未来信息化战场对参战官兵的作战能力提出了新的更高要求，单纯依靠现有的训练方式显然难以满足需求。目前，美国陆军与微软公司签订总价值4.8亿美元合同，旨在采购10万套增强现实眼镜，用来为美军下一步开展沉浸式军事训练提供支持。与此同时，美国陆军实验室也联合多家创新技术研究所，着力研究沉浸式技术对军事训练和战场作战的应用价值。

沉浸式军事训练系统能为参训者提供一个逼真的战场虚拟环境，士兵可完全沉浸其中开展训练，从而最大限度贴近实战，在提升训练效益的同时，还能减少训练伤并节省训练费用。目前，世界各军事大国都已认识到沉浸式技术在军事领域的巨大潜力，通过完善虚拟训练系统不断提升作战能力。

沉浸式技术——让未来战场扑面而来

■张瑷敏 张玉民

高技术前沿

虚拟战场触手可及

近年来，伴随着云计算、大数据、人工智能等技术的快速发展，军事仿真也逐渐驶入发展“快车道”，在装备建设、军事演习、作战训练与后勤保障等领域相继取得重要进展。尤其是近年来虚拟现实和增强现实技术的快速发展，能将计算机生成的虚拟图像实时、动态地融合到人体所能感知到的真实环境中。这样的技术一旦应用于军事训练，势必打造出一个能让士兵身临其境的虚拟战场空间。

沉浸式技术正是虚拟现实和增强现实技术发展的最新成果。借助头盔式或盔甲式显示设备，沉浸式技术能将用户的视觉和听觉封闭起来，产生虚拟的视听效果。同时，沉浸式技术借助数据手套为用户提供虚拟的触觉感官，通过语音识别器为用户提供一个可以替代真实环境的理想模型。美军目前正在研发的“士兵构建情报系统”训练保障项目，就是想通过提供设备、模拟器与仿真建模等服务，更好地辅助开展军事情报训练。

与传统的静态沙盘和作战地图相比，沉浸式军事训练系统不受场地限制，能在参战官兵眼前呈现出包含网络、电磁等跨空间的立体动态场景，从而提供一种身临其境的“现场感”。以沉浸式数字单兵虚拟体验系统为例，它能为士兵提供包含山地、丛林、沙漠等场景在内的沉浸式虚拟战场环境，参加训练的士兵只需携带各种传感设备，选择不同的战场环境和任务方案，就能在系统中体验到实战训练的效果。在这样的沉浸式训练系统中，导调人员同样可以临机设置不同的战场环境和突发情况，训练结束后回放观察训练过程，从而推动军事训练向实战化和信息化靠拢。

军事训练安全高效

沉浸式军事训练在提升训练效果的同时，还能有效避免训练伤亡，同时节省训练费用。专家预测，伴随着沉浸式技术快速发展，未来5到10年，沉浸式军事训练比重将大幅增加。近年来，美国已先后研发出数款沉浸式军事训练仿真系统，助推了美军军事训练的高效实施。

构建虚拟战场环境。通过对具体战场环境、战术背景和敌方兵力进行模拟仿真，沉浸式军事训练能为参训人员提供更为逼真的战场感受，军事背景、战地场景、武器装备和参战人员等全部包含其中，演习将越来越接近实战。美国海军专门开发出一款“虚拟舰艇作战指挥中心”，能逼真模拟舰艇作战指挥环境，提供生动的视觉、听觉和触觉效果。加拿大军队也通过沉浸式技术组织过模拟训练演习。2014年，美军公开展示了“增强现实沙盘”系统，通过直观反映战场真实地形地貌，使作战人员身临其境了解战场地形。

锤炼单兵技战素养。对于在2002年就推出过单兵训练游戏的美军而言，沉浸式军事训练系统并非新鲜事物。美国耗费巨资开发的“陆军步兵训练系统”，是近年来首个投入使用的沉浸式训练系统。该系统允许9名士兵同时参与训练，包括可穿戴计算机、人体传感器、具备光学瞄准镜的仿真武器等，能提供山地、丛林和沙漠等战场环境，如同在真实训练场上一般使用各类枪支弹药。由于该系统能对作战人员进行同一作战环境、同一作战任务的反复演练，从而大幅提高了训练效果。美军组织实施的“军官虚拟现实教程”则专门用来训练作战指挥人员，仅需5个月的沉浸式训练，就能初步培训出具有战术专家素质的指挥官。

实施联合作战训练。借助沉浸式军事训练系统，还可实现不同地域和环境下各兵种的联合作战训练。美国陆军的“近战战术训练系统”就采用了分布式交互仿真技术，建立起一个复杂的虚拟作战环境。作为沉浸式协作分析研究的一部分，美国陆军实验室推出的“混合现实战术分析工具包”，能通过仿真战术作战中心，为各军兵种指挥官和情报分析人员提供不受地理条件制约的沟通和协作环境，将加速实现联合战场关键信息的可视化仿真训练。

战场应用潜力巨大

当然，沉浸式军事训练系统也并非完美无缺，目前仍有许多亟待解决的技术问题。譬如，使用沉浸式仿真环境的各类显示器，不可避免地会产生模拟器眩晕症，对实施驾驶、武器操作等训练会产生不利影响。同时，现有的沉浸式军事训练系统大多关注对物理地形等战场环境的建模仿真，人文地形的建模仿真同样是未来军事训练虚拟仿真的重点领域。只是由于技术原因，目前尚未达到可以应用的程度。

事实上，开展沉浸式军事训练并非要取代真实训练，而是尽可能利用技术发展，提高训练效费比，进而实现战斗力的整体提升。未来信息化战争是陆、海、空、天、电、网多维空间同时展开的一体化战争，战役结构复杂、武器装备多样，对参战人员素质及其战法都提出了更高要求。借助沉浸式军事训练构建出虚拟战场，有利于让指挥员对未来战争提前具有感性认知，在战争开始之前做到“胸有成竹”。

沉浸式军事训练系统的使用，不仅能提高军事训练效益，还有可能启发新的作战思维。目前，美国陆军已计划通过沉浸式军事训练打造一个拥有“虚拟战场”的国家仿真中心。英国、法国、德国等多个国家开始使用“虚拟战场”软件，并通过软件迭代更新加速训法战法升级。英国和阿联酋等国还积极借助沉浸式技术服务征兵工作，为想参军入伍的年轻人提供虚拟战场体验。

沉浸式技术同样可应用于武器装备维修和战地医疗救护。维修人员能借助沉浸式虚拟现实系统提升装备维修的熟练程度，美国洛马公司目前就通过使用智能眼镜加速F-22和F-35战机维修速度。维修人员能通过眼镜看到投影于战斗机上的零件编号，从而减少维修错误。

制图：李 涛

科技云

科技连着你我他

微型无人攻击机引发战场新变化

■张德群 邱滨咏亮

在不久前结束的阿布扎比国际防务展上，以制造AK系列自动步枪闻名的俄罗斯卡拉什尼科夫公司，公布了一款已通过测试并即将投入使用的微型无人攻击机，引起广泛关注。据公开资料显示，该型无人机飞行速度80至130千米/小时，有效载荷3千克，续航时间30分钟，可通过自杀式行为精确打击60千米以外的目标，无论是续航能力还是攻击性能，均远超同类无人机。

微型无人攻击机公开亮相，预示着无人机发展的一大重要趋势，研制和拥有大量微型无人攻击机将成为一种潮流。随着大量新技术的广泛应用，微型无人攻击机的各项性能指标将会持续提升，未来如果得到大规模应用，或将引发信息化战场的革命性变化。

微型无人攻击机可能成为未来单兵装备的新标配。微型无人攻击机结构简单、便于携带、易于操作，不需要跑道和特殊的发射轨道，根据需要能随时随地发射，能像发射小型巡航导弹一样对目标发起精确打击。较当前有效射程不超过几千米的枪支而言，微型无人攻击机显然有极大优势，会更受单兵青睐。未来战场上，单兵携带数架微型无人攻击机，会像现在携带枪支一样普遍，单兵打击武器有望实现真正的远程化、精确化和立体化。

微型无人攻击机可能成为非接触精确打击的新方式。微型无人攻击机体积小、噪声低，隐身性能好、打击精度高，以低空、超低空快速飞行极易突破传统的防空体系，借助人工智能技术可以更精准地识别、锁定重要人物以及装甲装备、指挥中枢等要害目标。无论目标所处何种地貌、地形，微型无人攻击机都可直接奔袭目标，或按指令与其他无人、有人力量协同，对目标实施蜂群作战和饱和式攻击。

微型无人攻击机可能成为威胁空防安全的新课题。一方面，微型无人攻击机造价低廉，技术门槛和使用门槛不高，军人和平民、战时和平时使用的界线更趋模糊。另一方面，近年来反无人机技术虽然取得长足进步，但对微型无人攻击机尚不能实现有效拦截。恐怖分子可能利用微型无人攻击机对重要目标或重大活动实施自杀式恶意攻击，达成扰乱社会运行秩序、影响政局安全稳定的目的。这将成为构建国家空防安全体系面临的新课题。

维护网络空间安全刻不容缓

■朱 丰 吴永亮

论 见

3月7日，委内瑞拉电网遭受网络攻击，境内多个州和首都加拉加斯电力系统陷入瘫痪，国内主要交通、医疗、银行、金融、供水、通信等基础设施受到严重影响。世界舆论普遍认为，这是攻击方从网络空间发起的一次大规模突袭，破坏效果远超传统战争中的火力毁伤。充分认清这起事件的警示作用，对我们加速推动网络安全建设同样具有重要意义。

一是网络攻击已成为谋求对抗优势的常用手段，应聚力提升网络攻防能力，争取网络空间安全主动权。纵观美震网病毒攻击伊朗核设施、俄为配合地面作战对格鲁吉亚进行网络封锁等多起网络攻击事件，当今世界军事大国对网络攻击手段的使用越发频繁，甚至成为优先选用的作战手段。这启示我们，必须在深刻剖析网络空间作战规律基础上，不断提升网络安全防护能力，争取在网络安全技术领域“弯道超车”，赢得未来与作战对手的网络空间对抗优势。

二是网络空间作战准备是赢得对抗优势的必备条件，应合理借鉴他国经验做法，超前筹划准备，谨防被敌突袭。分析此次事件的深层原因，是攻击方事前做了大量的网络空间技术准备和针对性的网络攻防演练。为防止类似事件重演，应加快关键基础设施网络防护能力建设，定期组织国家层面的网络防护演练，全面提升网络安全应急处置能力。

三是网络空间行为准则是规约网络行为的法理依据，应力争相关国际条约制定的话语权，维护公平正义的网络安全环境。从对手发起网络攻击造成国家和民众严重损失却无需承担相应法律责任后果来看，现行的网络攻击行为没有受到相关国际法律准则的有效约束，基本处于零管控状态。为预防此类网络攻击行为的发生，必须呼吁国际社会加速推进网络空间国际行为法律准则出台，限制网络攻击行为滥用，最大限度避免网络空间战争灾难，使网络空间更好地造福人类。

波音飞机失事暴露智能软件设计缺陷

机器权限不能超越人类控制

■顾静超 刘海波

热点追踪

当地时间3月10日上午，一架从埃塞俄比亚飞往肯尼亚的飞机坠毁，机组人员及乘客共157人全部遇难。失事飞机为波音“737MAX-8”型客机，这已是该型飞机继印尼狮航2018年10月29日坠毁事故后，在5个月内的第2次失事。

初步分析，事故缘于空速管对飞机飞行状态探测错误，机载“防失速系统”（MCAS）自动控制飞机完成了俯冲，暴露出智能化软件设计存在的缺陷。

未来智能化作战中，人类会赋予作战系统一定权限，允许智能化系统在特定作战背景、作战条件下，满足规定的范围、条件或规则即可自主决策，实施机动、攻击、防护等战斗行动。但是波音“737MAX-8”事故警示我们，无论计算机系统的智能决策系统如何先进，它的权限赋值应该始终低于人。

首先，建立人机互信，要增强智能化系统对操作人员通过脑波意识、语音指令、手动操作等多途径传达的意图的理解，使得机器与人类形成目标的相同认知，在此基础上才能赋予智能化作战的相关赋权。其次，允许行动终止。一旦出现人与机器的冲突，或智能系统之间的相互冲突，必须允许人能及时进行干预、纠正或终止智能系统的行动。最后，突出人的最高赋权。系统逻辑中，如果多个智能系统相互冲突，必须将对人的信任度置于最顶层，必须交由人而非单个系统裁决冲突、解决矛盾；如果人与智能系统发生冲突，智能系统必须无条件服从人发出的指令。这样，才能保证智能化系统的可信、可靠、可用，避免悲剧的发生。