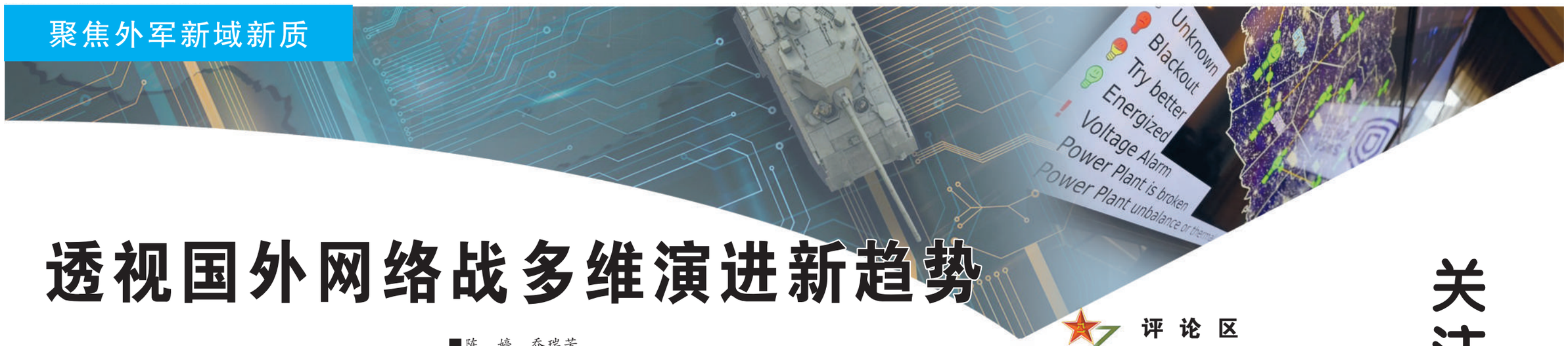
聚焦外军新域新质



透视国外网络战多维演进新趋势

■陈　婷　乔瑞芳

瞭望台

不久前，北约“锁盾2026”网络演习在爱沙尼亚举行。此次演习将应对人工智能驱动的网络攻击作为主题，体现了鲜明的实战化导向。近年来，随着网络技术快速发展，网络空间正成为大国竞争和军事对抗的“新高地”。为获取优势，多国纷纷将“先发制人”的网络攻击作为重要选项，并通过优化网络作战层级、手段和方式，谋求提升网络战整体质效。

作战层级纵深拓展，行动界限渐趋模糊

网络战武器具有“一次性”特征，需预置待机，其运用曾长期集中于战略层面。然而，随着人工智能、大数据等技术的快速发展，以及太空、电磁等跨域作战的深度融合，网络战正从战略层面向战役、战术层面延伸，愈发受到重视。

这一趋势在近年多起军事行动中得到印证。美军在“绝对决心”行动中切断委内瑞拉网络，为突击部队创造“单向透明”环境；以色列入侵德黑兰道路监控系统，精准锁定袭击目标。这些行动表明，网络战已能产生即时、大规模的毁伤效果，战略威慑与战术打击的界限日益模糊。美网络司令部司令约书亚·鲁德称，未来“针对战术军事系统的网络作战将愈发普遍”，并强调需将相关技术从实验室推向战场。

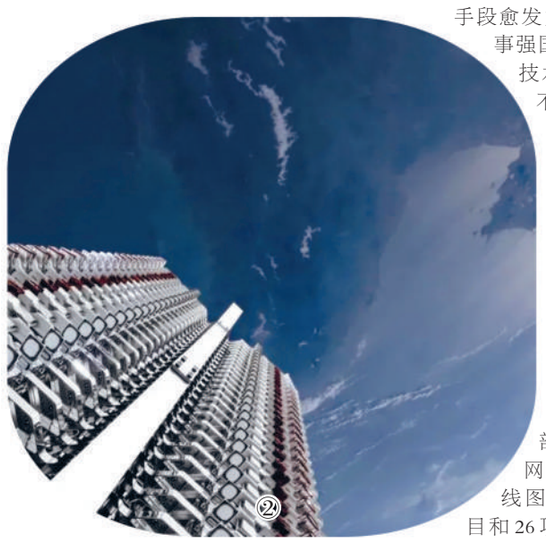
当前，多国正系统性推动网络作战能力下沉。2018年，美国《第13号国家安全总统备忘录》将部分网络行动授权由总统下放至国防部长。2025年，美陆军开始赋予军级指挥官更多网络作战权限，通过缩短决策链路，提升应对快速变化战场的灵活性。日本的网络政策转向同样引发广泛关注。2025年，日本通过“主动网络防御法案”，允许自卫队对判定为“攻击者”的网络实施先发制人打击，相关授权门槛也随之降低，将网络空间视为可率先发起战术攻击的“前沿战场”。

战术层级网络部队建设如火如荼。俄罗斯与以色列已在实战中投入专业化网络作战分队。美军正推动此类部队成建制发展，组建了陆军第11网络营、海军陆战队远征军信息大队等。2025年初，美陆军第11网络营团队在演练中通过射频等手段直接支援装甲、步兵和空降部队行动，表明“网络火力”已能融入联合打击链条，成为即时可用的战术选项。在另一场演习中，法军步兵营编配的网络战小组仅用11分23秒便成功瘫痪对手指挥通信网络，展现了将网络攻击能力直接嵌入基层战术单元的高效性。

值得注意的是，不同层级的网络战正呈现融合发展态势。美军提出的“远征+远程”协同模式即是例证：由前沿战术网络部队突破封闭网络获取访问权限后，移交后方网络任务部队实施复杂网络节点控制。这种战法将战术行动的灵活性与战略行动的系统性相结合，推动网络战在战争全域发挥更大作用，使网络空间从辅助作战域，向能直接影响战场胜负的核心作战域加速演进。

作战手段迭代升级，人工智能深度赋能

面对日益复杂多变、高强度对抗的作战需求，传统由人工驱动的网络作战手段愈发力不从心。为此，各军事强国正着力推动人工智能技术深度嵌入网络空间，不断提升进攻性网络作战能力。



②

这一进程首先体现在顶层规划日趋完善上。当前，人工智能技术存在诸多不确定性，各国主要通过顶层规划由上而下推动其与网络作战融合，确保技术优势稳定、可控地转化为作战优势。美网络司令部出台人工智能融入网络作战行动的五年路线图，推出60多个试点项目和26项新举措，并设立特别工作组推动项目落地。英国国防部在《2025年战略防御评估报告》中明确宣示，将在网络攻防中更广泛地运用人工智能，相关行动由其网络和电磁司令部统筹。这些规划共同的指向是，将前沿算法能力系统性注入国家网络作战体系，以夺取并维持人工智能领域主导权。

持续增加的研发投入为智能化网络作战手段落地注入强劲动力。以美国为例，2027财年，网络司令部“用于网络空间作战的人工智能”项目预算申请达1.38亿美元，较2026财年激增约26倍。此外有报道称，美国国防部已与OpenAI、谷歌、微软等顶尖商业公司达成协议，允许其最先进的大模型接入美军机密网络。此举意味着，民用领域的强大算力、海量数据和前沿算法，正被源源不断地输送至军事领域。

顶层设计与巨额投入正加速转化为战场上的实战能力。2025年夏，美网络司令部授予美国网络战初创公司“Twenty”一份价值1260万美元的合同，旨在为美军提供“迫切需要，并让对手感到恐惧”的关键能力。该公司的核心技术正是利用人工智能赋能网络装备系统，搭建可同时对数百个目标进行自动化、持续操作的智能攻击链条，大幅提高作战效率。此类实践表明，人工智能正成为驱动网络作战核心流程的“引擎”，深刻重塑网络空间作战规则。

作战方式注重协同，行动机制日益深化

伴随进攻性网络作战规模的扩大，单一国家独立实施和应对进攻性网络作战难度显著增大，费效比矛盾突出。为此，部分国家正积极构建网络空间军事联盟，通过强化情报共享与联合行动，追求更高的协同作战效益，推动进攻性网络作战协同向机制化、实战化和全球化方向发展。

协同机制日益深化。多国联合开展进攻性网络作战需建立战略共识，协同正由国防部层面向具体作战机构和任务部队延伸。2025年10月，德国国防部长和英国国防大臣宣称，双方将共同开发云网络，加强数据情报分享，深化应对网络攻击合作。同年12月，美空军第16航空队与波兰网络司令部举行高层指挥官会谈。双方承诺将加强联合战备行动，识别新型威胁，确保挫败任何破坏两国网络、关键基础设施和军事力量的企图。

协同内容聚焦实战。基于地区冲突的经验教训，当前多国联合网络演习正逐步摒弃预设脚本、流程固化的模式，转而强调在真实对抗环境中演练。2026年2月，英国陆军协会主办的“网络奇迹2026”多国网络演习在新加坡举行。演习中，新加坡网络司令部与英国参演部队组成联合团队，在高度仿真环境中，应对针对关键基础设施、政府网络和私营部门的一系列模拟攻击。

①

协同范围不断拓展。为整合更广泛的数据资源与技术优势，北约通过年度大规模双多边网络演习，进一步拓展联盟协作的广度和深度。其中，美网络司令部主导的“网络旗帜”系列演习最为典型。2024年8月启动的“网络旗帜24-2”演习首次将进攻性网络作战纳入核心课目，重点推动“五眼联盟”伙伴间的协调。2025年7月，“网络旗帜25-2”的参演兵力进一步扩大，吸引了20多个美国的盟友和伙伴国参加，演练内容包括供应链入侵、勒索软件和零日攻击等，旨在寻求超越传统“五眼联盟”框架的多国合作，汇聚更多网络作战力量提升集体网络作战能力。

（作者单位：军事科学院）

图①：美空军第747网络空间中队在执行任务。

图②：SpaceX星链卫星入轨画面。

版式设计：胡云艳

资料整理：吴家庆、窦天阳

本版图片均为资料图片

评论区

关注网络空间的「蘑菇云」

■吴尹清

2025年12月，委内瑞拉国家石油公司遭遇大规模网络攻击，再次以残酷事实警示我们，网络空间的无形攻击已演变为能够直接瘫痪国民经济命脉、威胁国家战略安全的现实威胁。

所谓进攻性网络行动，是指由国家或非国家行为体在他国网络空间实施，以达成特定政治、军事或经济目的的行动。随着互联网深度融入全球关键基础设施，网络空间已成为继陆、海、空、天之后的“第五疆域”，其战略地位日益凸显，成为大国博弈的重要领域。

近年来，进攻性网络行动在全球呈现加速扩散与升级之势。其规模持续扩大、频率显著增加、破坏力不断攀升，与常规军事行动的协同联动日益紧密。多国军队纷纷加速发展网络作战力量，并将其纳入整体作战体系进行训练与筹划。以美军提出的“联合全域指挥控制”概念为例，其核心在于实战中协同运用陆、海、空、天、网等多域力量，谋求作战效能最大化。现代军事体系中，武器装备、传感器与指挥控制中心紧密相连，网络贯穿其中。进攻性网络行动可瘫痪敌方防空系统、扰乱导弹制导、切断敌指挥链路等，成为影响现实战场态势的重要变量。

2024年12月，北约合作网络防御卓越中心开展了代号为“十字剑2024”的大规模进攻性网络演习，训练网络战人员在模拟危机中执行完整进攻性网络杀伤。这意味着进攻性网络行动已被更多国家和军事联盟纳入常规作战训练范畴。在近期的伊以冲突中，以色列通过网络手段全面渗透德黑兰的公共摄像头与通信基站，结合其他情报手段，最终完成针对性刺杀行动。这再次证明，网络攻击已深度嵌入现代战争进程，既可充当“开路先锋”破坏战略基础设施，也能在作战中作为“增效器”打击要害节点，甚至通过信息操控影响敌方认知。

然而，进攻性网络行动的泛滥正深刻冲击全球网络安全生态。个别国家秉持“网络空间没有蘑菇云”的投机心态，试图利用网络行动门槛低、溯源难、不易引发传统战争的特点，全力发展进攻性网络作战力量，甚至图谋“先发制人”以获取不对称优势。这种危险的零和思维极易引发网络空间军备竞赛的恶性循环，严重破坏各国共同依赖的和平、开放、稳定的全球网络环境。

更严峻的是，进攻性网络行动往往无视军用与民用目标的界限，极易引发人道主义危机。俄乌冲突中，作战一方曾对另一方的金融机构及电信公司发起网络攻击，导致其全球支付系统、部分银行服务一度瘫痪。此类攻击如果用在电力、能源、医疗等上，将直接影响社会正常运转，危及民众生命安全。随着人工智能技术融入网络作战，网络攻击手段与强度将会不断升级，进攻性网络行动或将加速扩散，网络空间的攻防斗争也将更加激烈。

历史与现实警示我们，网络空间并非没有“蘑菇云”。面对进攻性网络行动带来的严峻挑战和严重后果，国际社会必须凝聚共识，采取切实行动：一是加快构建具有普遍约束力的网络空间国际规则体系，明确“红线”与“禁区”；二是深化网络安全国际合作与互信建设，建立危机管控与沟通机制；三是大力发展网络攻击溯源技术；四是构建负责任的国家网络空间战争伦理观，倡导和平利用网络空间。唯有如此，方能有效规制进攻性网络行动的滥用，维护网络空间的持久和平与共同安全。

（作者单位：军事科学院）

日本加速构建“先发制人”网络战力

■付红红　谿　兔

焦点CT

3月17日，日本内阁会议决定，自今年10月1日起，将允许对网络攻击的源头服务器实施主动侵入，进行所谓“无害化处置”。此举标志着日本谋划已久的“主动网络防御”政策进入实操阶段，将对地区安全稳定构成新的冲击，值得高度警惕。

“主动网络防御”理念于日本2022年版《国家安全保障战略》中提出，并在2025年版《网络安全战略》中得到明确。与传统的事后处置不同，该理念强调在损害发生前，通过情报搜集提前探知威胁后，可采取使对手攻击能力失效的进攻性行动。一旦侦测到所谓网络攻击迹象或前兆，日本国家安全保障局将牵头拟定“无害化”处置方案，随后在国家网络安全担当大臣指挥及国家网络安全办公室协调下，由警察厅和自卫队具体执行。

为扫清自卫队涉入的法律障碍，日本在2025年5月出台法案，授权警察和自卫队在应对有组织网络攻击时，可采取瘫痪对手服务器等攻击行动。防卫省在同年7月的《防卫白皮书》中毫不掩饰地宣称，网络空间是军事领域的重要作战域，自卫队将全面配合国家层面包括“主动网络防御”在内的网络安全整体部署。日本从法律与政策层面正式将自卫队确立为网络战的行动主体，模糊了平时与战时的界限，使其在非战争状态下发动网络攻击成为可能。

为确保有效遂行进攻性网络战行动，日本在领导体制与作战力量建设上双管齐下，推进迅猛。在国家层面，2025年7月，网络安全战略本部升格，由首相亲自“挂帅”，成员囊括全体内阁成员；新设的国家网络安全办公室取代原内阁网络安全中心，成为统管网络安全的“司令部”。在自卫队层面，继2022年整合成立自卫队网络防卫队后，海上自卫队于2026年3月又将系统通信队群改组为网络防护群，作为新设情报作战集团的核心。更为值得关注的是，自卫队计划在2027年前将网络相关部队扩编至约4000人，规模在5年内增长近10倍，其扩张速度和野心令人侧目。

与此同时，日本正积极将这一危险的网络攻击能力用于开展阵营对抗。自2021年以来，日本已连续6次参加北约“锁盾”这一全球规模最大的实战性网络演习。今年在“肩并肩”联合军演框架下，日本首次以正式参演方身份，在菲律宾参与了多国网络演习，意图提升多边协同网络战能力。日本还透露，已签署由英国起草的网络安全国际合作文件，该文件大肆渲染网络威胁，具有鲜明的阵营对抗色彩。国际社会担忧，日本通过联盟捆绑，将其网络战能力投射到更广阔的国际舞台，将加速网络空间的阵营化与军事化。

从理念提出、法律松绑、战略更新，到机构升格、部队扩编、阵营协作……纵观日本一系列环环相扣的操作，其背后野心昭然若揭：既企图借此突破战后体制束缚，打造一支具备“先发制人”能力的网络攻击力量，也妄图巩固并利用盟友体系，强化网络威慑能力。这种“扩军”与“结盟”并举的扩张态势，必将加剧网络安全领域的对抗，推高网络摩擦与冲突风险，甚至可能催生网络军备竞赛，最终只会使自身陷入更危险的境地。

（作者单位：国防科技大学）

认知小站

“勒索”席卷全球

2017年，勒索病毒“想哭”席卷全球。该病毒具有强大的自我复制与主动传播能力。计算机一旦感染，其存储的所有文件即被加密，并弹出勒索对话框，要求用户支付以加密货币计价的高额赎金。该病毒在数天内横扫150多个国家和地区，感染数十万台计算机，众多民用目标受到波及。英国国家医疗系统瘫痪，上百家医疗机构的紧急手术被迫取消，急救系统陷入混乱，救护车调度失灵，严重延误患者救治。

攻击悄无声息

2010年，伊朗纳坦兹核设施大量铀浓缩离心机突然瘫痪。事后调查发现，这是一种名为“震网”的计算机病毒攻击所致。该病毒通过外接U盘进入纳坦兹铀浓缩设施的内部网络，而后利用该设施中计算机的Windows操作系统漏洞窃取设备控制权限，隐蔽地破坏铀浓缩过程中的关键设备。“震网”事件首次清晰展现了网络空间攻击可对现实世界中的关键基础设施造成与传统物理毁伤等效的破坏效果。

AI隐忧凸显

近日，Anthropic公司发布“克劳德神话”人工智能模型。该模型在发现软件漏洞方面展现出极强能力，据称已识别出常用软件程序中的“数千个”漏洞。其中一些漏洞相当隐蔽，难以被常规手段检测到，最早的甚至可追溯至27年前。测试显示，“克劳德神话”能够构建复杂的漏洞利用链，实施可绕过多层安全防护的多步攻击。这种能力若被攻击者掌握并滥用，将对经济发展、公共安全和国家安全造成严重后果。