关于小型无人机风险隐患及反制设备自动化系统化智能化建设的调研思考

■ 付　括

摘　要　近年来，随着芯片、通讯等领域科技发展，无人机相关技术趋于成熟，被广泛应用于消费娱乐、工业农业等领域。同时，无人机存在安全隐患和管理漏洞，被用于恐怖袭击、非法监控、非法运输等不法行为，对公共安全造成严重威胁。实施无人机反制，要对入侵目标进行有效侦测，整合信息进行智能分析及预判，制定反制策略，整体调动反制力量，实施系统化反制。

关键词　无人机　侦测反制　系统化　智能化

无人机是利用无线电遥控设备和自备程序控制装置的不载人飞机，主要包括无人直升机、固定翼、多旋翼飞行器等。小型（包括轻型、微型）无人机，是指空重不超过 15 千克或最大起飞重量不超过 25 千克的无人机，目前绝大多数民用无人机均属于小型无人机。随着科技进步，无人机从“航模玩具”，到消费娱乐“高空相机”，再到工业、农业、军事领域“蓝领工人”，经历了从无到有、应用范围逐步扩大的阶段。无人机具有自动化程度高、易操作、造价低廉、机动灵活等诸多优点，给日常生活带来便捷的同时，也暴露出越来越多的安全隐患，对社会甚至国家安全构成了严重威胁。无人机是先进技术积累的产物，涉及多学科领域，与其伴生的无人机反制行业，同样涉及到众多先进技术领域，将随着无人机的发展而不断进步。

一、多因素助力——无人机发展时代背景

无人机行业发展受益于复合材料应用、机电控制技术提升等多方面因素，但最主要得益于芯片和通讯技术的发展。芯片领域。目前制造工艺尺寸已提升至 3 纳米级别，随

作者：北京市公安局反恐怖和特警总队一级警长

本文系 2024 年中国警学论坛优秀论文。

着芯片集成度增加，一方面，算力增强，反应速度变快，可运行更为复杂的程序，有助于提升无人机自控、自主飞行能力；另一方面，芯片体积缩小，功耗减少，有助于提升无人机续航能力。通讯领域。信号传输技术持续发展，跳频、扩频技术在无人机领域实现应用并不断更新迭代，信号传输效率、抗干扰能力提升。目前，手机通讯已迈入5G时代，以星链为代表的卫星通讯技术逐渐“平民化”，无人机通过无线电信号、手机信号、卫星链路，高效、稳定传输数据已成为可能，这为无人机广泛应用提供了必要条件。同时，无人机作为飞行平台，其所搭载的各型设备相关技术不断发展，也极大拓展了其应用范围。

引领无人机发展的因素，一方面源于军事需求，从近年来爆发的俄乌冲突、巴以冲突，特别是中东战场哈马斯和胡塞武装依靠无人机“以小博大”，成功牵制美国和以色列，可以看出，无人机的出现和普及，已经改变现代战争形态。其中，小型察打一体无人机，不仅能够提供敌方目标实时坐标，引导炮兵远程攻击，还能对坦克等高价值目标进行直接攻击。大型远航重载无人机，携带高爆炸药，高空抵近敌防空圈，提升攻击成功率。另一方面源于市场推动，消费类无人机随着市场需求变化不断更新迭代，市场供需关系引领无人机生产企业向性能稳定、大载重、长续航、智能化等受消费者欢迎类型无人机的研发上投入资金，生产更多种类机载模块，推动相关技术迭代升级。

二、多方向拓展——无人机行业发展趋势

随着无人机技术不断发展，国内外新型无人机不断涌现。国内代表性的是具有200km/h以上飞行速度，机动灵活，第一视角操控的“穿越型无人机”；利用4G、5G信号，通过手机远程操控的“幽灵型无人机”；具备自主导航技术、抗干扰能力的“自主飞行无人机”；具有人脸识别功能、可自主寻找目标的“智能型无人机”；利用氢能源电池等新能源动力的“长航时无人机”。综合来看，现阶段无人机发展具备以下趋势和特点：

（一）飞控芯片集成化程度提高，算力增强

无人机飞行控制单元简称飞控，其本质为单片机，也就是简单的计算机，通过软件编程（固件烧写）控制无人机稳定飞行，同时接收各种指令，实现不同飞行动作。目前常见的消费级无人机飞控可以分为开源飞控和商业飞控。其中，开源飞控的最大特点是可以编写数据代码、修改程序，实现不同的飞行控制功能。随着飞控CPU主频的提升，无人机飞行稳定性增强，传感器接口增多，可实时规划路线并查看速度、高度等回传数据。例如穿越机F系列飞控，使用STM32芯片组，自2012年起共出现过4代产品，F1已退出市场，F3、F4、F7三代飞控分别发布于2014年，2015年、2017年，处理器运算速度分别为72MHz、168MHz、216MHz，F4有3个外接串口，F7扩展到5个，可以连接更多的外接设备。

（二）无人机飞行自主化、智能化水平不断提升

随着人工智能技术不断发展，智能算法开始大量应用于图像识别、目标分类、自主决策等领域。国外通过开展空战进化、进攻性蜂群等项目，发展具备自主飞行、近距离格斗、态势监控等能力的无人装备，减轻指

挥和操控人员任务负担。目前，APM、PIX 等部分开源飞控，通过地面站设定航向、航速、高度等数据参数，已经能够实现规划导航、自主飞行。国内民用无人机企业也将人工智能应用于无人机领域，如大疆公司精灵、御系列无人机，通过单一 2D 摄像头实现了手势自拍、视觉跟随、避障功能，同时大疆公司与微软正在合作开发能够识别包括水果等日常物品在内各种物体的智能无人机。

（三）无人机及搭载模块功能不断升级，高空高速长航时

随着科技的发展，无人机搭载模块也在不断升级，从单一摄像头，扩展到红外成像，再到能够分析作物和土壤状态，可用于禁毒工作的多光谱成像系统。无人机自身运动性能的提升一直是其设计制造者追求的目标，机身轻量化，电调、电池输出电量以及电机转速、扭矩的增加，例如，2024 年 2 月 28 日，红牛公司推出全球最快穿越机，仅需 4 秒就能达到 300 公里 / 小时，最高时速超过 350 公里 / 小时。机身轻量化设计、动力增加的同时，无人机电池续航能力也在不断提升，2014 年同济大学研制出我国第一架氢燃料电池固定翼无人机“飞跃一号”，连续飞行 6 小时，2020 年新研氢能研发的六旋翼无人机不间断飞行 331 分钟。

（四）仿生无人机逐步完善

仿生无人机是具备鸟类、昆虫外形结构，能够模仿鸟类、昆虫飞行的无人机，具备易携带、融入环境能力强、隐蔽的特点，是未来无人机研发的重要方向。美国麻省理工学院将微型导航技术、合成生物技术以及神经科学技术相结合，研发“蜻蜓”无人机，操作人员远程通过一个指甲大小的“背包”，产生电流刺激神经系统来控制昆虫肌肉，进而发号施令。我国西北工业大学研制的“信鸽”无人机，时速达 40 公里，可飞行 30 分钟，应用人工智能技术，该款无人机能够模仿真实鸽子 90% 以上的飞行动作。目前，仿生鸟类无人机已逐渐普及，网购平台售价千元左右，通过实飞测试，其已具备一定飞行稳定性，飞行距离尚可，但飞行状态与真实鸟类仍有一定区别。

三、多角度解析——无人机公共安全风险

近年来，无人机不仅在地形测绘、交通巡查、农田水利等领域大显身手，也在个人爱好者中掀起飞行热、航拍热。随着无人机广泛应用，“黑飞”“乱飞”事件逐年增多，暴露出严重的安全隐患和管理漏洞，给社会和谐稳定和公民人身安全构成威胁。

（一）无人机管理安全隐患漏洞

在众多“低慢小”目标中，无人机是受关注最多且最难管控的。一是无人机结构简单易组装、难监控。自组装无人机组成相对简单，结构原理为电池通过供电模块为飞控和电机供电，飞控接收遥控端指令，调节电机转速及舵机转动角度，控制飞机运动。由于组装无人机所需零部件可通过网络渠道购买，加之网上有大量组装教学视频课件，导致各类自组无人机大量出现，给监管带来极大困难。二是无人机操作系统易破解、难管理。无人机依托飞控系统程序设定，在卫星定位基础上，实现划定区域禁飞。无人机生产商如大疆、零度、极飞等依照民航局法律法规要求，在无人机自身模块中嵌入相关设置，实现禁飞区禁飞，有关部门对无人机自身设备识别码等进行了注册管理，但仍存在非法更改破解飞控系统，在禁飞区域违规飞行现象，仅北京市就发现多起破解大疆飞控

操作系统在中心城区违规飞行的案例。三是穿越机机动灵活易侵入、难防御。穿越机属于四旋翼无人机，其特点是机动灵活、加速快，最快飞行速度达到200公里/小时以上。随着穿越机遥控系统抗干扰能力增强、遥控距离增大，其活动空间将会越来越大，加之突防能力强，对复杂城市环境下的国家重点机关要地、重要设施等高价值安防目标构成现实威胁。四是无人机防区复杂易规避、难探测。相对于传统的载人飞机，无人机属于“低慢小”目标，受地形和环境限制小。在城市环境下，高楼林立，无人机在楼群中飞行，容易被各类建筑物遮挡，难以被发现。同时，其融入空域内复杂的电磁波环境中，更难以被探测。现有的雷达、无线电探测手段受城市楼群环境影响较大，雷达波易被楼群吸收反射，无法有效探测；无线电探测受到城市环境各类无线电波干扰，侦测效果受到影响；光电监控则存在楼宇遮挡现象，视野受限。五是改装机结构特殊易袭扰、难反制。一方面，消费类无人机，可以通过改装，实现高空抛投爆炸物，相关改装配件可通过网络渠道购买，增加了管控难度；另一方面，对于经特殊改装无人机，如通过加装惯性制导、图像识别模块、实现智能自主飞行无人机，加装光纤远距离遥控飞行无人机，改装小频点特殊频段遥控飞行无人机等，现有常规无线电反制手段效果一般。

（二）无人机对公共安全构成潜在风险

无人机如被不法分子利用，将会给公众隐私、财产、生命安全造成巨大威胁。一是实施恐怖袭击。无人机袭击具有隐蔽性、突然性强、袭击方式多样化等特点。无人机可以携带各种小型载荷，从空中投掷简易爆炸装置、手榴弹等爆炸物，喷洒毒气、易燃物、腐蚀性水剂等核生化类有害物质，具有巨大恐怖威胁。2018年8月，委内瑞拉总统在发表讲话时遭到无人机袭击，导致多名军人受伤；2021年11月，伊拉克总理官邸遭无人机袭击，6名保镖受伤。二是扰乱社会秩序。日常生活中，无人机的无序飞行会对社会公共秩序造成威胁，例如无人机会对飞行中的飞机造成异物损害，导致空域或跑道禁用；无人机射频辐射会干扰无线通信系统；无人机的出现会干扰室外重大活动，干扰救援、执法人员的紧急飞行操作等。除此之外，世界各地也频繁发生无人机投递非法物品、作为中继平台开展网络攻击等非法行为，对社会造成了重大安全隐患。三是进行非法监控。由于无人机便携性高、操作简单，并能够携带复杂传感器，因此最常用于监控和侦察。此外，无人机还可以搭载投放小型传感器，对较为广阔的区域进行持续监控。这些特性使得无人机适用于各种非法监控和侦察活动，包括个人隐私窥探、工业间谍活动、非法收集国防情报等。四是实施非法运输。无人机在飞行中，除承载自身重量外还具备一定载重能力，可以突破传统技防、物防设施运送违禁品。利用无人机运送毒品、手机或其他违禁品进入监狱等安全场所屡见不鲜，毒贩已经将其作为跨境运输毒品的新手段。

四、多渠道融合——无人机侦测指挥系统

反制系统对无人机进行有效反制的前提，是能够精确侦测到来袭无人机，并进行系统决策。一套成熟的无人机侦测指挥系统，应当包括雷达、光电、无线电等前端侦测设备，以及收到侦测设备信息后对其进行分析、梳理、研判，作出指令实施反制的指挥系统。

无人机反制过程中，知道袭扰无人机在哪里是第一阶段目标，进行智能分析决策是第二阶段目标，末端实施有效反制打击是第三阶段目标。

（一）无人机探测技术

一是雷达探测。雷达具备探测距离远，可测量飞行目标速度、方位和高度信息，全天候工作等优点，缺点是难以探测悬停或超慢速逼近的目标，对未知雷达截面的无人机难以识别，存在固有探测盲区。有源雷达对人体辐射较强，无源雷达受电磁环境影响大。雷达的布设方式也至关重要，应根据不同环境地貌，调整部署位置方向。

二是光电探测。光学探测设备，包括可见光和红外探测两种。可见光探测，探测设备应具有较大的放大倍率和较为充裕的视场，能够自动调整焦距和光圈，跟踪捕获移动目标。红外探测技术，其优势在于可无源接收热辐射信号，能够在夜间使用，缺点是容易受到其它热源的干扰。

三是无线电信号探测。无线电信号探测系统，是一种被动接收式的侦测系统，本身不发射任何电磁波信号，其原理为通过接收空中的电磁波，检测其中是否存在无人机与遥控器之间的通讯信号来判断是否有目标存在。此类无源侦测设备探测距离远，可全天候无人值守，适用于人口密集的城市环境。缺点是城市复杂电磁环境下虚警率高，高度测量精度较差。

四是声波探测。声学检测是通过声音特征确定无人机的存在和方位，同时也可发现枪械射击产生的声音。声学探测装置通过收集无人机螺旋桨声音数据，与后台数据库声音数据特征比对，确定声音是否来自无人机，并在识别的同时进行跟踪。声学探测容易被周边噪音所干扰，具有很大局限性，一线工作中并不常用。

五是利用 4G、5G 网络信号被动探测追踪无人机。基本原理为通过接收公网 4G、5G 毫米波信号在无人机上的反射信号，识别城市环境中的“黑飞”小型无人机，该技术类似于雷达侦测接收技术，为被动探测，不会造成无线电干扰，目前属于前沿领域，处于测试论证阶段，并未大规模应用。

（二）确定空间实时移动坐标点

对无人机进行有效侦测是进行反制的前提和基础，其直接目的，是发现一个或多个袭扰无人机，并得到实时三维空间坐标点。无人机飞行速度快，对其侦测具有时效性，需快速锁定。实战中，如某型侦测设备发现附近区域出现入侵无人机，得到实时三维坐标以及飞行速度等数据，中控系统聚焦该区域，利用先期发现坐标点，引导其它侦测设备对该区域进行精确探测，验证袭扰无人机，不同侦测设备通过内置算法同步更新实时坐标，形成时空轨迹，做到“单一感知，多方侦测”。实现这一目标的前提：一是侦测设备与指挥控制系统底层数据融通，二是数据传输没有延时或低延时，三是具备三维空间模拟数据模型，四是设定算法与相应阈值，通过融合不同侦测设备数据确定相对精确空间坐标点。

雷达、光电、无线电等常规侦测手段各有优缺点，需设定算法有效整合前端不同侦测设备提供数据，得到精确坐标点。同时，关注 4G、5G 信号波探测，街面摄像头图像识别等无人机侦测新方法、新技术，不断丰富侦测手段。

（三）分析提炼相关信息数据

在发现、确认袭扰无人机，并得到相对准确的实时空间坐标点后，中控指挥系统要结合后台白名单，综合能见度、风速、周边

要害建筑分布等基础信息，分析提炼相关数据进行研判，为下一步行动做准备。例如通过轨迹航线初步判断无人机袭击目标区域或目标建筑，通过风向风速判定气球等空飘物行进路线以及是否经过敏感地区等。中控指挥系统应通过现有数据自动快速分析出以下几类信息：一是通过图像识别、雷达波反射等手段，分析来袭无人机数量、大小、类型、载重量等客观信息。二是通过无人机或空飘物飞行速度、轨迹航线，分析其起飞施放区域、袭击目标、袭击发生时间。三是结合无人机飞行高度、速度、变轨特性、拟袭击目标等因素，判定无人机威胁程度。四是对袭扰无人机飞行航线、高度、速度变化进行预判，得到下一时段模拟飞行轨迹，分析可能出现的情况，通知现场指挥人员，为下一步实施反制提供方案预案。

（四）平台整合数据辅助现场决策

无人机反制指挥平台相当于无人机侦测反制系统的“大脑”，是接收侦测设备信息并做出分析判断、指挥反制装备进行策略反制的综合系统，其组成包括工作人员、软件平台、决策模型等。根据分工不同，人员组成应包括侦测组、反制组、指挥组、气象组、调度组等。软件平台是指挥平台的核心组成部分，连接前端侦测反制设备，其操作主界面应包括可加载不同图层，并实时显示无人机侦测情况的平面地图，以及操作控制界面。在平面地图上，使用人员可通过加载不同图层看到不同信息，包括袭扰无人机实时位置、重要警卫目标点位、侦测设备点位及范围、反制设备点位及范围、反制巡逻机动力量实时位置、民航客机实时飞行路线等图层。不同小组及席位可观看图层及开启侦测、反制设备权限不同，根据授权可在软件设置界面勾选叠加不同图层信息。

公安机关无人机反制指挥平台监控目标多为低空、短距离、突袭无人机，飞行时间短、速度快。应对此类空情，须保持通信链路畅通，确保指挥人员能够准确掌握袭扰无人机实时飞行动态，指挥控制系统结合前端设备反馈信息，通过决策模型进行自动化、智能化空情处置。决策模型进行反制决策过程中，一是设定不同防御圈层，设置白名单，外围防御圈发现无人机进行先期预警反制，核心防御圈层禁止一切飞行器进入，启用反制措施强度逐级增加。二是分析提炼相关数据信息，针对无人机袭扰目标、可能方向、模拟轨迹、威胁级别，做出分析判断，将相关情况反馈现场指挥人员。三是做出应对措施，启动反制阵地，指挥附近反制力量进行现场机动反制，通知相关部门降低次生灾害风险。四是平台最重要的作用是做出正确有效的应对措施，在探索实践无人机反制自动化、智能化的同时，更应重视人员配合以达到最佳效果。

五、多手段并用——无人机反制综合体系

无人机反制是建立在前期对无人机有效探测基础上的后续工作，主要包括“软杀伤”和“硬杀伤”两类反制手段。“软杀伤”是指无线电干扰、导航欺骗等反制方式，“硬杀伤”主要包括激光、网捕、撞击等反制方式。随着无人机智能化水平提升，其自主飞行能力逐步增强，在一线无人机反制安保工作中，要想确保核心目标绝对安全，应重视“硬杀伤”反制手段，同时各反制单元要联动协作发挥最大效能，实现团队效应。

（一）无人机反制技术

一是无线电干扰。优点是无附带损伤，

易于部署，可全天候无人值守。缺点是对干扰频段外的无人机无效果，采用全频全向的干扰方式会影响周边通讯设备正常工作。采用定向和频谱识别干扰方式，对侦测设备和干扰设备的性能有较高要求。

二是导航欺骗。对无人机定位系统进行干扰，优点是无附带损伤，功率小，可长时间全天候无人值守工作，部署使用简单，可用于多目标防御。缺点是产生次生灾害，对周边导航应用设备有影响，特别是对民航客机导航系统影响很大，易造成安全事故。

三是高能微波。高能微波主要用于毁伤雷达、预警机和无人机上的电子设备，具有攻击速度快、使用成本低、全天候适用等优点，打击效率高、效果好，对无人机群攻击具有较好的反制效果。缺点是对人体及电子设备存在较强的电磁辐射附带损伤。

四是激光打击。激光反制设备，对光电跟踪系统跟踪锁定能力要求高，优点是拦截目标类型多，效果好，成本低，是重要的技术发展方向。缺点是设备造价高硬杀伤、受环境影响大，具有一定危险性，在人员密集场所使用具有局限性，对于有防护措施或金属机身无人机反制能力有限。

五是网捕技术。网捕技术，是通过无人机携带网枪，高空发射网捕弹药，或地面人员操纵网枪发射网捕弹药拦截无人机的反制技术。优点是反制成本低，次生灾害较小，但技术难度较高，需将反制系统与雷达探测、光电定位、自动控制等技术结合应用。

六是物理撞击。主要有无人机（穿越机）撞击、动能弹密集打击等方式。动能弹密集打击方式对现场人员、建筑和设施存在附带损伤风险，经过一定距离后弹药会发散，攻击效率有限。无人机撞击方式对于反制无人机的飞行速度、机动灵活性及飞手的操控能力要求极高，需要进行针对性训练和技术、战术研究。

七是弹药毁伤。使用狙击枪、霰弹枪、密集阵火力系统或小型导弹，对无人机进行反制，此类攻击方式多用于军事领域无人机反制，次生灾害影响较大，不适宜城市环境下要地防御或重大活动等人员密集场所。

（二）系统化无人机反制体系

无人机系统化反制是在对入侵无人机进行有效侦测及分析基础上，无人机反制指挥控制平台进行自动化、智能化反制，各反制单元按照指挥平台制定的反制方案执行反制任务。实现系统化反制，应充分利用反制指挥平台提供的无延时空情信息，采用技术手段，消除各反制装备之间的相互干扰，有效执行多轮次多设备反制预案流程。

一是充分利用反制平台提供数据信息。一线指挥人员及反制设备要有效使用反制指挥平台提供的无人机大小、种类、速度、实时三维坐标、预判飞行轨迹等数据信息，引导网捕穿越机飞手通过实时三维坐标提前到达指定区域，追击或阻截入侵无人机，无线电定向反制设备实施精准定向干扰，巡逻车组携带反制装备提前到达点位开启反制设备，进行移动拦截。

二是消除不同反制设备间干扰。由于反制原理不同，部分反制设备工作时会产生相互干扰，不能发挥最大效能，例如无线电反制会影响网捕穿越机实施空中拦截，激光打击也存在误伤网捕穿越机可能。为有效发挥反制设备最大效能，应从技术和反制流程上，消除设备间相互干扰。技术层面，无线电反制设备进行信号干扰压制时应留出特殊信号频段供网捕穿越机使用，同时增大穿越机信号传输强度或采用特殊跳频扩频方法，增强抗干扰能力。反制流程上，错峰使用网捕穿

越机、无线电干扰、激光打击设备，避免同时使用造成互相干扰。

三是多种装备多轮次实施反制。在侦测到袭扰无人机后，单一反制手段可能对目标不能实施有效反制。无人机反制是一个需要实时监测，多种侦测、反制装备协同配合，进行多轮次反制的动态过程，明确反制策略与反制时序，多装备多手段同时或有序实施反制。目前，较为常用的反制策略是以无线电干扰、压制为常规手段，激光打击、网捕穿越机拦截为保底手段，进行多装备协同配合反制。在反制的同时，指挥平台应对袭扰无人机进行实时监测，观察其是否被有效反制以及飞行状态是否变化，对相关数据进行分析，指挥反制设备进行调整或通知相关单位采取必要应急措施。

四是重视硬杀伤反制方法。随着无人机向智能化方向发展，越来越多无人机具备自主飞行功能，其信号中断后，可以按照设定好的程序自动追踪抵近目标，完成既定任务，如大疆等机型的自动返航、环绕摄影、跟踪拍摄、光流定位等。因此在采取无线电反制等“软杀伤”反制方法的同时，应重视“硬杀伤”手段。图像（雷达引导光电）追踪识别技术，涉及计算机视觉与机电控制技术，对芯片运算能力要求较高，为“硬杀伤”不可或缺手段。区域拒止技术应用的典型案例为反导导弹发射后在某一空间区域内自爆，形成破片带，对来袭导弹实施破片拦截。无人机飞行速度快、目标小，进行精准撞击或枪械狙击难度极大，在有效规避次生灾害基础上，对来袭无人机进行轨迹预判，采取空对空或地对空方式，发射特殊“弹药”在某一区域实施大范围物理反制是较为可行有效的方法。

六、多管道齐下——无人机技术情报体系

随着科学技术不断进步，无人机应用及反制相关技术也在不断发展。紧跟时代潮流，关注人工智能、通讯传输、复合材料等领域最新进展，做好基础调研，开展对抗测试，是做好无人机应用及反制工作的重要基础。

（一）关注最新侦测反制技术及装备发展趋势

一是关注军事领域无人机侦测反制装备应用与实战效能；二是关注国内最新型号无人机侦测反制设备的应用；三是关注国内外前沿侦测反制设备及技术最新进展；四是关注激光打击、空对空智能网捕等前沿侦测反制技术及装备最新进展。

（二）跟进梳理无人机军事实战应用、恐怖袭击案例

一方面，收集无人机及自组装无人机在军事实战中的应用，梳理无人机实施恐怖袭击案例；另一方面，归纳总结军事战争中无人机使用发展方向，复盘恐怖袭击过程，复原战争以及恐怖袭击中投入实战的改装、自组无人机，还原战争、恐袭中战术战法，建立靶机库，进行对抗演练测试，形成实验数据。

（三）调研现有条件下民用消费类无人机现实威胁

一是调研大疆、道通等主流消费类无人机改装技术手段，包括但不限于破解系统软件实现禁飞区飞行、加装抛投器等，对其可行性进行验证；二是调研通过网络渠道购买配件自组装无人机相关技术，对自组装无人机稳定性、载重、续航、速度等性能技术参数进行实验验证；三是关注国内外无人机技术论坛，对其发布无人机刷机、改装案例及

教程，进行可行性验证，必要可联合有关部门封锁相关信息。

（四）调研特殊种类无人机现实威胁

主要针对高速、重载、远航、自主导航类，突防能力强、威胁大的无人机。其中，高速机关注涡喷、四旋翼、碳纤维结构固定翼等机型；重载机关注升力体、宽翼面固定翼、多旋翼等机型；远航机，一方面关注大功率传输、卫星通讯、4G 模块等远距离信号传输技术，另一方面关注油动、氢混电池等长续航技术研发与应用；自主导航机关注卫星制导、激光制导、惯性制导、图像识别自主导航等技术。关注光纤遥控类反无线干扰无人机，以及蜂群无人机相关技术发展及最新应用案例。

（五）关注无人机与新技术融合

新技术的出现，初期由于各种客观因素限制，不能广泛应用，然而，随着产品迭代，技术瓶颈不断被突破，新技术可能带来新变革，对原有技术实现“降维打击”，需要格外关注。无人机涉及前沿技术包括离子推进、人工智能、3D 打印等。

（六）关注无人机搭载模块发展趋势

无人机作为载体，其功能主要依靠搭载平台实现。一方面，针对无人机实施暴恐袭击，需对其搭载爆炸装置（或核生化制剂）、枪械进行袭击的可行性、可操作性进行实验验证，关注相关案例，摸索应对措施；另一方面，围绕警用无人机相关功能需求，关注搭载模块红外成像、光谱分析、智能识别等技术最新进展。

（七）建立技术信息数据库

一是收集整理常见商用消费类无人机飞行原理、重量、最大飞行速度、载重量等参数数据；二是对自组装无人机所需电机、电调、飞控等配件参数进行收集整理；三是通过实飞测试，归纳总结不同种类无人机光电识别、雷达反射以及飞行轨迹路线特点，并与鸟类进行区别，形成数据库，用以智能辨别无人机；四是对市面常见无人机图像传输及遥控接收无线电信号频谱等相关数据进行收集，建立数据库；五是对不同种类无人机载重能力、极限速度、雷达反射面积、信号传输距离、最远飞行距离进行测试，摸清各类型无人机实际飞行能力；六是使用现有反制设备，对各类型无人机，特别是大功率信号传输、搭载 4G 模块等经改装的特殊类型无人机进行反制测试，记录实验数据。

参考文献：

[1]周钰婷、郑健壮．全球无人机产业：现状与趋势 [J]. 经济研究导刊．2016．26

[2]李光．无人机的发展现状与趋势 [J]. 现代工业经济和信息化．2021．3

[3]阮晓东．无人机角色：从消费级到工业级 [J]. 新经济导刊．2016．8

[4]钟柱梁、李庭威、陈嵘杰、刘立程、王峰．军用无人机现状及发展趋势 [J]. 电脑知识与技术．2018．14

[5]张君．无人机技术和应用发展与监管研究 [J]. 现代电信科技．2016．3

[6]石红梅、谭晃．国外无人机监管及反制技术最新发展概况 [J]. 中国安防．2016．4

[7]孙泽梁．新形势下民用无人机恐怖袭击特征及防控对策探析 [J]. 北京警察学院学报．2020．2

[8]吴赛．无人机恐怖袭击威胁的特点与应对 [J]. 广西警察学院学报．2020．33

[9]黄璇、沈鸿平、彭琦．低慢小无人机监测与反制技术对比分析 [J]. 飞航导弹．2020．9

[10]张珣、唐艳、罗士伟．国外无人机反制系统发展概况 [J]. 电波卫士．2023．3

[11]马雯．反无人机技术发展研究 [J]. 航空兵器．2020．6

[12]吴小松、房之军、陈通海．民用无人机反制技术研究 [J]. 中国无线电．2018．3

[13]齐鹏文、施志刚、郭培恒、马乐、石岩．基于无线电的“低慢小”无人机反制技术研究 [C]. 全国信号和智能信息处理与应用学术会议．2021

[14]范殿梁、邱日祥、李扬．无人机反制技术研究 —基于导航欺骗技术的无人机干扰拦截系统 [J]. 中国安全防范认证．2016．6

[15]柳强、何明．海上小型无人机集群的反制装备需求与应对之策研究 [J]. 军事运筹与系统工程．2021．4

责任编辑 徐闻彬