

聚焦外军新域新质

人工智能重塑现代战争指挥保障体系

■李建平 纪凤珠

瞭望台

不久前,美国空军在内利斯空军基地“影子作战中心”举行第5次“人机协同决策优势冲刺”实验。实验模拟真实作战场景,重点检验人工智能在高对抗作战环境中处理海量战场数据、生成行动建议以及辅助指挥决策的能力。

这一动向,是人工智能深度嵌入战争进程的典型缩影。近年来,随着相关技术加速迭代,人工智能已从作战辅助工具跃升为指挥保障体系的核心赋能引擎。无论是在俄乌冲突还是巴以冲突,智能侦察、辅助决策、自主规划等能力均在实战中展现显著效能,并对战场态势产生直接影响。现代战争指挥保障体系的运行逻辑正在经历深刻变革。

智能融合感知,重塑全域情报保障生成链路

情报保障是指挥保障体系的前端核心,也是指挥员进行决策的依托。情报处理与分发效率,直接决定战场杀伤链的闭环速度。长期以来,多渠道情报分散存储、人工筛选研判效率低下,制约着情报保障效能。人工智能的引入,则可打破这一瓶颈,重塑情报保障生成链路。其不仅能对各类战场数据实时融合归集,还可自动进行真伪甄别和目标威胁分级,大幅压缩情报响应周期。

这一变革在俄乌冲突中得到充分印证。乌军“Delta”系统融合无人机侦察、卫星侦察、开源网络情报等多源数据,依托云台进行实时处理,生成统一态势图。有报道称,北约“刺猬2025”演习中,一支仅10人的乌克兰无人机小队借助该系统,在模拟对抗中击败北约两个步兵营。俄罗斯也推出一款名为“Svod”的新型指挥控制系统,该系统服务于战术层级,可将无人系统、卫星及其他情报源数据整合到共享作战图中,优化兵种间的协同。

以色列更加注重人工智能在精准打击中的深度应用。据报道,以方曾提前数年侵入伊朗交通监控网络,借助人工智能模型分析相关视频资料,逐步掌握伊朗部分官员的行动轨迹与生活规律,为精准斩首行动提供关键情报支撑。在加沙,以色列运用“薰衣草”等系统,基于通信记录、社会关系与行为轨迹对疑似武装人员进行自动化评估并生成打击清单。这种算法驱动的目标选择模式因误伤平民的风险引发极大争议。

美军则从“单点算法”转向“智能体+数据平台+大模型”的体系化部署。美国国防部推动“GenAI.mil”项目,在不同密级环境中为情报分析、图像视频判读、文书综合提供生成式能

力。2026年,美军宣布启动“智能体网络”项目,并将其列为《人工智能加速战略》框架下第二个“标杆项目”。其中,美国情报企业Dataminr推出的First Alert Advanced系统可利用智能体自主分析公开情报源,目前该系统已集成进美军Maven指控平台。

算法辅助决策,重塑人机协同指挥模式

指挥决策是指挥保障体系的中枢。传统作战主要依靠指挥员个人经验研判,参谋团队人工推演筹划,面对多域战场海量作战数据时,极易出现算力供给不足、跨军种协同壁垒突出、指挥人员负荷过载等问题。当前,多国军队正推动搭建“AI辅助推演、人类最终定夺”的混合指挥架构,力图以算法重构指挥决策运行机制。

俄乌冲突中,乌军运用GIS Arta系统,自主生成多套反击作战方案,自动排查兵力部署盲区和行动执行漏洞,优化一线临机处置流程。2026年乌军推出的Marichka决策支持系统,可与“Delta”情报分析系统协同,自动测算兵力装备对比、标注作战资源和潜在战损,并在交互地图上生成多套行动方案。此举有效压缩了旅团级部队方案筹划用时,指挥官则依然保留对作战目标、时机和兵力使用的决定权。

北约也在推进空中指挥体系智能化进程。近期,北约通信与信息局宣布,对美国安杜里尔国防科技公司开发的Lattice平台,展开为期9个月的测试,评估其能否作为北约成员国共享空战信息的新一代指挥平台。该平台采用人工智能驱动,可实现对威胁的自主检测、分类、跟踪与优先级排序,大幅缩短人工操作员的威胁识别时间。

值得警惕的是,日本也在试图为自卫队配备“AI参谋”。今年3月,日本防卫装备厅委托富士通研发“多AI智能体”系统。该系统可通过多个智能体协同自主生成结论,从而助力指挥官进行决策。该项目预算约1亿日元,计划于2028年前完成。此外,日本还计划引入美国企业提供的人工智能系统,辅助国产系统共同提高指挥控制中的信息处理和决策支援效率。

跨域智能调控,重塑火力打击协同保障形态

火力打击协同保障是指挥保障体系落地的末端环节,直接决定指挥意图向实战杀伤效能转化的上限。传统火力保障逐层逐级下发指令,运用单一平台一对一人工操控,力量调度流程繁

琐、多单元协同存在明显滞后性。人工智能将标准化作战规则前置植入各类作战平台,实现作战调度从“逐层逐级传递指令”向“无人集群自主协同、战损动态智能补位”转变。

俄乌冲突中,双方大量运用无人作战平台,智能化协同保障的实战价值得到充分彰显。其中,俄军“天竺葵-2”巡飞弹、“柳叶刀”攻击无人机搭载机载AI识别模块,指挥人员仅需划定作战空域、设置行动约束条件,无人集群便可自主巡航、自主索敌、自主发起攻击,大幅降低人力资源的投入。“蛛网”行动中,乌克兰运用AI技术实现上百架无人机远距离协同作战,实现对俄军重要战略资产的非对称打击。

在加沙地带,以军投入“美洲豹”半自动机器人,由AI集中调度管控,承担侦察、排爆等高危作战任务;空中无人集群依靠智能空域分配算法划分活动区域,规避火力交叉冲突。在巴以冲突中,美军AMORPHOUS系统同步统筹不同型号无人机,摆脱大型载具载体约束,分布式执行侦察、干扰、打击多类型任务。

欧洲国家也在加速推进相关技术运用。其中,法国推动无人机蜂群与“阵风”战斗机协同作战试验,探索有人/无人平台混编;德国则着力构建模块化无人作战保障体系,强化跨军种智能调度与动态补位能力。相关军事实践表明,智能化火力打击协同保障正从单域突破走向跨域融合。

实时智能评估,重塑作战效能评估保障体系

作战效能评估保障是完整指挥保障体系的关键一环。传统评估模式依靠战后抵近侦察、人工判读影像资料,反馈周期长、毁伤评估难,难以支撑火力即时复用和部署动态修正。人工智能联动全域前端感知终端,可重构作战

反馈保障体系,补齐可能导致完整指挥保障闭环断裂的短板。

欧洲军事强国在实践中既强调作战效能评估要“快”,也强调评估要“自主可控”。其中,英国正推动“数字目标定位网络”,利用人工智能实现从探测、定位到打击后核查的实时数据共享。法国则测试以本土大模型为底座的“阿卡迪亚”指挥控制系统,其设计尤为强调高烈度网络对抗中的抗毁性,即单一节点被毁或链路中断后,系统仍能保留剩余数据并维持评估链路。

亚太方向,日本防卫省已启动“战术AI卫星”研发,用于引导无人机、导弹。该卫星可锁定目标位置、分析战况,实现“边打边评估、边评估边修正”,把评估环节前置嵌入打击过程。

应当看到,当评估结论越来越多地由算法给出,误判的代价也会被算法的速度同步放大。智能化评估体系的建设必须与人工复核机制、可追溯的责任链条同步推进,方能守住可靠性的底线。

面向未来,伴随军事大模型、无人集群协同、全域数据互通等技术持续迭代升级,智能系统将承接更多重复性的保障工作,让指挥员聚焦顶层战略研判与关键作战决策。全域分布式、抗毁自愈型智能指挥保障架构将成为主流发展方向。唯有紧跟人工智能军事技术发展趋势,打通作战全要素数据高速流转通道,持续完善人机协同指挥保障运行机制,才能持续锤炼适配全域对抗、动态博弈场景的新型智能化指挥保障能力。

(作者单位:国防大学联合作战学院)

评论区

俄乌冲突中,乌军运用“棱镜”系统调度无人机集群发动袭击;加沙方向,以色列“福音”系统融合卫星影像、截获数据等情报,持续提供加沙地道、火箭炮等目标的坐标;美以伊冲突中,美军依托全域智能平台,实现上千数量级目标同步筛选。实践表明,AI技术不仅是情报处理的“加速器”,更已深度嵌入态势认知、辅助决策、火力协同、效果评估完整回路,成为指挥保障提质增效的核心变量。

“智者之虑,必杂于利害”。效率提升的另一面,是指挥保障体系对数据、算法和网络日益依赖,其内在的脆弱性与风险也随之放大。战场数据从来不是天然干净的。战时,来自卫星、无人机、雷达的海量信息涌入智能感知系统,如果算法只追求匹配速度,便容易把伪造目标信号、篡改地理轨迹等虚假信息当作真实样本,进而作出错误威胁研判、生成错误打击清单。此时,AI不仅不能发挥优势,反而会误导作战人员,甚至成为指挥保障体系中的软肋。

算法的固有局限会进一步放大这种问题。当前算法可解释性不足,战场又普遍存在训练数据所不能覆盖的情况。当敌方针对性实施算法欺骗,模型若不能“见微以知萌,见端以知末”,就可能被诱导生成背离实战的处置方案,将佯攻判为主攻、把次要方向判为决胜方向。以军AI目标库在使用中已出现目标误判的问题,美军也屡现误击友军、攻击平民设施等问题。

数据可信与算法可靠,最终都建立在网信底座上。无论是飞舞在俄乌战场上的大量廉价无人机,还是使用于加沙地带的以军地面无人作战机器人,其调度、识别、协同均高度依赖网信支撑。一旦网络被入侵、节点被劫持、投时被干扰、路由被切断,既有优势便可能发生反转。敌方甚至可通过网络攻击反向操控各类智能终端和无人平台,彻底打乱火力协同秩序,使无人平台偏离任务、火力协同误击友邻、指挥系统陷入信任危机。智能化越向末端延伸,这种单点突破引发的连锁效应就越强。

比技术层面更深的隐患,是人机权责在战争中被效率侵蚀,容易催生“智能依赖”型思维模式。目前局部冲突的实践

洞察智能风险 筑牢安全屏障

■曹炳华 张松芝

正呈现出同一趋势:AI将“决策周期”压得越短,人类审核越容易流于形式。智能化指挥保障的正确定位应是“人在回路、机在提速”。然而,长期依赖AI,极易形成“算法万能”的片面认知,进而抹杀人类的思维优势。此外,现阶段人机协同保障的权责划分尚未细化,任务突变时指挥人员可能无法及时干预修正方案,导致指挥保障链路中断、保障活动失序。

指挥保障拥抱智能化不能只讲赋能,必须同步讲控险。数据端要完善指挥保障数据治理规则,做好多源信息交叉验证;算法端要发展军事专用算法,强化可解释、可对抗、可降级能力;网信端要升级安全防护手段,为无人平台保留断网自主、返航受控和人工硬接管能力;协同端要健全相关机制,确保任何关键行动都有可归责的人类决定。智能指挥保障的真正成熟,在于用制度把AI的速度、数据的广度和人的判断力集成在一起。唯有如此,才能全面提升现代战争指挥保障能力与体系对抗优势。

认知小站

软件定义战争

软件定义战争是一项前沿的军事理念,主张通过软件定义技术构建灵活多变的军事系统架构,使软件而非硬件平台主导杀伤链,并将大数据、人工智能等深度融入作战体系。在近年来的局部冲突中,这一理念已得到充分体现,众包情报软件、数据分析软件、任务规划软件、毁伤评估软件等成为战斗力的重要组成部分,战斗力生成越来越由依赖武器装备转向软件能力驱动。

“人在回路”原则

“人在回路”的核心要义是人工智能系统承担数据计算、情报筛选、方案推演等任务,但最终决策权仍保留在指挥员手中。当智能系统随时介入,对AI输出结果进行评估、修正甚至否决。“人在回路”能够有效防范算法欺骗、模型偏差等内生风险,规避过度依赖AI,是智能化指挥保障应坚持的基本原则。

迈向军事智能体

近年来人工智能技术快速发展,军事智能体随之兴起。有别于传统军事人工智能侧重目标识别、路径规划等单向能力,军事智能体强调“感知—理解—决策—行动”全流程,能够在复杂战场环境中持续完成任务分解、资源调配、协同控制和动态优化。此外,多个智能体还可实现跨部门、跨任务链协作,共同为指挥保障提供支撑。

美军以Maven系统推动智能转型

■张晓军 李琳

焦点CT

今年3月,美国国防部以副防长备忘录形式,将帕兰提尔公司承建的Maven智能系统正式确立为标准化合设项目,要求在本财年内完成正规化建设,全面推动部署与应用。这一调整,标志着Maven系统已从试验性算法工具跃升为美军联合指挥体系的常设基础设施,成为推动美军智能转型的重要支撑。

Maven项目启动于2017年。彼时,美军面临情报处理滞后、军种数据割裂、决策链条冗长等现实难题,因而尝试借助人工智能这一技术杠杆撬动作战流程变革。历经多年算法迭代与战场检验,Maven系统已由单一的图像识别工具,发展为集多源数据融合、智能辅助决策、跨域协同调度于一体的综合性指挥保障平台。此次正式“列编”,意味着其已跨过“技术演示”阶段,成为联合全域指挥与控制体系中的标准化作战系统,直接服务于一线指挥员的实时判断与火力运用。

Maven系统正在重构美军联合作

战运行模式。在态势感知层面,系统融合陆、海、空、天、电、网全域传感数据,通过时空配准、冗余剔除和冲突纠错,生成统一、连续、可理解的战场全景,有效破除各军种数据壁垒。在情报研判层面,系统依托机器视觉与军用大模型,可自动甄别敌方指挥枢纽、防空阵地、导弹发射点位、装甲集群等高价值目标,并动态进行威胁分级与作战预案生成,大幅压缩情报研判周期。在火力协同层面,系统贯通前端传感器与各军种打击单元之间的链路,结合战场实时态势与附带损伤约束条件,优选打击力量,建立起“感知—研判—决策—打击—评估”的智能杀伤闭环。

美军通过实战进一步验证Maven系统的作战效能。据外媒报道,在俄乌冲突中,美军利用境外算力节点整合侦察数据,经脱敏处理后向盟友推送俄方炮兵阵地、后勤枢纽及指挥节点相关情报,依托复杂战场环境持续优化算法。在针对委内瑞拉的“绝对决心”行动中,面对城市地形复杂、军民目标交织的战场条件,Maven系统展现出精细甄别的能力,并依托海上移动指挥平台实现自主调度,有效支

撑特战渗透,空中牵制与电磁压制任务的同步展开。在美以对伊朗发动的打击行动中,Maven系统快速筛查千余处关键目标,统筹跨军种火力资源,将杀伤链时间压缩至分钟级,并完成自动化毁伤评估与二次打击筹划。值得注意的是,美军已为Maven系统规划了清晰的中长期迭代路径。在军种协同上,美军计划打通各军种指控系统接口,实现与主战装备深度适配;在技术层面,重点攻关多模态融合算法,拓展电网对抗、作战筹划、后勤保障一体化功能;在体系层面,则着重完善五眼联盟、北约分级情报共享机制,提升多国联军智能化协同作战水平。

不过,已经进行的相关测试运用也暴露出Maven系统的多个短板。强电磁干扰、城市遮蔽与伪装欺骗等对抗场景下,系统识别精度明显下降,误判风险增加。涉密数据的集中存储,使其安全隐患问题凸显。高强度作战节奏下,系统输出的海量信息可能导致指挥员认知过载,反而削弱决策效率。此外,受盟国数据主权法律约束,跨境情报共享链路脆弱,多国联合作战的协同效能如何仍有待进一步观察。

版式设计:李庆旭
资料整理:李庆旭、黄体彪
本版图片均为资料图片