聚焦外军新域新质



智能化战场倒逼网信体系“韧性重塑”

■李建平

瞭望台

据媒体报道，近期俄乌战场上，俄军侦察无人机依托热成像锁定乌军星链终端，配合FPV自杀式无人机与火炮实施打击，接连摧毁乌军星链地面站与通信设备。反观乌军，依托地面战术互联网保持指挥链路畅通，火力协同与无人机作业照常运转。这些战场实践，为观察智能化条件下的网信体系建设提供了重要参照。

智能化战争时代，作战体系高度依赖网信体系赋能，指挥调度、态势感知、火力协同都需要网信设施支撑。网信体系不仅是信息传递通道，更是影响指挥连续性与体系生存力的重要依托。当前，多国着眼战场态势演变和自身利益，加快转向分布式、去中心化、可重构、高韧性的网信体系建设路径，力图在持续高强度毁伤对抗中掌握战场主动权。

从“打节点”到“断链路”——网信枢纽成为战场重点打击目标

传统“中心—边缘”网络信息体系架构，高度依赖固定指挥所、干线通信基站、后方核心数据机房与集中式指挥网络，在高强度、快节奏、非对称对抗的智能化战场环境下，极易遭对手精确压制，难以适应形势发展。

电子侦察手段迭代升级，网信枢纽的暴露风险持续上升。无源测向、多源融合侦察、网络溯源等手段在战场广泛应用，网信枢纽的电磁信号、流量交互特征可被持续捕捉。俄乌冲突中，乌军依托多站协同测向系统，持续监测俄军后方通信枢纽、中继节点信号，标定位置并纳入火力打击清单。曾经依靠地形、伪装实现隐蔽的网信枢纽，如今更容易被持续发现和锁定，成为对方精准打击的靶子。

核心网信枢纽承载体系级信息功能，毁伤效益远高于打击普通末端节点。传统网信体系采用集中组网，各战术单元的通信、态势数据都向枢纽汇聚分发。俄乌冲突初期，俄军部分前沿指挥机构沿用集中式架构，指挥所作为本级网信枢纽遭乌军火力打击后，下属多个作战单元同步失联、指挥中断。一次打击便可造成大范围体系失能，相较于猎杀单兵终端，打击枢纽的作战效费比更高。

打击层级持续上移，信火一体打击正从“压制末端节点”升级为“压制拓扑”。“打节点、断链路”是战场毁伤网信体系的重要路径。俄乌战场上，俄军使用FPV自杀式无人机、侦察无人机持续搜寻并打击星链终端，同时依托电子侦察设备搭配“海鹰-10”测向无人机截获前沿通信信号并引导火力打击，属于典型的针对末端节点的毁伤行动。2026年9月，俄军连续空袭乌克兰信息通信基础设施设计与发展研究所与多座大型数据中心。这类设施是支撑大范围星链接入与智能指挥运算的网信枢纽，管控大量终端接入链路，摧毁枢纽可直接破坏对手整体信息拓扑，批量瘫痪下游节点，实现体系级压制。

从“集中汇聚”到“分布生存”——技术、实战、制度三路并进

随着通信枢纽、数据中心与网络链路成为现代战场的打击重心，各方网信体系建设的重点也随之从“防止被攻击”转向“在被攻击、被损毁后仍能保持持续作战能力”。尽管路径各有侧重，但核心目标一致：推动信息承载从“集中汇聚”转向“分布生存”。

技术驱动，夯实体系级抗毁底座。以美国为代表的技术强国以零信任改造安全访问机制、以云化重构算力承载体系，双向重塑网信底层根基。美国国防部2022年发布的《零信任战略》明确，美军将在2027财年末达到“目标级零信任”能力，即所有访问请求均需经过持续身份核验与动态权限授权，通过精细化权限管控实现安全隔离，即便单点失陷，攻击也难以横向扩散。美国国防信息系统局作为美军信息网络运维主责机构，依托“雷穹”项目推进零信任架构落地，加快在国防部与战区机构部署，并通过对外军售渠道向盟友输出相关能力。在云化重构方面，美军推出“任务网络即服务”模式，以算力与数据漂移替代固定机房部署模式，实现身份权限与算力资源的同步重构；该模式整合各作战司令部分散隔离的独立网络，构建统一云基的作战司令部共用网络，破解数据共享与跨区指挥控制瓶颈。欧盟投入约4000万欧元建设军事多域作战云，明确将自组网、自愈、服务降级与冗余维持列为核心能力指标。值得注意的是，体系级底座普遍存在投入大、建设周期长、运维复杂度高的问题。欧洲防务工业约72%的云服务依赖美国供应商。

实战验证，强化末端弹性组网。俄罗斯、乌克兰、伊朗等直面高强度对抗的国家，在设施损毁、电磁压制常态化的战场环境下，以冗余异构为抗毁核心，依托商用技术降低建设成本，探索适配前沿作战场景的组网模式。俄军自2025年以来逐步为多型无人机加装MIMO自组网电台，搭建多层空中中继链路，无人机互为机动通信节点，控制距离可达150至175公里，通信覆盖能力较之前提升一倍。乌军以Delta态势感知系统、GIS Arta炮兵火控系统与HIMERA战术自组网构成的地面战术互联网为骨干，采用多频段、多路径冗余设计，提升对手实施全域电子压制的难度。伊朗布局有线、蜂窝、卫星3套相互独立的通信链路，单条链路中断后可快速自动切换至备用信道。末端组网的核心逻辑在于“多”与“异”：多则难以被一网打尽，异则难以被单一手段全面压制。但也要看到，末端组网多依托商用技术与分散节点，存在标准不统一、体系化适配性弱的问题，难以独立汇聚成体系级作战能力。

制度配套，贯通全层级规则保障。网信韧性能力的构建不能仅依赖硬件网络的物理冗余，作战预授权、行动条令、法规机制同样是重要支撑，且覆盖顶层指挥与战术末端全层级。伊朗将全国划分为31个省级独立作战单元，配套独立情报保障、武器库储备与作战预授权、多级指挥继任机制，中枢受创后地方单元仍可独立遂行任务。美陆军2026年10月新版作战指导文件，明确断联作战、恢复重连、持续机动三项能力要求，从制度上下放前线自主处置权限。

从“全程防打击”到“受毁仍能战”——理念与边界持续拓展

当然，网信体系韧性建设不会止步于硬件冗余与链路扩容，而将从多个维度深度发力，持续向体系化纵深推进。

认知重塑，将容错续战纳入顶层设计。从趋势看，多国军队不再将链路中断、节点损毁视为偶发故障，而是将其预设为高强度对抗的常态。美军“项目汇聚”系列演习主动设置断网、强电磁压制等极限场景，将降级续战列为硬性考核课目。以色列优化战区指挥权责，下放前沿分队临机处置权限，明确通信中断时一线单元可依预案自主行动，推动建设逻辑从“全程防打击”向“受毁仍能战”转变。

韧性边界不断拓展。韧性保障内涵已从链路连通向算力存续、数据保活延伸。英军开展边缘算力前置试点，将目标甄别、情报解析模型部署至车载节点，后方算力链路中断时，前沿仍可独立完成情报初步研判。美军依托边缘数据网格，可在战场带宽不足、网络受袭时动态调度数据优先级，优先保障杀伤链核心数据传输留存。

民用技术加速溢出。多国跳出军用专网单一建设思路，挖掘商用资源的韧性补位价值。日本自卫队测试并引进美国商用星链高速通信服务，作为军用卫星被干扰时的备份通信链路。部分北约成员国推进开源通信协议军事化改造，依托民用成熟技术快速搭建机动备份网络，压缩研发成本与落地周期。

（作者单位：国防大学联合作战学院）



图①：美军士兵在演习中操作C-100无人机进行侦察。
图②：俄军操作“海鹰-10”无人机。
图③：2026年美军举行网络攻防技术演习。
本版图片均为资料图片

评论区

透视

网信体系韧性增强机理

■纪凤珠

西方军事思想中有一种说法——“战争的秘诀在于通信”，相传出自拿破仑。从冷兵器时代靠烽火报警、鼓声传令，到机械化时代无线电助力指挥员实现远距指控，再到智能化战争时代网信体系把分散在多域的侦察、指挥、火力、保障力量聚合成整体……信息流通的方式，不仅决定着指挥控制的半径与样式，还深刻影响作战体系的组织方式和战场制胜逻辑。

信息流不通，能量流就聚不起来。与以往作战靠单件装备、单一兵种就能拉开差距不同，如今陆基传感器、海基平台、空中火力、天基中继等依托泛在网络便可实现互联互通、跨域协同。杀伤链上任何一个信息节点断裂，能量流便失去指向，跨域火力、态势共享、联合指挥就可能同步中断，再先进的装备也只能各自为战，发挥不出体系效能。与此同时，作战对抗的重心正从打装备、打节点转向断链路、瘫体系，对手不再满足于单点摧毁，而是瞄准信息拓扑的薄弱处实施攻击，试图用最小代价让对手整个作战体系失能。在这一转变中，仅靠加固核心枢纽、增加带宽，已难以应对体系级断链打击；只有具备韧性的网信体系，方能经受持续压制与反复打击。

然而，韧性向战斗力转化，不能只靠简单叠加备份链路和设备，而要从整个体系架构设计的源头思考如何赋能作战。

在抗毁维度，将体系级失能拆解为局部降效。其核心思路是功能解耦，即解除作战职能与少数核心枢纽的绑定，将不同作战职能拆分至独立节点，各节点仅承载本职所需的最小权限与数据。美海军在水面行动群演练中，将预警、指挥、打击三类职能分置于不同舰艇。单舰遭干扰断链只会影响单一环节，不会造成整条作战链瘫痪，体系崩溃风险由此被严格控制在局部范围。

在续接维度，将指挥重建简化为态势对齐。韧性体系预先统一数据模型、时间基准与交互规则，节点断联后可自主重构拓扑，复联后只需校准态势差异，大幅压缩断链恢复周期。俄乌战场上，乌军Delta系统将多源态势汇入同一套云端数据模型，单兵、指挥所、火力单元在同一幅态势共享图上协同，一旦某个终端被毁，备用信道重新接入，数据自动汇入，不需要从组织层面重新对接。

在聚能维度，将分散节点聚合为跨域闭合。节点物理分散降低了暴露风险，但分散本身不产生战斗力。真正的聚能，关键在于共用一套身份与态势底座，使分散的节点随时能跨域协同。前沿传感器发现目标后可直连就近火力单元，无需层层回传指挥中心，网络降级状态下依然能闭合基本杀伤链。分散是为了活下来，聚能是为了打得出去。

把握这一赋能机理，网信体系建设方向也就更加清晰。在建设定位上，应在作战概念开发、力量编组、任务规划阶段就明确断链行动规则与能力底线，把降级运行、毁后再生作为体系固有指标，而非事后补充的应急手段。在架构设计上，要“两条腿走路”，既要强化顶层体系底座的统合能力，也要重视末端战术子网的自愈能力，推动核心节点小型化、机动化、分散化，构建多频段、多路径的异构传输体系。在检验标尺上，把韧性转化为可量化考核的实战能力，常态化设置断链、降级等极限对抗场景，以体系存续时长、指挥链闭环完整度等指标量化评估，在反复对抗中迭代优化体系设计。

（作者单位：国防大学联合作战学院）

认知小站

网状拓扑

传统战术通信依赖中心节点或固定枢纽，所有数据必须先汇聚到中心，再分发出去。一旦中心节点被电子压制或火力摧毁，整个网络即告瘫痪。网状拓扑的运行逻辑在于，包括单兵、无人机等在内的各作战单元既是终端也是网络节点，当某条链路被切断或局部节点被摧毁时，网络能自动寻找替代路径，避免单点失效导致整体瘫痪。俄乌冲突中，双方已经探索运用动态自组织网络，大量使用无人机等充当中继节点，在卫星通信受限后能切换至备用信道。

零信任架构

传统防务网络奉行“内网可信、外网不可信”的城堡式防护。这种模式的致命缺陷，在于内部身份一旦被滥用，边界就形同虚设。零信任架构摒弃内外网边界防护思维，遵循“从不信任、持续验证”的原则，实行最小权限管控。网络内部任一节点、终端、用户都不天然可信，所有访问、数据交互全程审核校验，即使单点被攻破也无法横向扩散，可有效降低网络渗透引发连锁瘫痪的风险。这是当前外军网信体系建设的主流方向。

资料整理：秦国立
版式设计：胡云艳

焦点CT

美军“常春藤集结”演习检验师级网信韧性

■贾　斐

今年5月，美陆军第4步兵师在科罗拉多州卡森堡及皮尼翁峡谷机动训练场举行“常春藤集结”演习，这是该师检验“下一代指挥控制系统”（NGC2）的阶段性收官演训。自2025年起，该师已开展多轮相关测试，重点解决指挥系统分散、数据不通、决策效率低等问题，并检验电磁干扰、网络攻击和通信降级条件下的网信体系韧性。

在指挥控制上，该系列测试从单任务链路验证起步，逐步把各类作战要素接入数字指挥网络，呈现出由功能级、营连级试用向师级联试扩展的趋势。第5轮“常春藤”测试已将NGC2应用范围扩展至60余个战术边缘节点、20余款作战应用和25类以上传感器与打击单元。“常春藤集结”演习则在此基础上实现整师级接入，联网终端设备超过2500台，战术边缘计算机超过130台，接入应用达到40款。第4步兵师在演习中投入多型武器装备，首次将异构平台纳入同一网络，各级指挥节点通过NGC2实现数据联通，使火力、侦察、后勤、防空等要素实现态势共享。

在对抗环境上，美军在演习中有意设置强干扰环境，检验NGC2能否继续依托本地数据独立作业、复联后能否完成态势对齐。美军在演习中安排假想敌对NGC2实施无预警技术攻击，通过挖掘系统漏洞、实施大功率干扰、制造GPS拒止与欺骗环境，并在部队机动过程中同步叠加通信干扰、太空对抗和网络攻击，持续对师级网络高强度施压。与此同时，演习将师级指挥所拆分为多个分散节点，重点检验“分散存续—重新组网—态势对齐”全流程的连续性，以及复联后各分散节点的态势、任务、目标和保障状态的同步能力。

在战术运用上，演习重点检验战术边缘节点支撑快速杀伤链的网信运用能力。在演习中，AH-64E“阿帕奇”武装直升机通过保密数据链和网络化目标指示系统，与地面部队、无人机、炮兵及指挥节点交换数据，实现前沿侦察单元与攻击机组目标信息直通，支撑快速火力打击。参演士兵还使用C-100无人机进行侦察与目标锁定，同时将实时数据整合进NGC2网络，旨在缩短从目标发现到火力打击的时间。美军正通过无人机、保密数据链和网络化目标指示系统，推动侦察、指挥、火力与保障要素数据直通，将网信能力下沉至战术末端。

总体来看，“常春藤集结”演习反映出美军的网信体系建设重点不再只是“联起来”，而是要在强干扰条件下保持持续作战能力。同时也应看到，网信韧性体系的价值取决于其可持续、可负担和自主可控程度，在一定条件下，体系适当分散、节点有冗余，其抗毁韧性越高。

（作者单位：国防大学联合作战学院）