■手段隐蔽性好
■附带伤害性低
■还能有效避免人员伤亡

无人机袭击大行其道 多款“软杀伤”招数能以柔克刚

据媒体报道，近日，隶属于俄罗斯南方军区的北方舰队第200独立旅的一名情报人员称：俄罗斯军方通过截获视频信号，识别出乌克兰自杀式无人机战术，在了解乌军无人机技术原理后，采取了针对性的干扰反制措施，有效切断了无人机通信链路，为士兵快速击落无人机打开了新思路。那么，这种“软杀伤”手段究竟是如何实现的呢？相比传统的反制无人机手段，在更加严峻的无人机威胁下又有何突出的亮点呢？

据澎湃新闻网

“软杀伤”隐蔽性好 “四两拨千斤”反制无人机

相比于枪弹等传统“硬杀伤”方式，“软杀伤”手段隐蔽性好、附带伤害低、安全可控，是极具性价比的反制无人机方式。传统军用无人机体型较大，机动能力有限，在进行侦察、攻击过程中非常容易被防空导弹系统或其他地面火力击毁。在吸取多次教训后，一些国家和组织采用体积更小、行动更加敏捷的无人机开展空中突袭和打击。

在近期的俄乌冲突、巴以冲突中，经常出现无人机“以小博大”的惊人场面。据媒体报道。乌军曾出动一架土耳其制造的TB-2察打一体无人机，秘密潜入克里米亚半岛西北海岸叶塔托利亚地区空域，发射一枚空地导弹摧毁了俄S-400防空阵地的雷达车，随后数枚乌军的“海王星”巡航导弹对防空阵地发动进一步的“饱和打击”。强如S-400的防空导弹系统有时候也对这些无人机毫无招架之力。

无线电干扰设施 可有效避免袭击中人员伤亡

在传统“硬打击”手段黯然失色的回合中，“软杀伤”方式却发挥了出奇制胜的优势。2018年8月4日，委内瑞拉总统在玻利瓦尔大道举行成立81周年庆祝活动。在演讲过程中，遭到了多架携带炸药的旋翼无人机袭击，然而现场部署了特殊的无线电信号干扰设施，对来袭无人机进行了及时的干扰反制，有效避免了人员伤亡，最终使袭击者的计划落空。对付这些战场上来去自如的无人机，只要充分了解其技术原理，从专业角度寻找它们的弱点，反制无人机就是轻而易举的事情。相比于枪弹等传统“硬杀伤”方式，“软杀伤”手段隐蔽性好、附带伤害低、安全可控，是极具性价比的反制无人机方式。

根据反制无人机的技术原理，“软杀伤”方式可以分为“断、骗、盲、黑”等类型。“断”即干扰阻断数据链路，使通讯无法正常闭环；“骗”即发送伪造信号，诱导无人机执行错误的指令；“盲”即致盲机上的传感系统，使其无法正确感知目标和环境；“黑”即借助黑客手段，夺取接入互联网的无人机的控制权限。

阻断通讯信号 让对方指挥员瞬间失去视野

今年10月，俄军某部队士兵在互联网上展示了一种临时自制的无人机干扰武器，该武器配备特殊的天线，可在五百米范围内对无人机的通讯链路进行干扰，切断乌军自杀式无人机的影像信号，使敌方操作员瞬间失去视野，为俄军击落无人机提供了极大便利。这种通过向无人机发射大功率干扰射频信号，使无人机与地面站失去连接的方式，便属于干扰阻断类“软杀伤”。

低成本无人机通常采用GPS与惯性仪器进行组合导航，对GPS信号进行干扰后，无人机只能依靠惯性导航，从而失去作业精度。无人机的电磁防护能力普遍有限，高功率微波和电磁脉冲都能使机上的电子元器件暂时失效或直接烧毁，导致无人机瘫痪或坠毁。国外一些国家在干扰阻断技术上发展较快，如俄军的REX-1便携式电磁枪，可干扰无人机的雷达和导航系统，在叙利亚战争期间取得过击落50多架无人机的战绩；2018年，以色列也发布了增强型“无人机卫士”地面系统，可对无人机进行有效探测、跟踪，并实施电磁干扰。

巧用导航欺骗技术 伊朗曾成功诱骗美军无人机

早在2011年12月，美国的一架RQ-170隐形无人机在执行任务时被伊朗控制，降落在了伊朗东北部的城市卡什马尔，一名参与诱捕行动的工程师表示，伊方先是对无人机的通信系统进行了压制，切断无人机与地面站的通信链路，迫使其进入自动导航状态，随后利用技术漏洞和GPS伪造信号重新修改了无人机的导航系统坐标，使无人机误以为自己已经到达美军在阿富汗的基地，实际上被欺骗降落到了伊朗境内。这就是著名的伊朗导航欺骗美军无人机的战例，引发热议。2012年12月，伊朗又在波斯湾上方捕获了美军的一架“扫描鹰”无人机，但具体细节并未透露。

导航欺骗技术的优点在于能够对敌方无人机实施诱捕，从而可靠截获机载的情报信息或秘密技术，但是有效的导航欺骗往往需要对敌方无人机技术有充足的了解，而且需要采用可靠的欺骗策略，需要生成无人机无条件信任的导航虚假信号，成功采用导航欺骗技术完成对无人机进行诱捕的战例简直是凤毛麟角。

迅速致盲高效反制 一些国家发展激光武器系统

无人机对目标的探测、跟踪依靠机载的光电传感设备来实现，好比他们的眼睛，那让它们变成瞎子也是一种有效的反制方法。近年来，激光武器凭借精度高、速度快、能量集中等优点备受各国关注，一些国家已经发展出车载、舰载、机载等平台上的激光武器系统。

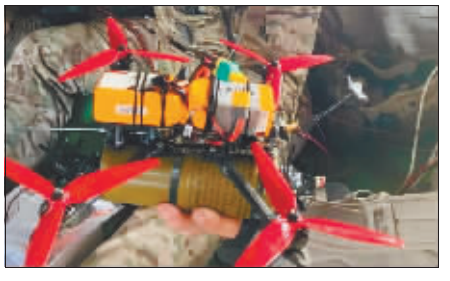
今年4月，土耳其首个NAZAR激光电子攻击系统交付土耳其海军司令部，标志着该国对激光武器的研制步入新阶段。该武器由指挥方舱、激光转塔、稳定系统和发电系统等组成，与其他激光武器不同，它抵御来袭导弹的方式是用激光实施致盲，使导弹丢失目标并失控。NAZAR系统的设计理念与第三代和第四代导弹普遍采用光电制导和红外制导导引头有关，当探测到来袭导弹后，系统会进行持续跟踪和锁定，推断出导弹的工作方式和导引头工作波段范围，发射出对应波段的激光，基本可以覆盖大部分导弹导引头的工作波段。

无形黑客利用漏洞 实现对无人机的无线劫持

现在的一些民用消费级无人机为突破传统无线电的传输距离，开始使用WiFi网络、4G等通讯方式，便于用户在移动终端上进行超视距操控，因此它们可被视作网络上的设备，通过黑客技术就能易如反掌地对这类无人机实现入侵控制。

在2015年10月的黑客大赛GeekPwn上，参赛选手成功演示了利用安全漏洞来实现对无人机的无线劫持。虽然受网络加密与WiFi路由信号衰减的影响，该技术的难度较大且存在距离限制，但随着无线通信技术水平的提升，该技术也将成为今后反无人机方式的一个重要发展方向。

1974年第四次中东战争中，曾在多次叙利亚“冥河”导弹袭击下吃亏的以色列反败为胜。当“冥河”导弹来袭时，以色列导弹艇利用电子干扰技术，使导弹无法正确识别以军舰艇，最终偏离目标，被以军速射火炮迅速击落，而以军则用导弹击沉了5艘未采用干扰措施的埃及和叙利亚的导弹艇，此次交战也成为电子干扰“软杀伤”和武器打击“硬杀伤”相结合的成功战例。“软杀伤”有着优异的反无人机效能，而随着无人机抗干扰、抗欺骗等先进技术的不断改进，现有的“软杀伤”手段也应当进行持续的升级与革新，在瞬息万变的战争态势下，发展多种类、体系化的无人机反制系统将为未来制胜创造更好的条件。



民用无人机改装的自杀式无人机。

土耳其激光武器系统。