北约加强网络防御的“门道”

■陈雅东

近年来，随着网络威胁的不断演变升级，北约持续调整安全政策与战略，并以此为抓手巩固北约“三大核心”任务，即集体防御、危机处理、合作安全，积极抢占全球网络安全制高点。

日前，北约通信与信息局牵头打造新“网络防御社区”，预计将于年底前覆盖29个成员国的网络安全机构，并逐步融入北约作战指挥链。这是北约近年来加强网络防御能力建设的一部分，不仅可为成员国间安全交换实时信息提供最优平台，也可促进相关机构与作战力量实现互联互通，值得关注。

办好“一个论坛”

在北约看来，网络威胁愈演愈烈，其应着重加强与伙伴国、私营企业、学术界的交流与互动，这对于有效应对动态的网络安全威胁至关重要。鉴于此，北约依托网络防御卓越中心，自2009年起在爱沙尼亚举办年度“网络冲突国际会议”。每年有近50个国家的约600名政府首脑、法律顾问和技术专家等出席论坛，他们以跨学科的方式研讨面临的最新网络安全挑战。

论坛对于北约加强网络防御带来三大利好：统一思想，使各成员国提高对网络防御领域的重视程度；促进合作，使成员国间了解彼此的网络防御程序和需求；分享经验，使成员国提高对网络防御最新趋势的认识。

此外，北约希望通过论坛碰撞出更多的创新火花，为其网络防御提供新技术和新倡议。2019年北约第11届“网络冲突国际会议”将于5月举行，主题是“无声的战斗”，与会代表将围绕大数据、物联网、人工智能等新科技对网络安全带来的影响进行研讨。

聚力“两个中心”

北约在网络领域的建设主要围绕教育训练和应急作战两条轴线展开，分别对应两个中心——北约合作网络防御卓越中心和网络空间作战中心。

北约合作网络防御卓越中心，于2008年在爱沙尼亚首都塔林成立。该中心由北约转型与改革司令部认证，汇集了军队、政府、法律等多个领域的专家团队，旨在为北约在网络防御方面提供相关专业知识和业务技能，提高北约整体网络防御水平。其工作规划是通过与北约成员国和伙伴国就网络技术、战略、作战和法律等问题展开研究、培训与演习，为北约网络防御中的关键问题提供最佳解决方案。

网络空间作战中心，由北约国防部长会议于2017年建议设立，是北约将网络空间确定为作战域的落地与延伸，也是北约新一轮指挥结构改革的重要组成部分。2019年年底，北约将出台第一部《网络作战行动概则》，为网络空间作战中心的工作提供基本指南。该中心的成立，将为北约在网络空间的作战行动提供更全面的态势感知能力。

统御“两场演习”

网络演习是适应现代科技飞速发展需要，确保网络技能融入作战指挥链的有力抓手，也是盟国合作处理网络事件的重要平台。北约经过多年的网络实践，形成了两个机制性网络演习，即“锁定盾牌”演习和“网络联盟”演习。

“锁定盾牌”演习具有培训性、技术性、对抗性的特点。如2018年的“锁定盾牌”演习，来自近30个国家的1000余名安全专家编成“蓝队”，扮演国家快速反应小组的角色，与“红队”展开了涉及近4000个虚拟系统、2500余次网络攻击的高强度演习，使参演专家得到技术、法律等全维锻炼。“锁定盾牌”演习每年都会引入新技术、新场景和新挑战。

“网络联盟”演习是北约最大规模网络演习，具有检验性、实战性、跨域性特点。如“网络联盟-2018”演习，全程采取实地实情方式展开网络对抗，着重测试了北约成员国和伙伴国在信息共享、网络空间态势感知、指挥决策程序等方面的情况。演习地点不拘泥于一个国家，参演人员在各自国家异地同步受领任务处置危机。

演好“三大角色”

近年来，北约面临的网络安全形势日趋严峻，如2016年，平均每月发生500起网络攻击事件，较2015年增加约60%。鉴于此，网络空间安全成为北约重点“关照”对象。2014年威尔士峰会上，北约首次将网络攻击确认为其集体防御的一部分；2016年华沙峰会上，北约正式将网络空间升级为与陆地、海洋、天空相平行的作战领域。正如北约秘书长斯托尔滕贝格在2018年“网络防御承诺年度大会”上所指出，北约在其网络空间的使命主要是发挥好三个重要角色，即网络事业的推动者、网络服务的提供者、网络安全的捍卫者。

在推动发展方面，北约主要成员国加大人力、物力和财力的投入。近两年来，北约国家网络事业飞速发展，法国先后投资16亿欧元，雇佣数千名网络专家用于维护自身网络安全；英国组建由1200名网络骨干构成的“第77旅”网络部队；德国建立“网络和信息空间司令部”，旨在保护其信息技术与武器系统免受攻击侵扰。

在服务提供方面，北约聚焦信息分享、专业培训和知识储备等基础类工作。由于传统的电子邮件和信息传输已不再安全，为抵御动态的网络威胁，北约致力于构建一个可安全交互新观点、新创意的平台，使之变为成员国间相互学习、利于培训、彼此借鉴的社区。当前，北约官网提供查询和下载全球90余个国家网络安全战略文本的服务，以及各类相关信息，为便利成员国学习和借鉴发挥着“智库”作用。

在捍卫网络安全方面，北约可谓“全面着眼，软硬兼施”。如依托北约防务学院，就网络防御的政治和军事问题提出战略构想和远景蓝图；依托美国和欧洲的技术与实战优势，共同制定关键设施保护规划，评估网络防御态势；依托“恶意软件信息共享平台”，全时全程监控各类网络威胁事件；依托北约网络应急快反团队，实时适时帮助盟国处理网络危机与挑战。

整体来看，近年来北约在网络领域投入较大、用力甚多、收获也不小。然而，在网络安全领域没有单一规则可以遵循，没有单一安全对策可以规避网络安全的所有风险。正如北约副秘书长罗斯·高特莫勒所坦言，“当网络危机发生时，北约并没有办法迅速化解一切问题”。

未来，北约在网络安全防御方面仍面临诸多问题：网络危机触发战争行动的门槛难以界定，到底多大规模的危机能够启动北约宪章第五条，北约至今仍未给出明确说法；法律的核心问题难以突破，如《欧盟基本权力宪章》第八条规定“任何人都有权利保护其个人资料”，大部分北约盟国在保护隐私权与加强网络监管之间摇摆不定；网络主权的让渡问题仍然难有进展，北约29个成员国情况复杂、诉求多元，彼此间难以达成共识，如法国就明确表示自身网络资产的独立性，北约无权调用其网络力量。因此，北约网络安全之路走向何方，仍有待观察。

资料提供：陈雅东
本版制图：梁 晨

军眼观察

美俄博弈迎来“新风暴”

马其顿今年一月更改国名为『北马其顿共和国』加入北约——

■阮光峰

日前，北约29个成员国代表在布鲁塞尔总部同马其顿签署加入北约议定书。议定书走完成员国国内程序后，马其顿将正式成为北约第30个成员国。随着北约东扩“再下一城”，以美国为首的北约与俄罗斯的博弈也将进一步加剧。

马其顿为加入北约，可以说是费了九牛二虎之力。早在1995年，马其顿就加入了北约的“和平伙伴国计划”，并在1999年成为北约“成员国行动计划”的一员。2008年马其顿的北约成员国申请，因国名争议被希腊方面予以否决。希腊认为“马其顿共和国”的国名暗示其对希腊北部马其顿省有领土和文化遗产的要求，并坚持让对方改名。多年来，马其顿与希腊互不相让。作为北约成员国，希腊通过一票否决权多次拒绝马其顿加入北约的请求。直到今年1月，马其顿决定做出妥协，其议会通过决议同意将国名更改为“北马其顿共和国”。随即，希腊为其加入北约“亮绿灯”——希腊议会首先表决批准北马其顿加入北约议定书。

其实，马其顿一心要加入北约，不免有“依靠大树好乘凉”的利益考虑，想要获得较快的经济发展和安全上的保证。但不可避免的是，这也将加剧美欧和俄罗斯两大力量的博弈，使其深陷大国斗争的漩涡。

对北约来说，马其顿地缘位置重要，北约可利用其进一步控制巴尔干地区，不断压缩俄罗斯战略空间。马其顿东临保加利亚，南临希腊，西临阿尔巴尼亚，北临塞尔维亚，地处巴尔干核心和南下地中海的门户，历来是重要的贸易和军事通道，也是北约东扩的必经之路。为此，北约一直对马其顿强力拉拢，自1991年以来，美国为马其顿总共提供了约7.5亿美元的援助。当前，巴尔干地区仍然面临着科索沃问题和波黑问题，北约成功解决马其顿与希腊的争端，可为日后经营巴尔干地区提供有效借鉴，有利于把巴尔干各国进一步整合到北约和欧盟框架内，从而进一步削弱俄罗斯在巴尔干地区的影响力。美方宣称“马其顿加入北约将成为俄罗斯的噩梦”，其“拉欧抗俄”的战略意图可见一斑。

对俄罗斯而言，北约东扩破坏了地区平衡，严重威胁和挑战了其国家安全。俄罗斯一直将巴尔干地区视为其传统势力范围。随着巴尔干半岛的保加利亚、罗马尼亚、黑山以及马其顿加入北约，俄罗斯担心产生“多米诺骨牌”效应，使格鲁吉亚、波黑等原本就心向北约的国家更加急于加入北约。因此，俄罗斯对马其顿加入北约表示强烈反对，认为这是北约的又一次严重挑衅，坚决反对北约“把基础设施和整个军事联盟继续向俄方边境推进”，并指出马其顿将“失去独立的外交决策权”“增加国防开支、承担北约相应份额的军事费用”。

面对北约的不断扩张，俄罗斯很可能对其施加的压力做出强力反应。俄罗斯国防部长绍伊古不久前指出，北约军事实力的增长破坏了世界现行安全体系，俄罗斯将被迫采取回应措施，并宣布增强西部军区兵力。俄近来还不断强化其核力量，加紧研发新概念武器，一些先进武器即将列装或已研制成功，如S-500防空导弹系统、最大飞行速度超过10倍音速的“匕首”高超音速导弹、“海燕”核动力巡航导弹、“波塞冬”核动力无人潜航器等。可以预见，俄罗斯与北约的战略博弈将呈现出一个长期复杂和螺旋式上升的态势，美俄对抗的强度也会进一步提高。

需要指出的是，一个不断扩大的组织必然面临着规模和凝聚力之间的悖论。随着北约“入伙”的成员国越来越多，不同国家出于经济发展水平、民族宗教、安全关切的差异，对北约的倚重程度各不相同，因此其分担防务的意愿也有所区别。成员国间的矛盾和离心力也将日趋凸显，北约的负担和内部协调难度随之增加，甚至导致其陷入整体弱化的困境。

网络战

网络战也称信息战，是为干扰、破坏敌方网络信息系统，并保证己方网络信息系统的正常运行而采取的一系列网络攻防行动。

网络战正在成为高技术战争的一种日益重要的作战样式，它可秘密地破坏敌方的指挥控制、情报信息和防空等军用网络系统，甚至可以悄无声息地破坏、瘫痪、控制敌方的商务、政务等民用网络系统，可谓不战而屈人之兵。

网络战分为战略网络战和战场网络战。战略网络战又有平时和战时两种。前者是在双方不发生火力杀伤破坏的战争情况下，一方对另一方的金融、交通、电力等民用网络信息系统和设施，以计算机病毒和黑客等手段实施的攻击。后者是在战争状态下，一方对另一方战略级军用和民用网络信息系统的攻击。

战场网络战旨在攻击、破坏、干扰敌军战场信息网络系统和保护己方信息网络系统，其主要方式有：利用敌接入路径和各种“后门”，将病毒送入目标计算机系统；需要时利用无线遥控等手段将其激活；采用各种管理和技术手段，对己方信息网络系统严加防护。

1991年海湾战争中，美军就对伊拉克实施了网络战。开战前，美国中央情报局派特工到伊拉克，将其从法国购买的防空系统使用的打印机芯片换上了含有计算机病毒的芯片。美在战略空袭前，利用遥控手段激活病毒，致使伊防空指挥中心主计算机系统程序错乱，防空系统失灵。

网络已经成为提升军队作战能力的“倍增器”，各国加速争夺制网权，网络军事竞赛已然开启。

（陈伟鑫、史云皓辑）

乌尔姆——

北约军事战略新“支点”

■初 颖 刘小辉

近年来，北约和俄罗斯围绕乌克兰东部局势博弈不断，北约频繁在东欧临近俄边境地区举行演习，还在德国乌尔姆组建了联合支援保障司令部，以快速响应盟国或伙伴国安全事态，支持北约对抗潜在或现实威胁。乌尔姆——这一传统军事重镇，也再次成为欧洲地区的战略要地。

乌尔姆是德国南部巴登-符腾堡州的一座城市，位于多瑙河畔。它附近的大城市有斯图加特和慕尼黑，居于德国经济和文化核心圈。特别是军事文化氛围浓厚，城市内随处可见军营式建筑和军事教育与宣传机构。正如德国媒体所指出，选择乌尔姆作为北约在欧洲的后勤支援与保障基地，既在于它的地理和资源，也缘于其深厚的军事文化。

历史上，乌尔姆的发展与繁盛几乎都与战争如影随形，并在战场或大国集团博弈对抗中扮演了关键角色。

16世纪起，这里就成为欧洲强国角逐的战略重地。特别是在1805年的法奥战争中，拿破仑通过快速机动战术发起并赢得乌尔姆战役，让俄英奥联军被迫后撤，转入战略防御，由此乌尔姆在欧洲地区的地缘战略价值更加凸显。一战前夕，乌尔姆作为重要军事要塞，在人口不足6万的情况下，仍有1万人担负驻军任务。二战时期，这里也是各大国竞相争夺之地，并因此遭受轰炸，建筑物被严重破坏。

尽管历经数次残酷的战争，当地人对在乌尔姆组建联合司令部仍普遍持积极态度。因历史原因，二战后德国在战争中更多是在后勤支援、地区维和等领域发挥自身作用。而这也成为在该地组建军需支援联合司令部的重要推力。

其实，早在2013年，德国联邦国防军就已经在欧洲快速反应部队行动司令部框架下，在乌尔姆主导组建了一个多国联合部队司令部，所属人员来自20个国家的陆、海、空军和医疗服务部队，主要任务是组织北约和欧盟部队人员联合训练，以及为执行人道主义救援和地区维和等任务提供物资技术保障。对此，西方媒体指出，高效的战斗预置、一流的训练水准以及最先进技术设备支撑下的指挥通信系统，能够确保部队随时、快速部署。

如今，凭借乌尔姆完备的通信与指挥控制设施，联合支援保障司令部已与北约和欧盟防务机构建立起顺畅的协调关系，并组织了危机事态下人员物资和装备的快速转移、欧洲内部兵员与物资调遣等程序演练。根据计划，该司令部将在2019年形成初始作战能力，与多国联合部队司令部协同应对日益复杂的欧洲安全形势，并在2021年底前具备全面作战能力。

下图：美军士兵参加北约大规模年度海军军演“波罗的海行动”。

新华社发

日本拟向埃及西奈半岛派遣陆上自卫队员——

频频“解扣”为哪般

■袁 杨 薛 军

据日本媒体报道，日本拟于今年春天向设于埃及西奈半岛的“多国部队观察员团”派遣陆上自卫队员，以负责监视以色列和埃及停战活动。这再次凸显了其为扩大自卫队海外活动范围“解扣”的意图。

事实上，海外派兵行动在日本国内并不是一个新鲜话题。早在上世纪50年代，日本就曾秘密研究过这一问题，并在1958年中东危机和1961年刚果“内乱”时，试图参加联合国维和行动。1987年的两伊战争和1990年的海湾危机期间，日本政府也都曾试图派遣自卫队前往海湾地区，并向国会提交了相关法律案，但均因遭遇在野党和舆论界的反对而作罢。即便如此，1991年3月，日本还是以确保本国船舶航行安全为由，派遣了海上自卫队扫雷舰前往波斯湾，开创了日本战后首次“海外派兵”的先例。

1992年6月，日本以“强大的国际压力”为名义，出台了《国际和平合作法》，这成为自卫队跨出国门、走向世界的第一块垫脚石。随后，日本便派遣了陆上自卫队员前往柬埔寨参与维和行动。在此后二十余年的时间里，日本自卫队还先后赴莫桑比克、卢旺达、东帝汶、尼泊尔、海地、伊拉克和南苏丹等国参与联合国维和行动和国际救援活动。

日本自卫队的这些海外派兵行动，在安倍政府上台以来不断扩展。安倍力推“积极和平主义”，其核心内涵是以日本的主动作为争当国际安全舞台的主要玩家，树立日本自卫队正面形象，并依靠防卫力量的国际化，即通过显示“海外军事存在”，为实现其“政治大国”目标“造势”。

在安倍政府的大力推动下，近年来日本不断架空安全与防卫政策“专守防卫”原则，有步骤地为海外派兵行动“解扣”，逐渐降低海外派兵门槛。如通过施行“新安保法”，日本为其进行战争动员、强化日美安全合作，以及参与海外军事行动提供法理保障；通过解禁“集体自卫权”，日本可实现为其“关系友好国家”提供“军事支援”的目的；通过修订“日美防卫合作指导方针”，日本进一步扩大化其防卫自主权，单独遂行“军事行动”的领域大大拓展；通过《国际和平支援法案》，日本可随时根据需要向海外派兵并向其他国家军队提供支援；通过出台新《防卫计划大纲》和《中期防卫力量发展计划》，日本从体制到装备做各种准备，为自卫队走向海外进行最大限度的预先赋能。

从未来发展来看，日本海外派兵将从“有限参与”走向“全面介入”，日本自卫队越来越多的人员将成建制地被派遣到海外参与多国联演、国际维和等行动。这一趋势将大大降低日本在海外强化军事存在的国内外阻力，甚至会助力其实现在海外常态化“驻军”，日本军力发展更会逐渐丧失“和平安全阀”，将严重影响地区和平稳定，值得国际社会高度警惕。