



“研究军事、研究战争、研究打仗”专论

筑牢军事智能化转型的网络安全之盾

■李建平 纪凤珠

引言

当今世界,新军事革命浪潮奔涌,智能化技术深刻重塑战争形态。人工智能、大数据、云计算等新兴技术融入军事体系,推动作战指挥、装备控制、后勤保障发生深刻变革,战场态势感知与决策打击速度呈几何级数倍增。然而,军事系统高度互联、数据深度交融,也使网络安全风险如影随形,呈现扩散化、复合化、智能化等新特征,成为转型征途上必须突破的瓶颈。将网络安全贯穿转型全过程,提前谋划、精准破局、扎实固本,才能为军事智能化转型行稳致远构筑坚不可摧的安全防线。

洞察风险:正视转型衍生的网络安全新挑战

军事智能化转型在重塑作战模式、提升体系效能的同时,也打破了传统网络安全防护边界。安全威胁已从单一点向全域体系扩散,“被动防护”模式难以应对“算法对抗”“智能攻击”等新型威胁,必须精准识变、科学应变。

数据安全风险加剧,核心资源面临被窃取篡改威胁。数据是军事智能化的核心驱动力,作战数据、装备参数、指挥链路等敏感信息成为首要攻击目标。随着智能化联合全域指挥与控制体系构建,海量数据在多域节点间流动共享,数据采集、传输、存储全链条安全漏洞被放大。国外利用设备发热量变化、硬盘噪声等物理特性研究开发跨网窃密技术,可突破物理隔离获取核心数据。同时,数据标注、模型训练中的隐私泄露问题也比较突出。一旦作战数据被篡改或窃取,将直接导致智能决策失准、作战效能锐减,甚至引发指挥体系瘫痪。

技术融合跨界渗透,防护体系面临传导效应的风险。转型推动各领域系统互联互通,形成跨域协同的复杂网络生态,也使得安全风险具备“一点突破、全域扩散”的传导效应。从芯片后门到操作系统漏洞,从数据接口泄露到算法模型投毒,任一环短板都可能引发“多米诺骨牌效应”,导致指挥链路中断、作战数据泄露乃至武器装备失控。这种体系特性使网络安全风险从技术层面上升至战略层面。不同智能系统间互操作性不足、防护标准不统一,进一步加剧了体系

化安全风险。

智能攻击多维演进,攻防对抗面临范式更迭的挑战。全球网络攻击已进入“算法化、无人化、规模化”新阶段。攻击者利用AI技术,可将漏洞渗透周期缩短至数小时,通过多代理协同攻击、生成式AI钓鱼等手段,实施“批量压制”式打击。更值得警惕的是,境外国家级APT组织运用大模型批量生成恶意脚本,大幅缩短鱼叉式攻击周期,传统基于关键词、黑名单的防护模式失效,攻防对抗进入“秒级响应”的智能博弈时代。同时,智能化装备供应链全球化,增加了“带病装备”入网风险。从核心芯片到基础软件,任一环节被植入后门,都可能成为战时致命隐患。

精准施策:构建全域网络安全防护新体系

应对多维网络安全挑战,必须秉持“技术赋能、体系防控、主动制衡”理念,将智能技术融入防护全流程,锻造全域覆盖、动态适配、攻防兼备的防护能力,实现从被动应对向主动制衡转型。

强化数据治理,筑牢智能时代数据安全防线。数据是基石,必须构建全生命周期防护体系。一是严格数据分级管控。依据作战数据秘密等级实施分类存储、加密传输,对重要作战数据应用区块链等技术,确保数据完整性和可追溯性。二是建立智能数据安检机制。运用机器学习算法实时监测数据异常流动,自动识别恶意篡改、违规导出等行为,做到“异常即告警、风险早处置”。三是规范数据共享权限。采用零信任架构,对每次数据访问进行身份验证和权

限审批,从源头防范泄露风险,严格落实信息安全等级保护要求。

驱动技术创新,打造智能防护技术赋能体系。发挥智能技术防护优势,实现“以智防智、以智制智”。在算法安全方面,研发可解释性AI技术,破解“算法黑箱”,建立安全验证与漏洞修补机制,通过对抗性训练提升算法抗干扰能力。在感知预警方面,部署智能传感器等设备,构建全域立体监测网络,融合多模态深度学习技术,精准识别微型无人机、隐蔽攻击信号等目标。在主动反制方面,发展AI网络对抗系统,动态分析敌方网络协议和攻击模式,实施精准干扰和溯源打击。

完善体系构建,打造跨域协同全域防护格局。按照“统分一体、纵深防护”原则,构建多域联动防护体系。一是统一防护标准规范。推进各领域系统安全协议兼容和技术互联互通,实现防护资源集中统管、动态调配。二是构建“虚实一体”防护架构。融合物理域硬防护与网络域软防护,利用数字孪生技术模拟战场网络环境,开展攻防演练和风险预判,提升体系韧性。三是强化供应链安全管控。加速核心软硬件国产自主化进程,对关键组件实施全流程安全检测,建立供应链安全风险预警机制,筑牢“自主可控”安全根基。

聚焦实战锤炼,提升攻防对抗实战应对能力。立足未来智能战争形态,强化网络安全实战化训练。一是构建智能攻防演练平台。模拟无人机蜂群攻击、算法投毒、跨网渗透等典型场景,常态化开展“红蓝对抗”演练,锤炼部队应急处置能力。二是融入联合作战训练体系。将网络安全防护纳入全域作战流程,做到同步规划、同步演练、同步评估,提升多域协同防护水平。三是建强专业化技术力量。深化技术研发与应用,组建由技术专家、作战骨干、情报人员构成的智能化网络攻防专项分队,重点培养精通智能技术、网络攻防与作战理论的复合型人才,构建“日常防护—应急处置—精准反制”闭环体系。

固本强基:凝聚转型长效安全支撑新合力

筑牢网络安全屏障,需要与技术赋能、体系构建深度衔接的制度、人才、文

化支撑协同发力,将保障举措嵌入转型全流程,形成长效支撑体系。

健全法规制度标准,立起智能防护刚性底线。紧扣军事智能化技术特点,完善覆盖数据安全、算法安全、系统协同的法规标准。将智能设备安全审查、算法安全评估、供应链管控等纳入战备考核、演训评估体系,确保数据全生命周期防护、零信任架构部署等制度要求刚性落实,为技术防护和体系防控提供坚实制度保障。

建强人才支撑体系,补齐攻防对抗能力短板。聚焦智能攻防复合型人才需求,构建紧贴实战的培养模式。在院校层面,增设“智能攻防战术”“算法安全实操”等交叉课程,将数据治理、智能防护纳入官兵必训内容。在实践层面,依托军地联合实训平台,组织官兵参与算法投毒反击、跨网渗透防护等实战化演练,锤炼“技术+战术”融合能力。在机制层面,建立军民融合人才储备机制,吸纳地方AI、网络安全领域高端人才,增强军队智能攻防能力,为主动制衡提供人才支撑。

培育智能安全文化,筑牢思想防护无形防线。推动网络安全文化与军事智能化转型深度融合。加强教育警示,通过剖析智能攻击案例、警示跨境渗透风险,强化官兵“智能赋能亦增险”的底线思维。做好专项培训,开展智能化设备安全使用、算法漏洞防范等培训,普及“数据涉密不上网、智能设备不违规”操作规范,将安全意识融入数据采集、算法应用、系统协同全流程。营造安全氛围,搭建技能交流平台,举办智能攻防比武、安全方案研讨等活动,营造“人人懂智能安全、事事守智能底线”的浓厚氛围,为技术防线、体系防线筑牢思想根基。

编后

军事智能化转型是赢得未来战争主动权的关键一跃,网络安全则是这一跃能否成功的关键一环。唯有坚持系统思维、创新驱动、实战导向,将网络安全深度融入军事智能化转型各领域各环节,以技术突破强化防护之“器”,以体系构建筑牢安全之“盾”,以人才培养汇聚胜战之“力”,以制度文化夯实长远之“基”,多维度协同发力,全链条精准施策,全面筑牢网络安全屏障,才能真正将智能化潜能转化为制胜未来的强大战力。

积极推动作战编组创新

■张自廉 吴培仁

谈兵论道

作战编组,是为遂行作战任务,对编成力量进行编组组合的基本形式。当前,各类无人作战平台与智能化武器系统加速迭代,深刻改变着传统作战样式和制胜机理,对作战力量运用方式提出全新要求。只有与时俱进创新作战编组模式,才能有效提升整体作战效能。

突出自主适应,优化编组方式。传统作战编组多在战前依据作战样式、任务、环境、对手等因素,预先确定兵力规模、结构比例与功能搭配,并配置于有利地域。作战过程中,严格执行既定计划,达成协同行动。受制于战场情报获取能力与部队掌控水平,这种相对固定的编组曾是实施指挥控制的有效途径,但其横向联接薄弱,精细协调难度大,关键节点一旦受损,体系易陷入瘫痪。信息化智能化战场上,样式混合多变、任务复杂多样、态势瞬息万变,作战效能高度依赖体系的灵活性。这就要求作战编组必须具有弹性与自主适应能力。应依托网络信息体系的链接效能,有机整合广域分布的作战单元、要素、模块与平台,形成功能独立、能力融合、任务界限模糊、可重构且韧性强的作战编组。作战中,根据任务时效、周期、规模等需求,通过功能互补、链路冗余、智能切

换等方式,灵活实施跨军种、跨领域、跨空间的临时拆分与重组。当体系节点遭攻击受损时,能迅疾自主重构、迁移功能,确保高强度对抗环境下作战效能的可持续释放,真正做到因敌而变、因势而变。

强化新质主导,重塑编组形态。传统作战编组常以特定军兵种部(分)队为主体,临时配属必要兵种及保障力量,形成侦察、机动、打击、防护、保障等能力。如防空突出高炮、地导部队,突击则以坦克、机步部队为主,其余力量实施支援保障。此类编组因各力量在机动、通联、指控等方面差异显著,虽形式“捆绑”,实则松散,难成一体,战场突变时难以快速调整。信息化智能化战场,制胜关键已非火力与投入资源的简单叠加,而在于以信息算法为核心的智能对抗,取决于智能主导下全域能量的聚合释放。因此,须以电网、智能装备、无人系统等新质力量为主导,融合人类智能与机器智能优势,编组人机协同、自主作战单元,构建“多域融合、功能耦合、纵向贯通、新质综合”的力量体系。作战中,各单元依托战场信

息网络,通过算法模型与软件系统的高效运行、快速响应,实现态势自主感知、数据智能分析、信息智能处理、效能智能评估,进而高效指挥决策、制定计划,形成战法行动优势,将智能优势转化为战场胜势。

创新动态分布,变革编组形态。传统作战编组为达成多维空间整体作战效果,常按方向、区域和任务,依作战进程将各部(分)队集中编为若干集团、群队,明确支援协同关系,按序依次投入交战,以求在主要方向、重要目标上形成静态优势,实现以强击弱。信息化智能化战场,在智能化网络信息体系支撑下,作战力量实现无缝链接融合、多域同步联动,战场感知、实时机动、指挥决策与协调控制能力极大增强,无需通过空间预先集中实现功能集中,可依托网络信息体系达成力量的“虚拟”集中与动态集优聚合。应彻底打破固定建制,临时配属的编组融入,自主作战单元,构建“多域融合、功能耦合、纵向贯通、新质综合”的力量体系。作战中,各单元依托战场信

今天,订单式外卖早已融入大众日常生活,成为人们满足个性化饮食需求的便捷选择——足不出户即可按需点餐、精准配送。这一生活中的变革,映射出供需关系中“需求主导、精准匹配、高效响应”的核心逻辑,而这一逻辑,正深刻重塑着后勤保障领域的发展格局,催生订单式保障这一全新模式。从民间消费场景到专业保障领域,订单式保障有助于在有限保障力量条件下,显著提升保障效能,更好地支撑未来智能化作战需求。

未来战场的深刻变革,对保障模式创新提出了刚性需求:一是分布式作战催生保障变革。广域分散、快节奏转换的战场环境,要求保障模式必须适应作战单元高度独立以及保障点位由线转点、由定转动的特点。传统保障链条环节多、周期长,难以满足即时响应、随需而至的要求,在多方向、多批次连续作战中易造成供需错位、贻误战机。所以亟须建立直达末梢、灵敏响应的新型保障方式。二是新质力量运用要求精准适配。无人作战平台、电磁频谱武器等新质作战力量对能源、备件、技术支持的需求高度差异化、专业化。同一战场可能同时存在弹药补给、数据链修复、无人载荷更换等性质迥异的保障任务。单一化、标准化的保障供给难以满足需求,实现保障要素与作战需求的精准对接迫在眉睫。三是强对抗环境亟须韧性保障。现代战争中保障设施是重点打击目标。集中部署的保障枢纽一旦受损,易导致保障链断裂。保障体系必须具备强大的抗毁性和持续保障能力,要求保障模式向分布式、去中心化转型,通过多源备份、动态切换,确保局部节点受损时保障网络能快速重构恢复,避免“一点瘫痪、全局失效”。

订单式保障是运用智能技术对保障流程的重塑,其核心是构建智能化保障平台,实现需求、资源、行动的精准高效联动:一要实现需求感知自动化。依托战场物联网、智能传感器与终端设备,实时自动感知作战单元物资消耗、装备状态等关键信息。当达到预设阈值或出现损伤时,系统自动生成标准化保障需求,变被动请领为主动感知,实现保障态势的全局可视与实时传输。二要实现资源匹配智能化。其核心是依托智能化保障平台,运用智能算法统筹广域分布的保障资源。平台根据保障需求的类型、紧急程度、地理位置、投送能力等约束条件,自动优化匹配方案,生成最佳保障力量派遣指令,极大缩短“需求—响应”链路,变逐级协调为平台直达。三是实现行动调控动态化。战场态势瞬息万变,保障行动需全程动态优化。基于实时战场信息流,平台可在线调整投送路线、动态切换供给节点,推动保障行动与作战进程紧密协同、动态调优,确保保障链路始终紧贴作战需求。

订单式保障通过流程再造与技术赋能,在关键效能维度实现突破:一是

缩短保障响应周期。压缩中间环节,优化投送路径,结合前置预置储备,大幅提升响应速度。需求直达平台、资源智能匹配,特别是随着无人投送平台发展,保障响应有望迈向分钟级,实现关键时间节点保障与作战的精准同步。二是提升资源配置精度。依托精准的需求感知和智能算法,推动保障资源在更大范围内动态共享、按需流动,变静态储备为动态调配。以物资保障为例,通过物联网实时感知消耗,自动生成需求、智能匹配力量,使资源配置由粗放配置走向精准配置,极大提高了单次保障有效性和整体资源利用效率。三是增强保障体系韧性。订单式保障的分布式网络结构和资源池化管理,赋予保障体系强大韧性。当某一保障节点受损或超负荷时,系统可自动将任务动态分流至邻近可用节点,维修力量随任务灵活调配,确保不因单点故障中断保障。这种弹性重构能力,使保障体系具备网络化自愈特性,在持续对抗中保持稳定高效的保障输出,为战斗力持续生成提供可靠支撑。

把握作战概念设计机理

■张震

挑灯看剑

世界新军事革命加速演进,智能化战争形态特征日益凸显。作战概念设计作为连接军事技术革新与作战方式变革、战略构想与战术实践的关键枢纽,正以前所未有的驱动力撬动军事理论创新。深刻把握其内在机理,方能激活理论创新引擎,为打赢未来战争赢得战略主动。

逻辑起点:源于实战、破解需求。作战概念设计的生命力,根植于对打赢未来战争核心需求的精准回应与前瞻破解,本质是面向未来战场的“问题求解”,其逻辑起点须锚定作战需求分析。这就要求作战概念设计必须精准预判痛点难点,深入剖析未来作战环境、对手能力、战场挑战,识别关键性“痛点”与颠覆性“难点”;聚焦非对称制胜,以形成非对称作战优势为根本指向,将作战需求有效转化为明确的能力缺口;细化设计约束条件,将抽象的能力缺口分解为可操作、可衡量的具体设计约束,从而确保概念的实战指向性。脱离实战需求的作战概念,如同无源之水、无本之木,纵使逻辑精巧、技术炫目,终难逃“纸上谈兵”之困。作战概念设计的真正价值,在于精准把握“未来仗怎么打”的制胜需求,而非技术堆砌或理论空想。

核心路径:技术驱动与作战牵引辩证统一。作战概念设计绝非“技术决定

论”的盲目跟从,亦非脱离物质基础的“战术空想”,其生命力源于技术与作战必要性之间持续互动、相互塑造的辩证过程:技术突破赋能作战构想,人工智能、自主系统、高超声速武器、量子信息技术等颠覆性技术,为突破现有作战范式、构想全新作战样式提供物质基础;作战需求牵引技术发展,前瞻性、颠覆性的作战构想,为技术研发指明方向,提出明确指标要求,形成强大倒逼机制;概念设计充当关键枢纽,在技术与作战的“交汇点”上,作战概念设计发挥着“翻译器”与“集成器”的核心功能——将技术潜力“翻译”为战术优势,将作战构想“集成”为技术发展路径。技术演进与作战需求在作战概念设计的催化下,始终处于相互成就的螺旋上升之中。

关键形态:体系融合、动态演进。现代战争是体系与体系的对抗。平台概念设计必须超越单一战法或平台创新的局限,以体系化构建为基本形态和成败关键。要注重要素集成,将前瞻作战构想、新型力量编成、高效指挥控制、创新战法运用及关键装备支撑等核心要素,进行系统性整合与优化;强调方案落地,形成可操作、可验证、可推广的系统解决方案,实现从概念到能力的实质性转化;强化动态适应,敏锐响应作战环境、对抗格局与技术条件的快速变化,实施持续迭代、动态演进的体系化构建。成功的作战概念设计,必然是顶层构想与底层能力同步推进、相互支撑的系统工程。