“研究军事、研究战争、研究打仗”专论

透视外军网络战发展新趋势

■周 磊 欧 微

引言 **经过数十年的发展，网络空间已经成为人类社会生产生活的重要领域，成为继“陆、海、空、天”后的第五维战场。近年，美国等发达国家争相出台网络空间战略，组（扩）建网络战部队，实施网络攻防行动，在网络战建设、发展、运用等方面的举动值得世人关注。**

重视网络空间安全，加速构建配套战略与法规条令体系

由于网络空间安全属于新兴领域安全问题，绝大多数国家均缺乏配套战略和法规条令体系。近年来，世界主要国家将其定位为重大安全领域，出台网络安全战略和法规条令的步伐明显加快。如自2000年首次提出国家网络安全战略以来，美国不断制订、拓展、更新各类网络安全领域的政策、战略、法规、条令，仅网络战略就包括《国家网络战略》《网络空间国际战略》《国防部网络战略》和军种网络战略等，以此规范指导网络战建设发展与运用。2014年10月，美军还发布全球首部《网络空间作战》联合条令，对网络空间作战的概念、行动、任务等进行阐述和规范。为应对美国和北约的网络攻击，俄罗斯2014年就公布了《俄罗斯联邦网络安全战略构想》，2016年又颁布了新版《信息安全学说》，提出要确保网络信息安全。为加强网络安全事务的统筹指导，印度于2013年出台《国家网络安全政策》，并计划出台“国家网络安全战略”；印度军方已制定《陆军网络安全政策》《海军信息安全政策》等政策法规。

强化网络战力量专业化建设，注重借助民间网络力量

近年来，组建、整合、扩充专业化网络战力量已在外军中形成风潮。美国是最早提出网络战概念的国家，也是最早组建专业网络战部队的国家。美军2010年成立网络司令部，2018年将之升级为一级联合作战司令部，所辖网络任务部队数量达到133支，约6200人。俄罗斯2013年成立专业信息战部队，网络战是其重要职能。日本自卫队于2014年成立网络防卫队，最初100余人，目前增加至近300人，未来还计划扩建至千人规模。英国2020年也宣布即将创建国家网络部队。在此基础上，外军对网络战力量普遍进行了体系化设计和布局。在网络战领域内，网络攻击、网络防御、网络运维等力量密不可分；在外部，网络战力量与信号侦察、电子战等信息作战力量一体建设、融合发展。如美军网络司令部司令兼任国家安全局局长，网络攻防与信号情报侦察相互融合。日本自卫队专门设立一级司令部，统管太空、网络、电子战事务。

值得注意的是，外军的军方力量构成了网络战力量的“正规军”，民间网络安全公司、科技公司、黑客组织等也成为重要的网络攻防力量，备受重视。臭名昭著的“索伦之眼”“方程式组织”等黑客组织都与美军有千丝万缕的联系，近年来伊朗、俄罗斯、委内瑞拉遭遇网络攻击，都有“方程式组织”的影子。印军也在考虑吸纳其丰富的IT业人才组建网络战后备部队，以进一步壮大其网络战力量。

积极研发和建设网络武器库，智能化武器系统初现端倪

网络武器是用于网络攻防的特殊武器，可以是病毒、漏洞，也可以是拒绝服务攻击、钓鱼攻击等攻防技术，或者是网络攻防系统平台。俄联邦国际信息安全协会理事长阿纳托里·斯米尔诺夫曾于2019年披露西方多个国家在开发网络武器；美国、英国、德国、日本也都毫不讳言拥有网络武器。据斯诺登和“维基解密”的披露，美国情报机构及美军已建设形成了体系化的攻击性网络武器库，有的武器威力堪称网络空间的“大规模杀伤性武器”。2020年英国战略司令部司令帕特里克·桑德斯主动宣称，英国已研发出“摧毁性”的网络武器，能有效杀伤敌国电力网等设施设备。

网络系统平台方面，美军构建了全球最完整的网络战系统平台，包括联合网络指挥与控制、统一平台等指控管理系统，IKE项目等网络战规划与执行基础系统，“舒特”等网络战与火力战一体的武器系统。印度则在网络监视和防御方面开发建设了中央监视系统、网络流量分析系统、网络安全监控与评估系统等系统平台。

网络武器与智能技术有着天然的“亲缘关系”。目前，网络态势监控、网络攻防、密码破译等领域的武器系统，已在网络空间优势国家出现智能化雏形。随着人工智能技术的发展，网络武器智能化的趋势将越来越明显。

着眼增强网络攻防实战能力，创新网络演训方式方法

鉴于网络威胁的现实性和破坏性，外军非常重视通过实战背景下的网络演习和训练活动，检验信息网络系统的安全性，提升军队、政府机构的网络攻防能力。

在参演力量上，涵盖了军队、政府机构、预备役以及民间网络力量。方法模式上，普遍设置对手，确保演习对抗性。有的还创新运用悬赏方式，吸引黑客“合法”攻击特定目标网络，帮助查找网络系统防御漏洞。演训环境方面，积极建设网络靶场，模拟己方及对手信息网络环境。美国、英国、日本、加拿大以及北约均建立了专业网络靶场。作为全球规模最大的多国网络演习，北约“锁盾”演习2019年曾模拟设置了一个国家的信息网络环境。演练内容上，包括响应能力测试、防御漏洞查验、选举干扰分析等。印度定期举行“网络堡垒”演习，据称在2015年组织的“网络堡垒-8”演习中，印度陆军网络大队利用远程渗透等手段，成功获取了印军某网络系统的管理员权限，并发现了13个大类的安全漏洞。此外，美军已开始演练网络战与其他领域作战的融合问题。美军“施里弗”演习中，太空作战与网络战的融合就是重要内容之一。

目前，有的国家已将一些严重网络攻击视为战争行为，随着网络空间国际行为规则对网络攻击的约束和威慑作用越来越强，网络演习可能将取代实网行动，成为外军培育提升网络攻防能力的首要途径。

强调先发制人攻势作战，实战趋向慑战一体多域融合

网络系统的庞大、复杂、脆弱导致网络防御的难度大和成本高，为此，美国等国家将自身网络安全政策和作战思想由最初的全面防御逐步转变为先发制人的攻势作战，强调通过前出到敌方网络中实施先发制人的攻势作战，消除潜在或现实威胁。

在攻势思想的驱使下，网络战在国际冲突中屡见不鲜，而且攻击目标不再局限于军事目标。美国是最早将网络战应用于实战的国家。2009年美军利用“震网”病毒对伊朗核设施实施网络攻击，导致1500多台离心机报废，伊朗核进程被按下暂停键。2020年美军在刺杀苏莱曼尼后，对伊朗革命卫队指挥控制及导弹、防空系统实施网络攻击，威慑、防止伊朗实施军事报复。当然，攻击性的网络作战思想并不要求具有绝对的网络优势，一些非网络强国也提出利用非对称的网络能力对敌弱点实施先发制人攻击的理念，进而在网络博弈中达成以小博大、以弱制强。

值得注意的是，近几场国际冲突中，网络战与火力战、电磁频谱作战、认知域作战等领域的多域融合趋势已经十分明显。如2020年阿塞拜疆与亚美尼亚在纳卡地区爆发武装冲突的同时，双方在网络空间一方面展开网络攻防，一方面也围绕国际国内舆论、军心士气、法理道义等展开了激烈的认知域对抗。

当前，网络战的行动低烈度和模糊特性，吸引着某些国际行为体不计后果频繁实施网络空间作战行动，冲突升级失控的风险正在不断积累。为此，世界各国应尽早展开网络空间国际行为规则和网络武器军备控制的协商谈判，共同制约网络空间军事活动，打造网络安全新格局，构建网络空间命运共同体。

群策集

战略通道安全不可忽视

●从苏伊士运河堵船谈起——

■许 炎

●战略通道是涉及一国经济安全、军事安全和能源运输安全的重大战略问题，在国家发展战略中占据极为重要的位置，必须引起高度重视。

近日，“长赐”号重型集装箱货轮在苏伊士运河横向搁浅，导致包括美军“艾森豪威尔”号航母战斗群在内的几百艘船只被堵在苏伊士运河上下游。作为世界最重要的海运通道之一，苏伊士运河堵船造成的损失全球每天可达几百亿元人民币，这对新冠疫情冲击下的世界经济恢复和发展都产生了影响。这再次警示世人，战略通道的地位重要而特殊，必须充分认识战略通道的地位作用，切实维护好战略通道安全。

战略通道地位作用特殊。战略通道是涉及一国经济安全、军事安全和能源运输安全的重大战略问题，在国家发展战略中占据极为重要的位置，发挥着举足轻重的特殊作用。战略通道是全球物质交换的大动脉，对世界贸易与经济的稳定和繁荣起着关键性作用，一头连着能源资源地，一头连着世界工厂和市场。战略通道一旦堵塞，世界经济活跃度就会骤降，甚至导致某些地区或国家经济梗死崩溃。此次运河堵塞事件几乎让全球供应链“一舰封喉”就是鲜活例子。战略通道是国家经济发展的生命线，绝大多数国家的经济发展对外依赖性加大，对外能源、原材料、市场以及运输的需求及其稳定性要求不断提高。如果战略运输通道不安全，就会给外向型国家的经济运行带来巨大冲击。战略通道是国际战略博弈的大舞台，各国战略利益交汇于此，为便于控制对手供应链同时保护自身供应链，围绕战略通道战略博弈较量持续不断，国际上各种力量围绕着战略通道分化组合，或是结盟或是争斗，推动着世界格局的演变和发展。战略通道是战争胜负天平的控制阀，扼守住这些咽喉要道，就能控制运输的通道和补给线，为赢得战争创造条件；相反，如果失去对战略通道的控制权，就会陷入被动甚至失败的境地。

战略通道安全面临风险挑战。战略通道面临着传统安全和非传统安全威胁叠加的风险。一是地缘政治风险。战略通道所处国家或地区安全形势和政治局势直接影响战略通道安全，地区局势紧张和国内政局不稳成为最为直接风险因素。二是大国介入风险。出于战略博弈需要，有的大国持续对战略通道地区或国家施加政治、经济和军事干涉，导致战略通道地带动荡不安，存在域外大国运用战略影响力或军事手段控制战略通道进而实现排他性运用的风险。三是自然灾害风险。战略通道所在区域总体自然环境比较稳定，但是不能排除地震、火山、海啸、冰冻等突发性自然灾害，这些灾害一旦发生将不是点状破坏而是面状破坏，克服灾难影响难度更大、时间可能更长。四是交通运输风险。战略通道作为交通枢纽，难以避免出现各种交通运输事故等突发事件。五是恐怖袭击风险。当前国际恐怖主义、宗教极端主义、民族分离主义仍然未能得到有效根治，海盗问题、恐怖袭击造成一些战略通道所经过区域风险居高不下。

战略通道安全需要建设维护。切实维护好战略通道安全，是国际社会共同利益所在。要打造多元化运输体系。注重多维空间战略通道建设，促进国际货物运输多样性，加速战略通道多元化，综合运用海洋运输、铁路运输、航空运输、公路运输、运河运输、管道运输等运输方式，形成国际运输综合体系，降低对某一战略通道依赖性。要加强多边化国际合作。通过双边或多边磋商与对话，建立国际协调合作机制，建立争端解决机制，完善危机处理机制，建立综合治理机制，共同维护国际战略通道良好秩序。要构建多样化能力手段。提升反恐、情报、执法、救援水平，切实增强战略通道安全维护的手段，遏制少数国家或组织疯狂掠夺、肆意妄为的举动。要完善实案化反应机制。建立突发事件预警反应的机制，根据突发性事件的性质，实施相应的预警、反应、处理等预案，从而能迅速、有序、高效地组织国际力量，控制突发事件在强度和范围上的扩展，最大程度地减少突发事件所造成的损失。

实施作战指挥须“平衡有术”

■胡有才

观点争鸣

●作战指挥是科学统筹的平衡艺术。实施作战指挥，运筹帷幄、调兵遣将、调整部署等行动，其目的无不是求得自身平衡、破坏敌方平衡，进而夺取作战胜利。

平衡是一种科学统筹的艺术，从某种程度上说，作战指挥也是一种平衡艺术。作战指挥中，需要指挥员根据战场态势、遵循战争矛盾运动规律进行决策筹划与指挥控制，科学统筹，灵活把握“平衡点”，避免“过犹不及”，想方设法确保作战体系的稳定有序运行。

把握指挥跨度与指挥能力的平衡。为了减少指挥层级和信息流通节点、力争扁平化指挥，指挥员通常在本级内平行编组更多的作战单元。但指挥规律和人的思维特点告诉我们，指挥员在作战中通常只能关注5—9个作战单元，作战编组太多，势必造成指挥跨度增大。作战中，指挥员无法做到关注所有单元，或“眉毛胡子一把抓”毫无重点，或“挂一漏万”而顾此失彼、应接不暇，造成指挥失当。因此，在进行兵力编组时，应把握好指挥跨度，既注重编组多元作战力量，该有的单元与要素一个不能少，形成整体作战能力，又注重不超过指挥员思维和指挥通信条件的上限，适当编组，确保指挥跨度与指挥能力的平衡，使作战指挥始终做到统筹兼顾、整体协调。

把握集中指挥与分散指挥的平衡。“兵权贵一”，集中指挥方能保证作战体系形成整体作战能力。现代科技特别是信息技术的发展，使指挥员可远程获取情报信息并对作战行动进行集中管理和控制，推动了决策权上移和集中，便于指挥员实施高度集中统一指挥，以克服下级对作战任务理解偏差和行动偏差。但实际作战中，这种过度集权的指挥方式不仅影响本级对作战全局的整体谋划，还会抹杀下级指挥员的主动性和创造性，甚至给战场带来混乱。因而，应注意把握指挥权限集中的程度，确保集中指挥与分散指挥的平衡，统分结合实施指挥，“统”好意图、目标、任务、规则、资源，防止各行其是；在此基础上，合理“放权周边”，使下级在职权范围内保持决策和行动自主权，作战中能根据战场形势的变化自主定下决心、创造性指挥战斗行动，以赢得战场主动权。

把握情报获取与快速决策的平衡。信息时代作战，遍布战场的侦察监视装备可以适时获取广袤战场的情报信息，“云计算”“大数据”等技术的运用，极大地提高了情报信息精确分析能力，使得有些指挥员企求在精准全面掌握“山那边的情况”基础上进行指挥决策。然而，无论侦察监视与情报分析技术如何发展，“战场迷雾”始终存在，定量分析也有不可逾越的边界。试图精确掌握战场情况、使战场完全“透明”是做不到的。事实上，“一个不够完善的决心比姗姗来迟的正确决心强”。因此，指挥决策过程中，指挥员应科学衡量情报获取的颗粒度，保持情报获取与快速决策的平衡，既要防止忽视情报收集的“情况不明决心大”，又要防止过度追求“战场透明”久拖不决而贻误战机。在获取一定情报信息基础上，及时果断定下决心，快速指挥，做到以快制快。

把握兵力投入与作战效益的平衡。“多兵之旅必胜”，集中兵力是战场获胜的重要法则。为达成力量优势、增大胜算，指挥员往往集中大量兵力于战场尤其是重点作战方向上。然而，过度的力量投入，必然造成指挥、协同、保障等难题，尤其是信息化战场侦察监视能力和打击能力的提升，将给大密度的力量配置带来毁灭性的打击风险，兵力密度越大，损失越大。因此，指挥员在力量使用时，应注意把握兵力投入与作战效益的平衡，因地、因情、因敌灵活部署力量，在恰当的地点投入恰当的力量，做到既要达成能取胜的必要数量优势，又不过度集中，提高作战的效费比。

把握赋予任务与作战能力的平衡。赋予任务时，指挥员通常希望各作战单元进攻作战中歼敌越多越好、夺占空间越大越好，防御作战中坚守时间越长越好、防守空间越大越好。但各作战单元作战能力是一定的，当任务与能力不匹配，要求过高，超出作战能力而赋予过大的作战正面纵深和歼敌数量，不仅无法完成任务，还会造成自身损失甚至影响作战全局。因此，赋予任务时要把握赋予作战任务与作战能力的平衡，在科学分析敌我作战能力基础上，结合战场环境实际，合理确定和赋予各作战单元作战任务，使各作战单元既能满负荷运转、又能对敌形成优势，从而顺利完成任务。

把握行动节奏与全局态势的平衡。“兵贵神速”一直为兵家所重视和强调。信息化战场上，更是要求速战速决。但不顾战场实际，一味追求作战行动的快，往往适得其反。第四次中东战争中，以军第190装甲旅，依仗其快速突击力，高速穿插，孤军进入埃军第2师阵内，反而全军覆没。因此，作战指挥中，应把握行动节奏与全局态势的平衡，依据战略全局和战场情况，合理控制部队行动速度，做到“到得早不如到得巧”，避免“欲速则不达”。特别是信息化战争中，作战行动必须服从于政治、外交、战争战役全局上的需要，该进则进，该停则停，该快则快，该慢则慢，在恰当的时刻出现在恰当的地点，做到把握分寸、游刃有余。

感悟底线思维

■傅泽云 高 凯

挑灯看剑

当今世界正面临百年未有之大变局，局势复杂多变，充满不稳定性、不确定性。这需要运用底线思维界定与防范危机风险。

底线思维是一种战略考量。战略问题是根本性问题，战略上判断得准确，战略上谋划得科学，战略上就能赢得主动。战略思维就是着眼战略问题，为实现全局性和长远性目标而制定科学性、前瞻性和创造性决策的思维，它是一种高瞻远瞩、统揽全局的思维方法。底线思维是战略思维重要思维形式，要从基本国情和基本矛盾出发，着眼于解决关系人民群众切身利益的、攸关国家未来发展的、具有重要性和紧迫性的现实问题，划定具有目标和任务导向的底线，力争做到早谋划、早行动，确保在可控范围内实现预期的目标和结果。

底线思维是一种忧患意识。唯物辩证法告诉我们，事物的质变和量变是辩证统一的，量变的积累超过一定的度就会引起质的变化。在国家治理中，微小的社会矛盾、社会问题如果长期被忽视而得不到有效解决，则会引起负能量的积聚，并在一定外力影响下产生不可预计的后果。底线思维是忧患意识在思维领域的集中体现，是一种具有自觉性、主动性的思维。底线思维要求始终保持谨慎小心、兢兢业业的处事态度，准确把握质变和量变的关系，立足最困难的情况下分析问题，在最坏的可能性上解决问题，根据事物发展趋势和运行状态及早划定恪守的底线，以防止事态向更糟糕的方向发展，避免引起难以预料的后果。

底线思维是一种主动思维。底线思维不是守住底线而无所作为的消极、被动思维，而是着眼最坏、谋求主动，奋发向上的积极、主动思维。底线思维，就是要弄清什么是底线、底线在哪里、超越底线的最大危害是什么、如何有效规避不可预期的风险等问题，从而更好地把握事物发展的规律和趋势。尤其强调要采取积极主动的应对策略，在思想上做好准备，在各种对策上思谋周全。这样，无论出现什么情况，都能相对保持思想上的主动，保持从容不迫的心态。

底线思维是一种积极准备。“凡事预则立，不预则废。”做任何事，以风险危机意识预估可能出现的最坏情况，防患于未然，才能化危机为契机、变挑战为机遇，最终取得成功、获得胜利。底线思维的根本指向，是立足于最坏情况、进行最细致的准备、追求最好的结果；是杜绝“一切撞大运”的心态，把成功建立在穷尽我们所能实现的认知、竭尽我们所能具备的力量上。坚持从成功中查找不成功的因素、从落实中查找不落实的环节、从放心中查找不放心的成分，把导致失败的各种因素尽可能想到，坚持全过程、全方位、全员额准备，实现纵向到底、横向到边的全覆盖，不断提高成功胜算。