R“咖”说科技

在自主可控的技术底座上持续创新

刘庆峰



只有让用户敢用、愿用、用得起、用得好，技术能力才能转化为行业能力，创新成果才能真正形成生产力

从回答问题到执行任务，随着人工智能应用走向深入，更需要建立在自主可控、安全可信的技术底座之上。系统能否稳定运行，数据是否安全，判断是否有依据，出了问题能否追溯，决定了人工智能是否可以实现规模化价值创造。

自主可控，解决的是技术发展的主动权问题。只有掌握关键核心技术，才能把发展的主动权牢牢掌握在自己手中。其中的关键，在于芯片、框架、模型和应用能够协同，使大模型训得出、用得稳、迭代快。近年来，国内产业界持续推进软硬件协同创新，已经实现基于国产算力的大模型全链路训练和推理。这说明，依托自主可控的技术底座，我国有条件构建具有国际竞争力的大模型体系。下一步，还要在框架适配、训练效率、推理成本以及模型架构、训练方法等方面持续突破。

有了自主可控的技术底座，还要把安全可信落实到产品设计和业务流程中。哪些数据可以调用，哪些操作需要确认，哪些判断必须由专业人员复核，出了问题如何追溯，都要在产品设计和业务流程中明确。技术供给有保障，使用边界够清楚，人工智能才能做到安全可信。

基层医疗的实践体现了这一点。科大讯飞智医助理已覆盖国内800多个区县，它不替代医生做最终判断，而是以清晰的循证医学依据提供辅助诊断和风险提示；教育场景同样如此，人工智能可以批阅作业、分析错题，帮助教师掌握学情、找准薄弱环节，但讲解准确、内容适宜、学生信息得到保护，是这一切的前提。

让人工智能的价值在更多行业得到体现，走向规模化应用，还需要跨越成本、场景和生态三道门槛。跨越成本门槛，要让更多企业用得起、用得好。通过模型优化和端云协同，让常规任务在本地完成、复杂任务按需调用云端能力，使模型能力与业务需求、部署条件相匹配，在保障安全和效果的同时降低使用成本。

跨越场景门槛，关键是适应复杂的工作环境。工人操作设备、医生进行手术时，通过语音调用信息、下达指令，但现场噪声、方言口音、多人交谈，都可能影响理解。只有把感知、交互、大模型和终端设备一起打磨，做到软硬一体，再与行业知识和操作规则结合，才能让人工智能从问答工具变成工作助手。

跨越生态门槛，则需要更多企业、开发者和行业专家共同参与。技术企业开放模型能力、开发工具和成熟经验，行业从业者参与定义问题、检验效果，科研机构和开发者共同改进方案，才能把通用能力变成可靠的行业应用。

“十五五”开局之年，人工智能要在自主可控的技术底座上持续创新，在安全可信的前提下深入经济社会发展的更多场景。只有让用户敢用、愿用、用得起、用得好，技术能力才能转化为行业能力，创新成果才能真正形成生产力。人工智能发展的最终价值，不只是让机器完成更多任务，更是让人从繁重、重复的劳动中解放出来，让创造力得到更充分的释放，让更多人分享科技进步带来的成果。

（**作者为科大讯飞董事长、语音及语言信息处理国家工程研究中心主任**，本报记者**谷业凯**采访整理）

R深度观察

从源头破解“看不清、测不准”难题，人员静态定位精度优于0.2米

我国地下空间导航实现突破

本报记者　郑海鸥

“地下停车再也不用毫无头绪地满场转悠，跟着导航走，每层的车位状态一目了然。”河北雄安新区，中国电子科技集团网络通信研究院（以下简称“网通院”）工程师陈冲驾车来到雄安科学园地下停车场，打开星原导航APP，点击“去停车”，车位总数、空闲数量和具体位置一目了然。选定车位后，导航直接从地面延伸至地下，引导他穿过入口、坡道和岔路，直达目标车位。“如果途中车位被占用，系统还会及时推荐新的空闲车位。”陈冲说。

地下空间如何导航？

当卫星导航信号在地下空间不够灵敏，就需要地下空间高精度定位导航的帮助。

理论突破、技术创新、芯片研制、落地应用……致力于解决地下大空间远距离大容量高精度自主定位与无人导航控制服务难题，这项由网通院综合时空网络与装备技术全国重点实验室牵头研制的国家重点研发计划项目“地下大空间高精度定位导航与控制技术”，已顺利通过科技部验收，标志着我国在地下空间综合时空网络方向取得重大原创成果。

精准定位，在卫星信号抵达不了的地下

办完事，陈冲立即在手机上轻触“去找车”，步行导航又将他引导到车前，“如果乘坐网约车，只需输入车牌号，就能找到车辆所在的楼层和车位。”

陈冲体验的这套地下停车场智能导航服务，背后的技术支撑，就是网通院综合时空网络与装备技术全国重点实验室团队研发的“星原”北斗微基站地下空间定位导航系统。

传统的地下停车场导航，往往有3个弊端——卫星信号进不去、普通手机定不准、导航入口不连续。

实验室主任、项目负责人蔚保国介绍，团队通过在地下停车场部署北斗微基站辐射北斗信号，突破智能布网和地上地下无缝定位导航技术，实现普通智能手机也能在地下空间定位导航。

停车、找车难题解决了，意味着地面成熟的导航出行和生活服务可“丝滑”延伸至地下。

在蔚保国看来，以后车辆可以精准寻找车位，乘客可以准确找到网约车，充电平台可以引导车辆直达充电桩，未来还可为自主泊车、地下物流配送、地下机器人作业、应急疏散等提供精准的定位导航授时支撑。“车位将不再只是供车辆停放的物理空间，而成为可识别、可检索、可导航、可调度的数字化交通节点。汽车企业、地图导航企业、停车场运营商、网约车平台、商业物业和充电运营商，都可以在这一位置服务底座上开发新产品、拓展新服务。”蔚保国说。

地下空间，不仅包括人们习以为常的停车场，还有复杂的地下物流通道和综合管廊。

在雄安新区，地下空间开发是其智能化建设的重要板块，对定位导航技术的精度、容量、智能化水平要求极高。“星原”北斗微基站地下空间定位导航系统，让人员巡检、群体作业管控、无人物流等均得以实现。

巡检人员进入危险区域时，后台及时发出预警；无人运输车辆在没有卫星信号的地下通道内，也能稳定行驶、准确停靠……“我们自主研制的这套地下空间定位导航系统实测数据显示，地下空间人员静态定位精度优于0.2米，高速无人车辆可实现亚米级稳定导航。”陈冲介绍。

突破地下定位导航技术瓶颈，不仅能解决行业实际需求，更能保障国家产业链供应链安全、赋能全域空间智能化。蔚保国介绍，团队联合国内优势力量，启动地下大空间高精度定位导航与控制技术系统性攻关，目标就是构建一套全自主、全链条、可规模化落地的地下综合时空网络技术体系。

另辟蹊径，破解理论与技术难题

在地下空间，大家习以为常的传统卫星信号导航，为何就不够灵敏了？

“简而言之，就是卫星导航信号无法穿透厚重的岩土、混凝土与金属结构。而且，地下空间巷道狭窄、结构遮蔽严重，加之金属设备、粉尘等，无线信号会受到多重影响，使得电磁传播环境极端恶劣。”蔚保国介绍，同时，地下场景跨度大、形态也各不相同，既有狭长的矿井巷道、隧道，也有开阔的地下车场、物流空间，网络部署难度很高。加之自动化智能化的业务需求涌现，各类地下自主作业设备都需要亚米级甚至更高精度的定位支撑，靠传统技术难以满足。

地下空间信号“看不清、测不准”，是制约定位导航的首要问题。

“传统信号建模有点像‘看日历猜天气’，主要根据历史数据总结一般规律。”蔚保国打了个比方，这种方法可以提供大致参考，但地下结构调整，车辆和人员活动，都可能改变信号传播状态。如果模型不能及时更新，预测就容易出现偏差。

另辟蹊径，团队创新提出在线实时数据采集与离线模型优化相结合的数字孪生信道建模方法。新方法更像现代天气预报：前端如同“气象卫星”，实时感知现场变化；后台则像“预报中心”，结合长期积累的数据反复计算、校准模型。随着地下环境发生变化，模型也能随之调整。

技术的核心是绘制一张“地下无线环境图”，如同天气云图，把信号哪里强、哪里弱，从哪个方向传来、经过多长时间到达等直观地呈现出来。“借助这张图，原本看不见、摸不着的无线信号变得可观察、可预测、可推演，从而为地下定位导航提供可靠支撑，从源头破解信号‘看不清、测不准’的难题。”蔚保国解释道。

在地下空间，不仅要导得准，还要足够智能。

“比如，要让无人车自主运行，首先得解决‘在哪儿’的问题。我们设计了‘图、网、端’三级弹性定位标准。这就像给无人车上了‘三重保险’，即便地下环境恶劣导致某一种定位失效，其他定位也能立刻补位，确保车辆不迷路。”项目团队导航控制课题负责人潘树国说。

在内蒙古鄂尔多斯市门克庆煤矿，一名矿工携带矿用智能手机从地面进入井下。穿过纵横交错的巷道，系统不仅能显示他所在的巷道，还能准确判断其所在水平和高度。即使进入工作面、水泵房等金属设备密集区域，定位仍能保持连续稳定。需要前往另一作业地点时，矿工可直接用手机发起叫车请求，系统根据其位置调度无人接驳车辆；车辆沿规划路线自主穿过岔路、弯道，精准到达指定地点，完成接送。

“上述应用背后就是团队部署的井下空间综合时空网络。过去，矿井定位更多是在一条线上寻找大致位置，地图也是静态、平面的，遇到井下金属遮挡区域还易出现定位盲区。现在，人员和车辆位置可以在三维空间中连续呈现，北斗定位能够从井上延伸到井下，矿用车辆也具备了精准自主导航控制能力。”项目团队系统集成技术负责人杜世通表示。

杜世通介绍，系统还配套煤矿业务数字化管理平台，实现井上井下统一时空基准，为人员和车辆提供网络化导航服务，支持安全生产作业管理调度，为煤炭行业智能化转型提供技术支撑。

研制芯片，打破国外技术垄断

在地下定位导航领域，核心芯片是产业链的“心脏”，也是制约行业发展的关键因素。

“在2022年项目启动前，国内UWB（超宽带）定位核心芯片长期依赖进口，不仅成本高、供应链不稳定，而且核心技术与标准完全被国外掌控。”回忆起过往岁月，蔚保国心有不甘，他说，“没有自主芯片，地下定位导航技术就会受制于人。核心芯片国产化突破，必须实现！”

反复摸索、不断求证，团队意识到要从信号标准源头进行原始创新，提出原创的HNav-UWB（导航增强型超宽带）自主信号标准，彻底改变了传统技术“通信优先、导航为辅”的设计思路，转向“导航增强、通信协同”的全新范式。

“经全方位测试验证，相比国际通用标准，新标准覆盖范围提升28%，测距精度提升6%，单站容量提升65%以上，核心性能指标全面超越国际主流标准。”作为HNav-UWB信号标准设计负责人，杨梦焕颇为自豪地说。

基于原创HNav-UWB信号标准，国内首款全自主可控“探界100”脉冲定位芯片被成功研制。

为何取名“探界”？“寓意探测环境空间边界、探索测量性能边界。”团队成员齐声说。

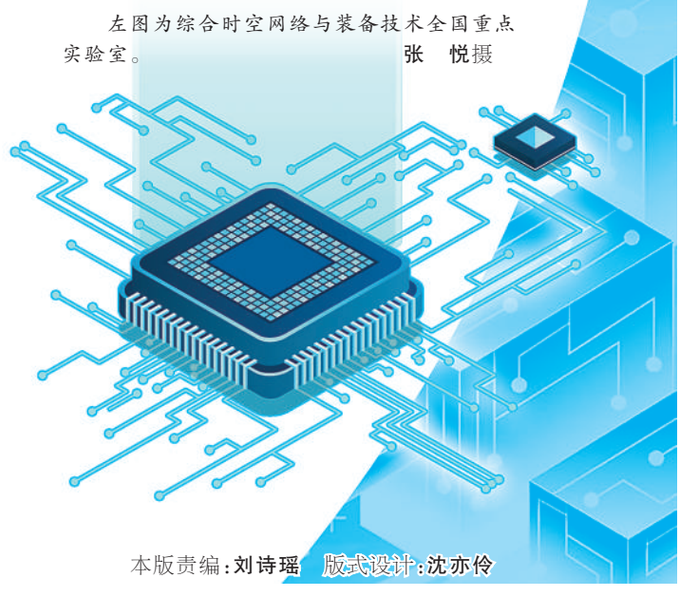
“该芯片采用射频与基带一体化高集成设计，测距精度优于10厘米，测角精度优于3度，双模可定制UWB是国际首创。在环境复杂的地下空间，这款芯片能够实现媲美地面北斗导航的超高定位精度，从根本上解决了传统地下定位模糊、误差偏大的行业痛点。”芯片研发负责人赵军表示。

探界100芯片的成功研制，打破了国外对UWB定位技术标准及核心芯片的垄断，标志着我国在国际UWB定位技术演进方面率先做出了新探索和新成果，也为地下空间定位导航自主化、规模化高质量应用奠定了坚实基础。

未来，地下空间开发利用将进入规模化、智能化、体系化发展新阶段，泛在精准时空信息服务需求将持续攀升。

蔚保国表示，“我们将继续深耕综合时空网络领域，持续优化核心技术与装备性能，拓展技术应用场景，推动成果在城市地下综合管廊、地铁隧道、深层矿山、地下人防工程等更多领域规模化应用落地，进一步提升我国在全球地下空间定位导航领域的核心竞争力，树立全球地下空间智能开发的‘中国标准’，为经济社会高质量发展提供有力支撑。”





左图为综合时空网络与装备技术全国重点实验室。　张　悦摄

本版责编：**刘诗瑶**　版式设计：**沈亦伶**

R我身边的最强大脑

用“火眼金睛”识破换脸把戏

田　天

借助AI（人工智能）技术，AI换脸足以以假乱真。如果相关技术被恶意使用，则可能滋生制造虚假信息、诈骗等违法活动。如何识破AI换脸把戏？这是我和团队攻关的方向之一。

精准有效的检测，是实现这一目标的关键。随着AI大模型迅猛发展，伪造技术也持续“进化”。传统检测方法，就像拿着一本固定的“犯罪图谱”去抓犯人——针对已知的伪造技术表现尚可，一旦遇到从未见过的新型生成方式，性能就急剧下降。与此同时，算力和数据门槛降低，快速批量生成伪造文本、图片甚至视频已成为可能，进一步增加了检测的难度和成本。

破解难题，还得靠AI。我们希望用AI打造“火眼金睛”，去甄别AI换脸等风险，让AI应用更安全更可控。技术落地应用并不容易。面对层出不穷的新型伪造手段，有一段时间，我们总是跟在后面疲于应对，最初设计的方法准确率也不高。

为什么要被动“见招拆招”，能否让AI拥有应对“未知”的能力？求学阶段在贝叶斯深度学习领域的积累，帮我打开了新视角。我想到，不一定要让检测模型对每个样本给出非黑即白的答案，当证据不足时，为何不能诚实承认“无法确定”？

经过反复论证、试验，我们在检测模型中引入贝叶斯神经网络，不再将模型参数视为一组固定数值，而是用概率分布描述参数可能的取值。通过多次概率采样，模型能够综合不同参数假设下的判断结果：预测一致时，说明证据充分；预测分歧较大时，则意味着样本可能来自未知生成器、经过复杂改写，或本身处于人机混合的模糊边界。面对这类高不确定性样本时，我们训练模型不再草率地给出真伪判定，而是教它承认“不确定”；在此基础上，再针对此类样本进行优化，提升模型性能，使其在面对新型AI合成方法时，依然能够识别80%以上的合成数据，误判率得到有效控制。

这意味着，模型不再把大量精力花在一眼就能判断的简单样本上，而是将学习重点转向“不确定”数据。资源集中到真正有难度的地方，模型就能更快、更准地摸索出识别AI内容的策略，面对新的AI合成内容时表现更好。当技术路线得到验证的那一刻，团队上下倍感振奋。我们不再是伪造技术被动的追赶者，而拥有了一套主动应对未知风险的底层逻辑，“教”AI从更深层上理解规律，识别应用风险、拒绝有害请求。

如今，基于团队技术开发的AIGC（生成式人工智能）内容检测平台等AI衍生安全风险治理以及AI内生安全产品，已经在金融、政务、公安、互联网等场景中落地应用。由于存在安全焦虑，一些企业最初不敢放心使用大模型，经过我们技术安全评测与安全加固后，解除了后顾之忧，真正享受到了AI的便利。

AI在进化，风险也在变。随着智能体和具身智能机器人兴起，AI正从“回答问题”的对话框，变成“执行任务”的行动者，相关风险也从虚拟世界延伸到物理世界。具身智能机器人的安全风险更为直接。这类机器人在物理世界开展作业，一旦无法应对特殊情形，就有可能对人类造成伤害。用人类智慧驾驭AI，这是智能时代必须直面的时代课题。我和团队将继续深耕AI安全研究，助力AI健康有序发展。



田天近照，AI修饰生成素描画

（**作者为新一代人工智能产业技术创新战略联盟专家委员，姜子钰、喻思南**采访整理）