为满意与不满意两类并进行演化预测。基于事理认知图谱的用户演化分析流程如图2所示。

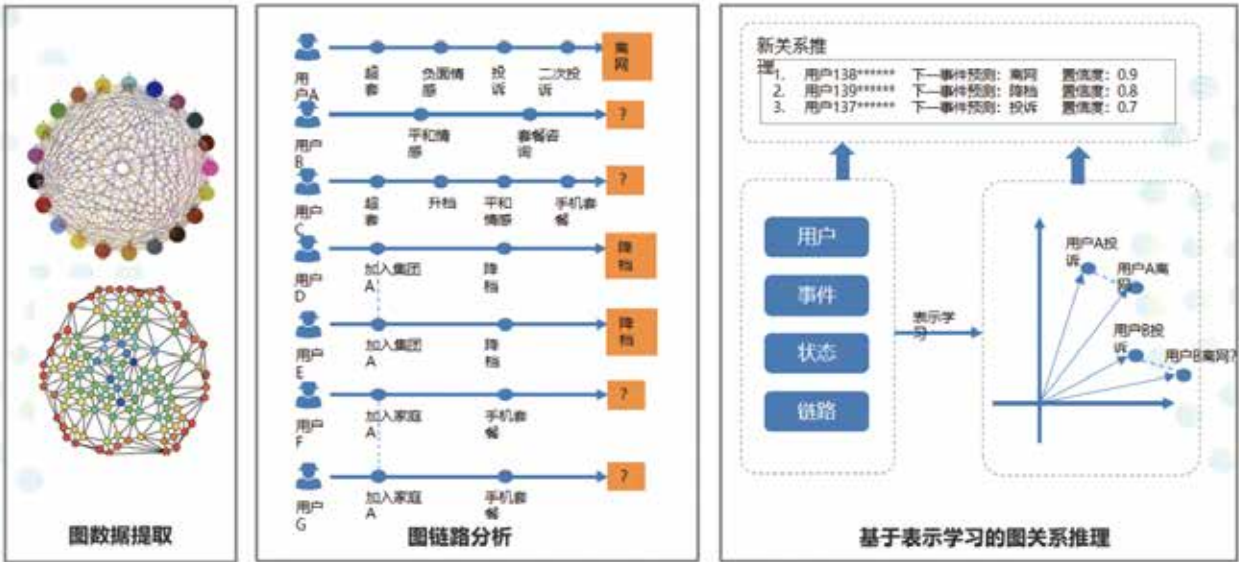


图2 基于事理认知图谱的用户演化分析流程

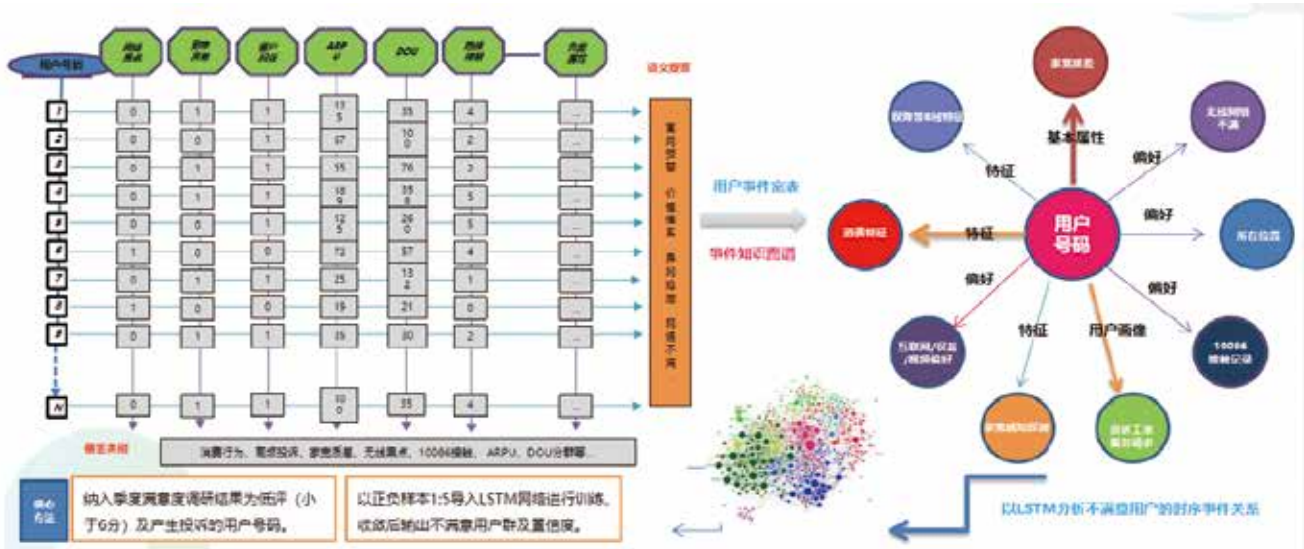


图3 事理认知图谱的构建模型

对于已有服务场景下弱时序的稀疏事件序列，既有方法很难直接从事件序列中挖掘出用户对服务的满意程度。为此，本文提出了一种PA-LSTM模型，它分为事件特征提取、用户画像构建、个性化预测3个模块。

事件特征提取模块使用LSTM从用户事件序列中提取事件特征，包括网络黑点、家庭宽带网络低质探测特征、无线网络质差、10086服务热线满意与否、投诉工单原因等，实现多维度、多场景下来源复杂用户数据的时序关系特征向量化表达。用户画像构建模块使用TCN根据用户的属性信息（如在网时长、当月通话、当月流量等）提取用户固有的时序画像特征。个性化预测即使用注意力机制分析用户敏感事件，基于事件数据和画像数据，并根据用户相近群体的满意度偏好来辅助判断用户满意度。事理认知图谱的构建模型如图3所示。

步骤1：针对现有事件图谱数据源，基于移动通信领域服务事件时序关系弱以及事件稀疏的特点，提出了PA-LSTM模型，使用事件特征提取事件语义信息，进行用户敏感度分析，指导用户画像构建。

步骤2：系统通过用户的属性信息、业务信息、位置信息以及无线网络感知和家宽探测等数据，为用户构建了基于时序事件关系的画像。同时，系统利用注意力机制个性化地学习特定用户的事件序列，同时考虑用户群体的满意度倾向来辅助预测。

步骤3：在中国移动的实际工业数据集上进行应用，通过回收运营结果，证明本方法能够很好地预测用户不满意度，

为提前进行干预提供重要帮助。

面向用户自感知的事件知识图谱满意度预测分析结果示例，如图4所示。

事理认知图谱应用实例

2022年初，该方案已在天津移动存量运营工作中正式应用。据统计，正式应用以来，该方案模型查准率达85%，查全率达63%，已执行了75.2万名用户的维系挽留，推荐成功率达32%，带来直接经济收入超4700万元。该方案的生产运营效益主要体现在减少潜在离网用户量、降本增效、节约人工成本等方面。

营销收入拓展

该方案成果应用于存量用户智慧运营体系，以机器学习算法、知识图谱对运营进行动态调优，并在多次迭代优化中，不断提升目标用户输出与策略匹配的精准度，促进营销外呼成功率提升及其他方案的2倍。针对存量用户价值循环升档、到期续约、低端用户维系、异动修复、5G终端营销、权益营销等，共完成1100万次营销，成功104万人次，推荐策略满足用户价值循环升档，用户折后ARPU提升了6.35元/户/年，方案总体创收金额达到660.5万元。

减少离网率，提升在网收益

该方案通过多场景联合运营，有效提升了用户保有率，减少了用户离网率。截至2021年12月，月均离网9.3万户，同比减少36.7%；运营用户离网率低于大网离网率，挽回流失

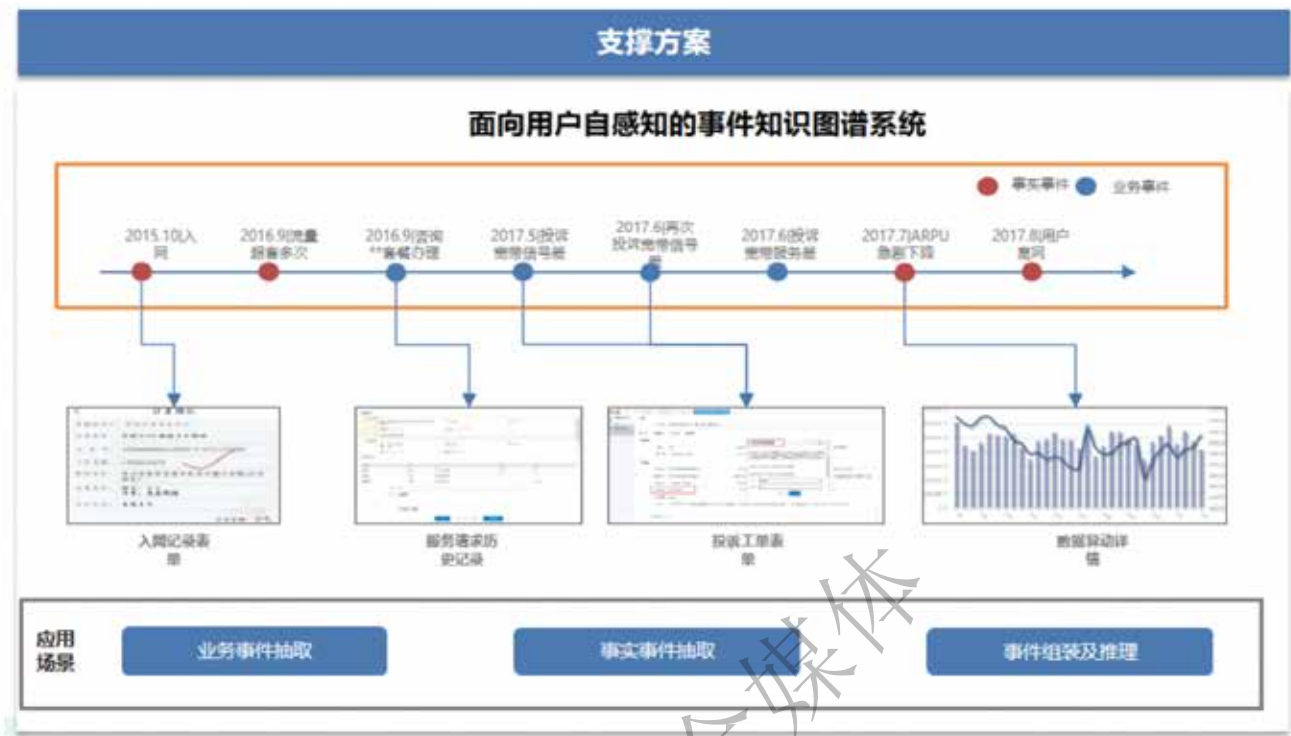


图4 面向用户自感知的事件知识图谱满意度预测分析结果示例

用户12.4万户，户均挽回损失46.5元，年挽回损失（在网收益）3459万元。

事理认知图谱方案价值

本方案遵循自下向上的构建方法,通过模式设计、抽取实体、关系计算3个主要步骤，构建了面向运营商户的潜在不满意预测事理认知图谱。提出的个性化不满意预测模型PA-LSTM，能够很好地结合用户属性信息分析用户事件序列对用户满意度的影响，同时考虑到用户群体的不满意偏向性，该模型在中国移动提供的真实用户事件数据集上取得了良好效果。

本方案依据天津移动实践经验构建的事理认知图谱，融合业务数据与大数据标签数据，使图谱语义网络能够捕捉用户的潜在意图及推荐商机，并且基于多种可能的推荐链路进行推荐排序，能够支撑市场营销人员的权益推荐、用户维系以及策略制定等运营工作。与此同时，本文以AI技术驱动运营体系进行图谱化重构，实现了推荐、维系、策略、数据分析结果可读可理解，对于打造人工智能智慧运营的认知分析图谱具有重要价值。

本方案对中国移动全网知识图谱试点工作具有重要支撑作用，提出的基于认知分析的知识图谱构建方案对全网分析

类知识图谱有较强指导意义。本方案的构建方法可以适配通用场景，在运营分析、服务预警、离网预警等方面具有广泛的应用前景。

本方案对认知图谱在满意度预测领域的应用及业务运营具有重要意义，将传统机器学习的知识图谱构建与推理改进为纳入语义分析能力的认知推理，在电信运营商户业务推荐、存量运营、服务感知分析领域体现出“可解释”的优势。目前，认知图谱已收纳天津移动900万用户的73个大数据标签、32个家宽探测特征和9个无线网络特征并建立起原子网络，以“监督+自动生成”方式产生了29个原因概念和50余个基础概念，在天津移动满意度预测中提升了查准率，为预测结果提供了明确的解释理由，为运营人员提供了有力抓手。

结论

本方案利用无线、家庭宽带、资费等多源数据构建事件序列知识图谱网络，以清晰、有逻辑的事件图谱串接相关数据，并进行演化规律预测，可以有效帮助服务运营人员分析用户不满意的原因。本方案打造的事理认知图谱，实现了以无线、家庭宽带、资费数据为基础的事理逻辑分析，已在天津移动的大数据分析、存量运营、服务推荐等场景取得良好效果。

工业互联网领域商用密码应用 安全性评估研究

■ 中国工业互联网研究院 唐明环 彭浩楠 王伟忠 查奇文 王聪

工业互联网是新一代信息通信技术与工业经济深度融合的产物，它以网络为基础、平台为中枢、数据为要素、安全为保障，是工业数字化、网络化、智能化转型的基础设施，是制造强国和网络强国建设的重要支撑。但与此同时，工业互联网的发展使工业系统逐步从“封闭隔离式”演进为“开放交互式”，引入了极大的信息安全隐患。

密码是目前世界上公认的保障网络与信息安全最有效、最可靠、最经济的关键核心技术。密码技术通过保障网络空间实体身份的真实性，信息的保密性、完整性及行为的可信赖，实现网络空间安全、可信、可控的互联互通，切实保障信息系统和数据资产安全。同时，当前被动、外挂式的传统网络安全防护措施已不足以应对日益复杂的网络空间环境，密码与网络及设备的深度融合，可使网络及设备自身具备安全防护能力，从而构建基于密码的主动、内生防御体系。

商用密码应用安全性评估（以下简称密评）是规范密码应用、发挥密码作用的必要手段，也是保障数字时代网络空间安全的客观要求。在工业互联网领域开展密评，可有效促进商用密码在工业互联网领域的应用，充分发挥密码在数据加密、身份鉴别、访问控制、取证溯源等方面难以替代的重要能力，构建以密码为基础的工业互联网安全保障体系，有效降低工业互联网安全风险。

工业互联网面临的网络信息安全威胁日益严峻

随着工业互联网的快速发展，全球工业互联网安全形势日益严峻。近年来，针对工业互联网领域的网络攻击层出不穷，美国最大的燃油管道运营商科洛尼尔公司、俄罗斯钢铁制造商Evraz公司、葡萄牙跨国能源公司EDP等遭受勒索软件攻

击；美国旧金山湾区最大的机场SFO、瑞士铁路机车制造商Stadler、新英格兰地区最大的能源供应商Eversource遭遇大量数据泄露；黑客入侵美国佛罗里达州奥尔德斯玛市的市政水处理系统，获取了远程控制权，并试图将某种化学物质的含量提高到可能使公众面临中毒风险的程度。

密评是保障信息系统安全的必要手段

密评是法律法规制度要求

自2015年《国家安全法》提出“实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控”以来，我国相继出台了《网络安全法》《密码法》《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》等法律法规，明确了使用密码技术加强重要数据和个人信息保护、落实重点防护措施的总体要求。《密码法》还对关键信息基础设施运营者提出了开展的具体要求。

工业和信息化部印发《工业互联网创新发展行动计划（2021—2023年）》，将“深化商用密码应用”作为重要工作内容，指出“加快密码应用核心技术突破和标准研制，推动需求侧、供给侧有效对接和协同创新，推动密码技术深入应用”，并强调“加强工业互联网密码应用安全性评估能力建设。”

公安部、财政部、国资委、市场监管总局、证监会等十部门联合发布《促进商用密码产业高质量发展的若干措施》，强调依法督促建设密码保障体系，并强化重要网络与信息系统密评的执法检查，从而形成需求牵引。同时，明确指出要发挥商用密码在推进传统产业数字化转型、促进数据要素安全有限高效流动等方面的重要作用，促进商用密码与新一代信息网络、量子信息、人工智能、物联网、先进制造、工业控制、区块链、智能网联汽车等融合创新。

密评有效规范和促进密码应用

密码应用安全需要相关技术人员具有一定的密码知识储备,包括密码算法、密码协议、密码产品、密钥管理等多个方面,否则会导致密码错用、误用,如系统中使用了已被破解的密码算法、使用存在安全漏洞的密码协议、密码算法相关参数使用不安全、数字证书签发及有效性验证过程不规范等。

密评是评判系统是否合规、正确、有效使用密码的标尺,通过不同技术层面,密评全方位评估密码使用,并从管理层面评估密码管理手段,是一项专业性强、覆盖面广、技术要求高且需对系统和密码应用理解深入的工作。密评依据科学全面的测评标准,通过专业的技术人员和技术手段,对信息系统密码应用情况做出评价,对密码应用问题给出专业、可行的改进建议,为网络运营者掌握系统密码应用情况并开展进一步密码应用改造提供支撑。

密评在工业互联网安全中的实践

根据GB/T 39786-2021《信息安全技术信息系统密码应用基本要求》,密评需要在密码应用的技术层面和管理层面,对网络和信息系统密码应用的合规性、正确性和有效性进行评估。

技术层面包括物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全,在测评过程中需要获取一系列证据形成有效的证据链来支撑测评结论。每个测评指标从密码使用有效性、密码算法/技术合规性、密钥管理安全3个方面进行考量。一是识别密码技术是否被正确、有效使用,以提供机密性、完整性、真实性和不可否认性保护。如信息系统部署了SSL VPN设备,但是在实际使用中未启用,未起到保障通信链路安全的作用。二是识别系统使用的密码算法、密码技术是否合规。如是否使用符合要求的商用密码算法和协议,包括SM2、SM3、SM4算法以及国密SSL、IPsec协议等。三是密钥管理的全生命周期是否安全。识别用于密码计算或密钥管理的密码产品、密码服务是否安全,如三级系统使用二级密码模块进行密钥存储。

安全管理测评从管理制度、人员管理、建设运行和应急处置4个方面,对被评估系统的密码安全管理进行商用密码应用安全性管理测评。密码应用安全管理制度应主要从密钥管理、人员管理、建设运行、事件应急处置、密码软硬件及介质管理制度等方面开展检测评估。人员管理应主要评估是否设置密钥管理员、密码安全审计员、密码操作员等关键安全岗位,是否对相关人员开展定期培训考核等。建设运行主要评估是否

根据密码相关标准和密码应用需求制定密码应用方案,确定系统涉及的密钥种类、体系及生存周期,系统投入运行前是否进行密码应用安全性评估等。事件应急处置主要评估是否制定应急处置策略,在密码应用安全事件发生时是否遵照执行所制定的应急处理流程等。

技术层面的物理和环境安全主要由信息系统所在机房的依赖设备来实现,管理层面主要关注系统责任单位的相关管理措施,不在本文讨论范围内。以下主要从基于PaaS平台的网络和通信安全、应用和数据安全层面展开。

工业互联网平台密码应用典型场景

工业互联网云平台为工业企业提供先进智能制造、设备远程运维、安全生产监控等工业互联服务能力,实现各类设备的云端接入、数据采集、统计分析、反馈控制、边缘计算等功能。典型工业互联网平台密码应用场景如图1所示。

1. 密码资源池

云平台为租户提供加解密、签名验签等云密码服务。在实际中,不可能为每个租户配置相应的物理密码产品。当业务扩展时,通常需要添加或者升级新的密码设备。然而,在面临频繁变化的应用时,传统依靠增加密码设备的扩展方案难度较大,无法做到按需弹性扩展。因此,通常在云平台建设过程中,搭建密码资源池,统一为云平台和云上应用提供密码计算、密码服务等资源,实现加解密、身份鉴别、签名验签、密钥管理等功能。

2. 统一密码服务平台



图1 典型工业互联网平台密码应用场景

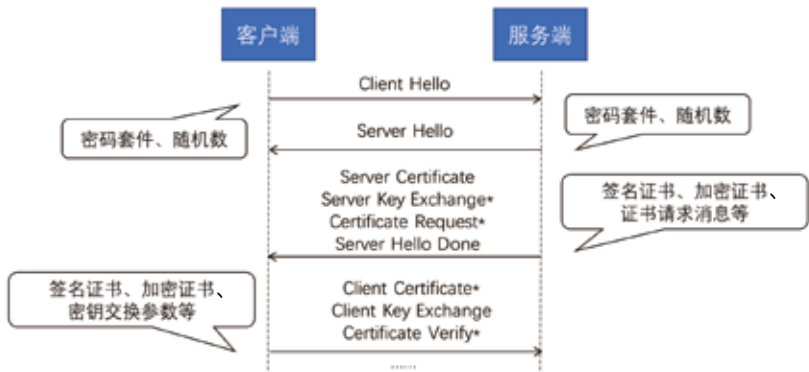


图2 SSL握手协议过程

云租户业务应用种类繁多，用户量大，关键数据复杂多样，安全机制不一致，这也为密码应用和管理带来难度。因此，密码资源池需要对云平台上所有业务应用系统提供统一的密码服务，提供多租户的密码服务能力。

密码管理平台是对若干台密码设备的统一调度管理平台，在对云平台密码资源池里的密码设备进行运维管理的同时，建立统一的密码服务接口，面向云平台上的所有应用系统提供密码接口服务，为云上租户密码应用带来便捷。

3. 安全接入网关

云平台网络边界部署SSL VPN网关，实现设备和用户数据的传输安全。与之相应的，管理面用户侧部署USB Key、国密浏览器密码模块与SSL VPN网关，建立安全的传输通道。设备侧由于工业设备类型多，协议、接口复杂，且密码的自主知识产权较少，因此，短时间内商用密码替代难度大。本文所述场景下，设备侧通过终端加密网关，一方面能够让工业设备与工业互联网接入区的SSL VPN网关之间，建立基于商用密码算法的安全通信链路，另一方面终端加密网关可以让各种工业设备接口、协议实现统一，有利于工业互联网平台与工业设备之间的快速、便捷连接。

工业互联网云平台密码应用安全性评估

工业互联网平台本质上是云平台，其密码应用安全性评估应首先遵循云平台的密评原则。云平台密码应用分为两个层面，一是云平台为满足自身安全需求所

采用的密码技术，二是云平台上的租户需要通过调用平台提供的密码服务，为自身业务应用提供密码保障。因此，云平台密码应用和安全性评估一方面要考虑云平台本身的密码应用需求，另一方面也要考虑为云上应用提供密码支撑能力。基于以上分析，工业互联网云平台密码应用安全性评估参考方案如下。

1. 网络和通信安全层面

根据GM/T 0025-2014《SSL VPN网关产品规范》，客户端和服务端建立基于国密算法的SSL安全通道，对通信双方进行身份鉴别，保证通信数据的机密性、完整性。

SSL协议通过握手协议进行通信双方的身份鉴别，并协商出连接会话所需密码套件。密码套件包括公钥密码算法、对称密码算法和密码杂凑算法。SSL握手协议过程如图2所示。客户端发送Client Hello消息，携带客户端支持的密码套件，服务端回应Server Hello消息确认使用的密码套件。接着服务端发送Server Certificate签名证书和加密证书，客户端通过验签对服务端进行身份鉴别。

网络和通信层面的测评对象主要是工业互联网云平台、管理用户和设备终端加密网关之间的通信信道。值得注意的是，租户管理员对所分配的云资源有较高的管理权限，作为云平台的用户进行测评。

在用户客户端和终端加密网关通过网络抓包工具抓取通

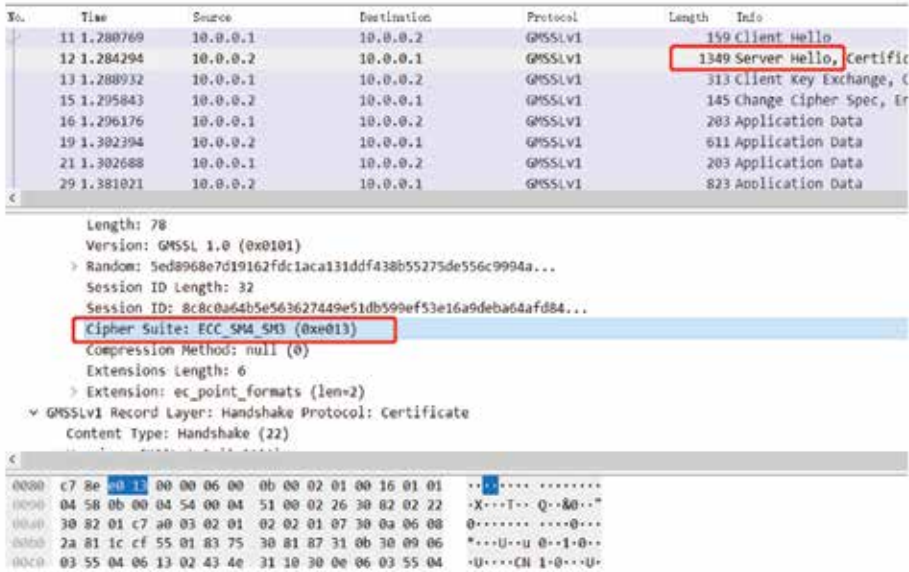


图3 SSL握手协议密码套件协商过程数据包分析

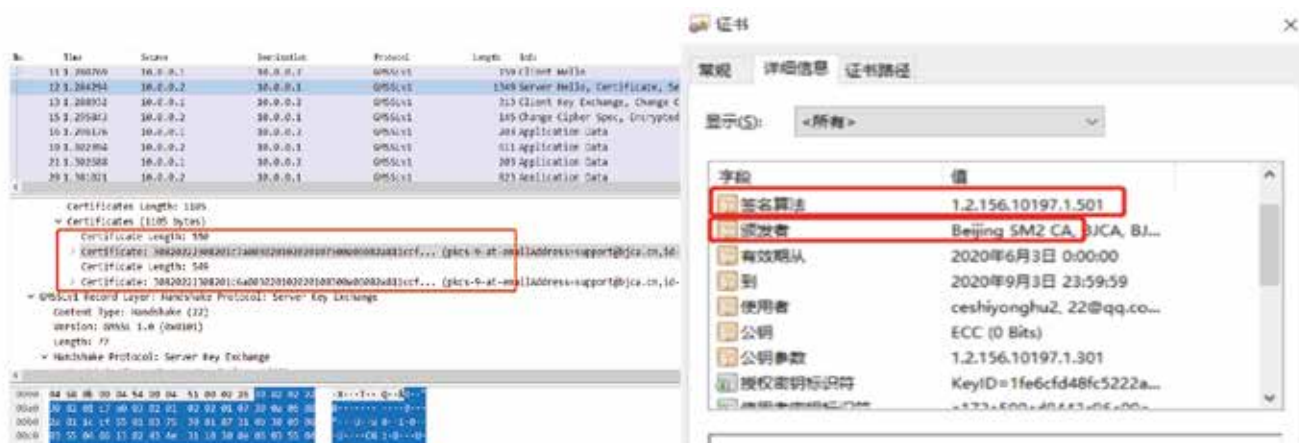


图4 SSL握手协议数字证书分析

道建立过程的通信数据包,分析数据包中采用的通信协议,如图3所示。服务端Server Hello消息中协商确认的密码套件为ECC_SM4_SM3,说明本次建立的通道采用SM4算法保证数据传输机密性,并用SM3算法保证数据传输完整性。

提取数据包中的服务端数字证书,如图4所示。数字证书中的签名算法OID为1.2.156.10197.1.501,说明采用基于SM2算法和SM3算法的数字签名进行服务端身份鉴别。

2. 应用和数据安全层面

云平台和应用系统通过统一密码服务平台调用密码资源,对用户身份鉴别数据、平台重要数据进行传输、机密性存储、完整性保护,防止这些数据被窃取和篡改。使用HMAC-SM3对应用日志记录进行完整性保护,防止应用日志记录被非授权篡改。

身份鉴别需要重点查看用户智能密码钥匙中存储的数字证书是否合规,在用户登录过程中,云平台是否调用签名验签服务器对用户进行身份鉴别。为保证数据存储机密性和完整性,需要重点查看重要数据是否加密存储,如果是明文存储,说明未采用密码算法进行数据存储机密性和完整性保护。如果是密文存储,需要分析密文长度是否符合规定的密码算法输出长度,如果密文长度不符合,说明未采用合规的密码算法;如果密文长度符合,需要查看日志记录、流量数据显示是否调用密码设备,如果无相关日志和流量,则证据不充分,不宜判定为符合,如果日志和流量显示调用了密码设备,还可以查看密钥表中存储的密钥是否与密码设备一致、密码设备配置的KEK是否为合规的密码算法等,以辅助证明数据存储进行了机密性和完整性保护。

3. 密码管理平台作为应用系统进行测评

密码管理平台是对若干台密码设备的统一调度管理平台,

在对云平台密码资源池里的密码设备进行运维管理的同时,建立统一的密码服务接口,面向云平台上的所有应用系统提供密码接口服务;业务逻辑复杂,是云上系统实现密码应用的重要支撑,故应将其作为应用和数据安全层面的一个管理类应用系统进行测评。

4. 云平台为云上应用提供密码支撑能力

云上应用的部分测评结论需要依赖于云平台的测评结果。云平台需为云上应用提供GB/T 39786中的物理和环境安全、网络和通信安全、设备和计算安全,甚至应用和数据安全等层面的密码支撑。

(1) 被完全评估的支撑能力

被完全评估的支撑能力指云平台的某些测评对象同时支撑云平台和云上应用,同时将云平台和云上应用作为测评对象。如果云上应用被完全评估的支撑能力所支撑,此时云上应用相应测评对象的测评结论完全被云平台覆盖,如果云平台已经通过密评且安全等级不低于云上应用,则云上应用测评对象的测评结论可视为不适用。

(2) 被部分评估的支撑能力

被部分评估的支撑能力指云平台提供的支撑服务仅用于云上应用而不适用于云平台,或者将服务于云平台和云上应用作为不同测评对象。如果云上应用被部分评估的支撑能力所支撑,那么需要结合“云平台支撑能力说明”对云上应用测评对象进行充分测评并给定结果。

结语

本文阐述了工业互联网面临的安全风险,提出了工业互联网平台密码应用场景,并基于该场景分析了密评如何开展,为工业互联网密码应用及安全性评估工作提供参考。

科技创新 为节能减碳助力



 通信世界