高技术前沿

今年9月，俄罗斯“乌什库尼克”科研生产中心宣布，将批量生产“蜘蛛”无人机声学探测系统。系统由多个自主传感器组网构成，依靠声学信号对无人机等目标等进行探测，识别空中目标类型，估算飞行方向与速度。

今年10月，立陶宛国防部宣布，最新融入了射频探测能力的Sky Fortress声学探测系统，将进入该国进行试点部署。据悉，该系统通过捕捉低空目标发出的声音，进而对留下声学或电磁痕迹的目标进行识别分类，最终实现对低飞无人机、巡航导弹这类雷达难以有效应对的目标进行探测。

事实上，声学探测网络并非新生事物，其技术背景也并不复杂。有人形容它为“会听无人机的耳朵网”，通过布设很多低成本声学传感器节点，专门抓取、搜集低空中慢速飞行的小型无人机的声音。

那么，世界多国为何不约而同地将目光投向无人机声学探测网络？在未来的反无人机作战体系中，它又将发挥怎样的作用？请看本文解读。

在战场需求的强力牵引之下，声学探测网络技术“重获新生”——

“听”见无人机

■张 鑫



俄罗斯无人机声学探测网络示意图。 作者供图

百年“听风”，为何重回战场

声波看不见，却从未离开战场。

俄乌冲突中，当乌克兰街头响起俄罗斯“天竺葵”系列低成本远程巡飞弹的轰鸣声，当地一座座巡飞弹预警装置依托无人机声学探测网络，早在人们听到这些轰鸣声之前就已被相继“点亮”、接力运转。

无人机声学探测网络的出现，最早可以追溯到第一次世界大战时期。当时，飞机逐渐成为战争中关键的作战力量。为了发现来袭敌机，技术人员发明了机械式的声学对空预警探测系统，并将其投入实战。该系统设计思路十分简单——用巨型喇叭或反射面收集飞机引擎的声音，再由听音员根据声音判别飞机方位。

其中精度最高的，当属法国物理学家让·佩兰研发的佩兰听音器。这套系统本质上是一组声学集音装置，据测算，其角度误差仅为2至3度，探测距离可达7至8公里。

到了二战时期，当雷达这只看得更远、辨得更准的“千里眼”技术成熟后，声学探测网络技术便很快退出了对空预警领域舞台，此后长期沉寂。

转折出现在2010年代中期。此时，小型多旋翼无人机大量出现，给战场带来了新的“变量”。

到了2022年2月，俄乌冲突爆发，双方首次大规模将第一人称视角（FPV）无人机、巡飞弹等低空低速空中打击手段引入实战。

在交战区域前沿，一架价值仅几百美元的FPV无人机，携带廉价的火箭助推榴弹，就成了一件“精确制导”的反装甲武器。它能迅速穿过战场，精准快速地摧毁价值数百万美元的先进坦克，或装满步兵和物资的车辆。

面对FPV无人机、巡飞弹造成的严重威胁，俄乌双方均发现，传统防空雷达预警体系在探测这类目标时显得力不从心：受目标速度、材质等特性影响，加上受到低空地形和地杂波的干扰，雷达的探测距离与效能大幅下降，雷达“千里眼”变成了“近视眼”“青光眼”。

短板在哪里，机会就在哪里。

FPV无人机、巡飞弹飞行时，螺旋桨、电机或发动机等部件会产生特定声波。这一无法被掩盖的物理特征，让沉寂良久的“利用声音实现对空预警”的思路，再一次进入人们视野。

同一时刻，声学探测网络技术融合现代微电子、信号处理和人工智能等技术，识别能力也大大提高。

乌克兰率先把这一技术大规模推上现代战场。

战场之上，乌克兰“Sky Fortress”声学探测系统投入使用后，从另一个维度打开了对FPV无人机、巡飞弹等低空慢速飞行目标预警的大门，让声学探测网络技术在21世纪的现代战场“重获新生”。

从一只“耳朵”到一张网

今天的无人机声学探测网络，由多个像耳朵一样的声学传感器节点组成。这些声学传感器节点，主要包括电源模块、麦克风和计算与通信模块：电源模块为节点供电，麦克风负责捕获环境中的声波并将声波转换为电信号；电信号经过数字化处理后，进入计算与通信模块，随后进一步借助信号处理和人工智能技术，从背景噪声中提取微弱的无人机声纹，并将声纹结果对外发送。

这些声学传感器节点的运用方式不同，能力有强有弱，无人机声学探测网络也随之分出不同的类型。

——小规模阵列型网络。

此类网络的单个声学传感器节点包括由多个麦克风组成的阵列，节点能够对麦克风收集到的声音信号进行恰到好处的延迟和叠加，进而增强声波。这类网络能帮助指挥员辨别无人机的来向，探测与无人机的距离。乌克兰的“FENEK”、美国的“Drone Hound”、挪威的“Discovair G2”等声学探测网络均属此类，能够对来袭无人机实施近中距离的探测，但其探测距离和角度分辨能力受节点阵列大小限制。

——分布式低成本网络。

这类网络的单个声学传感器节点通常不具备麦克风阵列，声波感知能力有限，整体性能依赖多节点协同与通信条件的好坏，但胜在成本低廉，其体积、功耗能够支持长时间野外使用。乌克兰的“Sky Fortress”和俄罗斯的“蜘蛛”都是这种类型，能够在雷达探测受限区域实现大范围隐蔽覆盖。

两种网络，各有优势。

小规模阵列型网络单节点能力强。它可将少量节点部署在需要防护的关键设施周边，将探测信息发送给反无人指控系统，为雷达、光电等探测手段提供引导，并与其他探测信息融合，提升目标识别的可靠性。以乌克兰战场应用的“FENEK”为例，它对“沙赫德”型无人机的探测距离达到3公里，对巡航导弹的探测距离达到5公里，还能综合多个节点测量的目标角度解算目标坐标。

分布式低成本网络部署便利，有助于实现网络的规模化覆盖。它通常通过大规模节点部署和组网，形成对区域的预警探测。典型如乌克兰已部署的“Sky Fortress”，对部分小型无人机的探测距离仅有150米至450米；但在2025年，它已依托民用基础设施部署约14000个节点，并计划增至30000个节点以上，构成了乌克兰反无人机早期预警网络。

俄罗斯的“蜘蛛”相对乌克兰的“Sky Fortress”作了进一步优化：在提高对无人机探测能力的基础上增强了网络部署的便利性。据悉，该系统的部分节点可通过空投落地固定，也可挂附树枝部署，从而在峡谷、森林、沼泽、河道等低空无人机突袭航线上，构建起生存性极高、部署弹性极大的低空预警探测网络。可以预见，“蜘蛛”未来正式部署后，将有效提升俄方应对大规模无人机突袭的预警能力。

不可或缺的“沉默哨兵”

现代战场上，各类小型无人机、巡飞弹日益活跃，作战样式不断变化迭代，这让各国都不得不重视反无人机体系建设。

作为反无人机链路中的关键环节，预警探测能力的建设是体系建设的重点。与雷达、光电、电子侦察等传统手段相比，无人机声学探测网络的优势究竟在哪里？

从有效性看，它补的是“看不见”的盲区。随着光纤控制无人机和智能目标识别等技术的发展，声学探测网络技术不依赖电磁信号、被动探测的特点更显珍贵：难以被敌方侦察与干扰，能够用非电磁方式发现雷达“看不见”、电子侦察“搜不到”的低空无人机目标。

北约一项评估报告中确认的一起战例颇具说服力：一次防空作战中，乌克兰通过声学探测网络技术，对进入领空的84架俄罗斯无人机全部实现了追踪；基于声学系统提供的早期预警数据，机动火力小组拦截并摧毁了其中的80架。

从经济性看，它省的是“铺不起”的成本。最直观的差别，体现在传感器单价上。乌克兰“Sky Fortress”系统单个声学传感器成本在400至1000美元之间。与之形成鲜明对比的是，即便是小型雷达系统，单价也需要约2万美元；而高性能防空雷达系统的价格，则达到百万美元以上。

从体系建设看，它织的是“接得上”的链路。在雷达覆盖的边缘和盲区布设无人机声学探测网络，用以提高对低空慢速目标的持续监测能力，再将探测数据实时注入指控链路，引导其他预警探测手段，帮助拦截力量提前反应、提前准备，这将有效提升反无人作战的成功率。

俄乌冲突的实战数据也印证了这一点：据乌克兰官方媒体报道，2025年的战场上，无人机声学探测网络帮助追踪了进入乌克兰领空约20%的目标。这一比例说明，声学探测网络已成为反无人机体系中重要的感知层之一。

目前，在以消耗与反消耗为特征的无人化战争中，无人机声学探测网络的价值，或许正在于它足够便宜、足够简单，可以足够多地铺开——用足够多的传感器节点，在战场上铺设一条应对低空无人机的预警带。即便部分节点被毁，网络整体仍能运行。这些不发声、不辐射、不倦怠的“沉默哨兵”，正成为反无人机体系中越来越重要的一环。

新看点

另辟蹊径的分子计算机

■江 舟

今年9月，爱尔兰梅努斯大学研发团队在《自然》杂志上发表一项研究成果：他们造出了一台DNA分子计算机。

与运行在硅芯片上的传统计算机不同，该系统是由浸泡在少量盐水中的相互作用的DNA链组成。通俗地说，这种计算机不靠芯片，它的“算盘”是试管里的一群DNA分子。其计算的核心思路可以分为三步——

第一步，编码。把要解决的问题“翻译”成DNA序列。计算机文件本质上是一串二进制数据，编码就是按照特定规则，将二进制数据映射为DNA序列。

第二步，写入。编码完成后，工作人员需要借助化学方法将设计好的序列拼接成一串DNA分子，这就是“写入”。“写入”的核心，是把数字世界的0和1，翻译成A、T、C、G四种碱基的排列组合。DNA依靠碱基的排列顺序来编码写入信息，一条DNA单链就是一串可以被“读取”和“操作”的符号。

第三步，读取。这是指在需要读取数据时，工作人员通过对DNA样本的测序，读出其上的碱基序列，再通过解码规则将信息还原成二进制文件。不过，目前的读写过程仍相对复杂耗时，效率较低。

DNA分子计算机的杀手锏在于“并行计算”。在合适实验条件下，一管DNA溶液，可以容纳数量极大的分子同时进行配对反应。对于传统电脑需要通过一步步串行计算处理的组合问题，DNA溶液可以在一次混合中同时尝试大量计算可能。

北京大学信息科学技术学院时任副研究员张成打了一个比方：DNA计算环境下，每条DNA单链都可以看作一台计算机，海量链条组合在一起，就是一个容纳成百上千台计算机同时工作的天然“机房”。

当然，DNA分子计算机并非万能，在迈向实用化的路上，面临着一系列挑战：一方面，DNA分子稳定性低，容易发生降解，这会影响计算结果的可靠性；另一方面，DNA分子计算机的核心操作依赖分子扩散和生化反应的快慢，其速度远不及电子计算机。“读写”速度受限，使其巨大的理论算力难以被充分利用。

人们长期以来习惯把计算机理解为硅基芯片设备，而这则新闻让我们看到，DNA分子同样可以承担计算任务。当硅基芯片的性能逼近物理极限，我们或许可以另辟蹊径从分子层面寻找新的计算范式。或许在未来的某一天，DNA分子计算机可以走出实验室，成为造福人类的新工具。



DNA分子计算机概念图。 资料图片

AI+军事

量子算力如何赋能未来智能化战场

■赵 林

量子算力，是基于量子叠加、量子纠缠等量子学特性形成的新型计算能力。它突破了经典计算机依靠串行计算模式处理数据的算力极限，可并行处理海量数据，在优选方案、大规模仿真、密码破译等领域展现出较大潜力，正在成为赋能未来智能化战场的重要力量。

——驱散战争迷雾，指挥决策“更敏捷”。

“战争迷雾”的核心，是战场的不确定性：敌方动向不明、态势信息杂乱、海量情报真假难辨……面对智能化战场上海量多源异构数据，传统计算机算力有限，很容易“算不过来、反应慢半拍”，极易贻误战机。

相比之下，量子算力实现了指数级并行运算，大大提升了系统的运算效率。这意味着，原本需要数小时甚至数天才能完成的复杂战场仿真、多域态势融合、作战方案推演等，可被压缩至秒级完成。

这能够帮助指挥员精准预判敌方意图、筛选最优作战方案，大幅提升指挥链的敏捷性与精准度，有效驱散“战争迷雾”。近年来，世界许多国家已竞相展开探索。美国国防高级研究计划局2019年启动某量子设备优化项目，围绕航线规划、传感器与目标分配、后勤调度等作战筹划中最消耗算力的难题展开攻关；2024年初，北约发布首份《量子技术战略》，把量子计算、建模与仿真等列为军事应用的重要方向，看中的同样是量子算力压缩战场仿真耗时、加快战场指挥链路循环的潜力。

——突破算力瓶颈，武器装备“更自主”。

未来智能化战场上，智能化武器装备想要做到“反应快、打得准、会应变”，离不开算力的支撑。传统计算条件下，不管是无人机集群协同突防，还是精确制导武器自主搜索、识别、锁定目标，都面临着算法训练迭代慢、算力供给不稳定等问题，很难适配瞬息万变的战场环境。

相比之下，量子算力为智能装备效能的发挥提供了前所未有的硬核动力。一方面，海量算力资源为智能算法打通了极速迭代的通道，为装备的“智能大脑”提供了全天候、高强度训练环境，装备可通过海量战场数据样本快速进化；另一方面，随着量子计算模块小型化技术的进步，轻量化量子计算模块未来有望嵌入作战装备，实现算力实时赋能战场，让无人机集群自主避障、协同突击，让精确制导武器实时修正弹道、灵活规避拦截，真正实现把数据优势转化为打击优势。

例如，德国航空航天中心2022年立项的“量子计算用于合成孔径雷达”项目，专门研究量子算法在合成孔径雷达系统设计等方面的应用，目的是为装备的自主感知与维护提供算力支撑。

——筑牢安全底座，信息防护“更坚固”。

未来智能化战场的核心竞争力，既在于“算得快、打得准”，更在于“守得住、防得牢”。传统信息防护依靠复杂的数学运算构建防护屏障，但在高强度算力攻击下逐渐暴露短板，被破解风险持续升高。

针对智能化战场中新型网络攻击的威胁，量子算力可支撑加密算法高强度快速迭代，快速生成适配的防护策略，同时实时监测指挥节点、装备终端的运行状态，及时发现并处置潜在安全隐患，防范敌方入侵指挥系统、破坏终端设备。例如，美国发布《商业国家安全算法套件2.0》，要求国家安全系统在2035年前完成抗量子密码改造。北约发布的《量子技术战略》同样提出，推动各成员国密码系统向“量子安全”过渡，以应对“现在收集、日后破译”的现实威胁。

从驱散“战争迷雾”，到突破算力瓶颈，再到筑牢安全底座，量子算力正从实验室加速走向战场，悄然塑造着未来智能化战场的力量格局。当前，世界多国纷纷加快量子科技军事应用布局，这场围绕量子算力的竞逐才刚刚开始。