首次举行国家级“断网”演习，旨在全面加强网络安全防护——

俄积极备战网络空间

■于淑杰 许斌 欧翔

军眼聚焦

俄罗斯前不久举行了首次国家级“断网”演习。演习期间，俄主要研究了其电力设施的网络安全问题、政府部门间协作水平、通信网络故障检修能力以及在遭遇外部断网时俄境内互联网运行的完整性和安全性等。俄此次演习既是对外部网络威胁的一次震慑，也将对全球网络安全格局产生深远影响。

目的是打破美国在网络空间的“一家独大”

早在2014年，俄政府便开始酝酿“断网”演习，并于当年举行“特别网络演习”，2017年又进行第二次，此次为第三次，同时也是首次国家级“断网”演习。俄连续举行“断网”演习，背后动因主要有：

维护网络主权安全的迫切需要。俄认为，美国对互联网根服务器的垄断和在网络空间的霸权，导致国际法的主权平等原则受阻。同时，互联网所具有的开放性和不确定性使敌对势力通过操纵网上舆论、攻击服务器和数据中心、收集敏感信息等形式，对特定国家的网络空间展开战略性袭击。为打破美国在网络空间“一家独大”的局面，俄主张国家对信息网络空间行使主权。2011年，俄发布《国际信息安全公约草案》，明确提出“所有缔约国在信息空间享有平等主权，缔约国须作出主权规范，并根据其国家法律规范其在信息空间的权利”。2017年，俄提出独立于全球域名系统的“独立互联网计划”，以避免在政治、军事等危机中被美故意切断互联网连接，使其成为信息孤岛。

抵制个别国家将网络空间转变为国家间对抗空间的企图。2018年9月，美国防部对外发布《国家网络战略》摘要，认为美国正处于来自俄罗斯等国长期战略竞争的安全威胁之中，需通过提高网络空间作战能力等举措来加以应对。为此，俄总统普京于2019年5月签署了《主权互联网法》，为互联网流量经由政府控制的基础路由器传输确立法理依据，也使非常时期的“断网”合法化。根据该法案，俄将在境内建立独立的网络基础设施，每年至少举行一次“断网”演习，并将从2021年1月1日起，俄公民、企业和组织只可使用国家主权网络，俄国家机关必须使用国产加密信息设备。

紧急时刻，确保俄内网与互联网“无缝切换”

其实，俄并非想另建一套与国际互联网不兼容的网络体系，而是想通过建立“备份”解析服务器，以“无缝切换”的方式维持网络互联，且完全不影响网络用户的日常使用。通过剖析俄内网软硬件基础架构，可窥见其完成“断网”的技术基础。

建立备份域名解析服务器。1989年，美政府建立互联网域名与地址管理机构，以管理支撑互联网运转的13个根域名服务器。其中，唯一的主根服务器设在美国，12个副根服务器中有9个在美国，这是美国网络霸权的硬件基础，美可借此控制全球互联网的域名解析服务，即控制全球网络的通断。2019年2月，据俄《主权互联网法》拟制者之一、议员克利萨斯披露，俄已向本国网络通信企业投资200亿卢布，建立了自主的全国域名系统和自主地址解析系统，可在紧急时刻通过暂时“切断”外部网络连接并改用本国主权网络“RuNet”，确保网络空间安全。

建立物理隔绝的军用互联网。俄军和军工企业集团为确保自身大量敏感信息的安全，已启动“与世隔绝”的专网建设。2016年，俄国防部开始建设名为“数据传输闭环系统”的军用专网。2019年4月，俄国防部又展开专属的军事互联网——“多服务通信传输网”（MTSS）建设。据悉，该网能够在全国范围内快速传输大容量信息，同时还拥有穿越北极海底的专属光纤网络，可保证战时稳定运行。未来“数据传输闭环系统”将并入该网，故MTSS也被称为俄“军用互联网”，能够通过物理隔断达到全面防御外网攻击的目的。

建立独立保密数据库。建立与国际互联网物理隔绝的军用独立数据库，可使俄军在“断网”条件下依托“军用互联网”确保军事数据的存储、加密、交换和备份等功能正常运行。据俄《信息报》披露，俄国防部已投入3.9亿卢布，在2020年前为各大军区建成“超级保密iCloud”，即保存内部和秘密信息的保密“云库”，并成立分区设置的数据处理中心。目前，俄军西部、南部军区的集团军和驻叙军队集群已拥有保密“云库”，数据中心不但受到严密保护，还拥有自主电源、可靠的冷却和消防系统。

建立基于可信任软硬件的信息生态圈。2018年1月，俄军宣布将使用俄公司开发的Astra Linux操作系统取代原Windows操作系统，以降低网络安全风险。此外，2019年12月2日，普京签署了有关要求在俄销售外国手机等IT产品需预装俄产软件的法律。该法将于2020年7月1日生效，目的是保障俄国家信息安全，以高度可信的俄产网络设备和软件为基础环境，打造逐步隔离西方敌对势力的信息生态圈。

通过演习，实现“一石多鸟”

俄通过此次演习达到了“一石多鸟”的效果。一是检验了俄国家主权网络的强大功能。由国产信息技术支撑的俄国家主权网络在不依赖国外任何服务器的情况下仍能正常运转，充分证明俄信息技术水平已达到相当高的水平；二是摸清了俄境内网络安全方面存在的一些“暗桩”，为俄下一步有针对性地防范和抵御各种网络攻击、加强网络安全防护、提升反侦察情报能力提供了明确的“靶子”；三是全国性“断网”虽是应对强敌网络进攻的最后保底手段，但也不啻为一种战略威慑。立足最坏情况演练最后保底措施，正如同核武器试验一样，同样能起到对网络威胁进行威慑的效果；四是通过使用“主权互联网”理念对个别国家的网络霸权提出挑战，无形中削弱和抵消了对手的网络战能力。

（作者单位：军事科学学院）

此前，一款新型勒索病毒“坏兔子”在欧洲国家蔓延，涉及俄罗斯、乌克兰、德国、土耳其等国，受害者包括俄罗斯的国际文传电讯社、乌克兰敖德萨国际机场、乌克兰基辅地铁系统等欧洲多国基础设施。多家网络安全机构监测分析发现，“坏兔子”会以感染的设备为跳板，攻击局域网内的其他电脑，形成“一台中招，一片遭殃”的情况。图为俄罗斯网络安全公司的一名员工在电脑前工作。

新华社发

军眼观察

『世纪协议』缘何难换中东和平

阿盟日前宣布拒绝接受美国政府提出的『中东和平新计划』——

■李瑞景

美国总统特朗普与以色列总理内塔尼亚胡日前联袂抛出“中东和平新计划”的政治方案，连同此前已公布的经济方案，美以的“中东和平路线图”清晰可见。2月1日，阿盟外长紧急会议宣布，拒绝接受美国政府提出的“中东和平新计划”。

根据目前透露的消息，该计划主要包括以下内容：其一，以色列在耶路撒冷建都，而将耶路撒冷东郊定为未来巴勒斯坦国首都；其二，以色列保留现有约旦河西岸犹太人定居点以及其间的交通网，同时承诺冻结定居点建设；其三，巴勒斯坦放弃难民回归权；其四，巴勒斯坦国非军事化，不能建立正规军队；其五，国际社会将向巴勒斯坦投资，规模预计达500亿美元。

美国和以色列认为，这份“世纪协议”是对巴勒斯坦的“大让步”，是送给世界和平的一份“大礼物”。美方更是声称，该协议至少将为巴以带来80年的和平。讽刺的是，作为协议的另一方，巴勒斯坦总统阿巴斯却称，“我们已经讲了一千次了，不！不！不！”伊朗更称，这份协议是一场“大骗局”，是扇向巴勒斯坦的一记“大耳光”，连80分钟的和平也维持不了。

之所以针尖对麦芒，主要是因为相关方思考问题的基点根本就不在一个维度。美以“中东和平新计划”的核心是“投资换和平”，立足点在于要巴勒斯坦人“承认现实”，即承认打不过以色列，还不如放弃一些已经丧失的权益，以换回一些现实的经济利益。而这与巴勒斯坦建立以东耶路撒冷为首都的独立国家的目标背道而驰。正如美国前国务卿奥尔布赖特所说，只有当巴勒斯坦人关心自己的孩子甚于关心耶路撒冷是否是以色列首都之时，中东和平方可实现。

美国这种厚以薄巴的做法，使该计划注定失败：其一，从巴勒斯坦内部而言，妥协的声音难占主流。即便有部分人想当“精致的利己主义者”，安心过小日子，但他们终归不敢发声。因为一般而言，面对战和问题，主战派比主和派能量大，激进派比温和派有市场，主张达成和平协议的人很容易被扣上“软弱”甚至是“卖国”的帽子。而且，主战派也自有其道理——反抗武装也曾逼使以色列从黎巴嫩南部和加沙地区撤军，更何况，即便现在真的打不过，还可以等待未来的变局，一切皆有可能……总之，巴勒斯坦很难认命，阿巴斯的发言正是对民心的回应。

其二，对周边一些有影响力的伊斯兰国家而言，他们不可能轻易认同该计划。比如最近几年都在同美国“硬杠”的伊朗，就不可能不反对。伊朗最高领袖哈梅内伊就表示，如果承认耶路撒冷掌握在犹太人的手中，这就是愚蠢的。伊朗最高领袖外事顾问韦拉亚提更称：“伊朗将不会保持沉默。伊朗领导人以及伊朗人民都将巴勒斯坦问题视为伊斯兰世界的头等大事，并将竭尽所能继续同支持巴勒斯坦的其他阿拉伯国家共同协商。”从某种程度而言，伊朗政权一直将保护圣城耶路撒冷、维护伊斯兰兄弟利益视为其政权存在的合法性支柱，因此自然不会坐视不理。更何况，伊朗也一直将巴勒斯坦问题视为同美国博弈的重要战场，更不能轻易放弃。

正是看到了问题的复杂性和各方利益的不可调和性，联合国中东和平进程特别协调员尼古拉·姆拉德诺夫表示，“中东和平新计划”不是巴以和平谈判的基础。美国中东问题专家班纳曼也表示，单方面改变耶路撒冷地位以及巴以边界的做法，破坏了美国此前的承诺以及与有关方面达成的协议，将会对美国过去作出的承诺造成难以逆转的破坏，并将使巴以和平前景受挫。

不知美方在推出该计划时，是否也想起过40多年前美国主导达成的“戴维营协议”。其实，美以要实现真正的和平，还需回到“土地换和平”原则，回到国际社会普遍支持的“两国方案”，即“以1967年战争前边界为基础建立两个国家”。看来，要解决巴以问题，还要少些利益算计，多些对和平的关心。

强调应对新型威胁——

英“国家网络部队”呼之欲出

■孔 刚

外军纵览

据媒体日前报道，英国即将组建完成一支安全部队——“国家网络部队”。该部队主要负责发动进攻性网络战，打击对英国构成威胁的恐怖组织、敌对国家和有组织犯罪集团。这是英国为了应对近年来国家安全面临的复杂形势，尤其是在新兴的网络安全领域，国际斗争日趋白热化，以及日益增多的网络攻防事件，而采取的一项重大安全举措。

据英国媒体透露，这支部队将由国防部和政府通信总部共同负责，指挥和控制权由两大部门共享，人员预计将从武装部队、情报部门、学术界以及私营部门招募。

英国对网络安全的重视由来已久。早在2011年11月政府内阁办公室出台的《英国网络安全战略：在数字世界中保护和促进英国利益》的文件中，便指出“国防部正在加大对网络安全的投入”，“新组建的联合力量司令部将从2012年4月起负责领导网络防御能力的发展与相互整合”。近年来，英国遭遇的网络安全事件频频发生。在西方媒体所谓“俄罗斯干预欧美国家大选”、俄前特工在索尔兹伯里中毒等事件中，英国都感受到了对手在网络空间施加的巨大安全压力。与此同时，在近年来打击国际恐怖主义的斗争中，网络与新兴媒体也是国际社会与极端主义势力展开激烈攻防的一大战场。英国恰恰处于多个国际安全焦点议题中，强烈地感受到来自网络空间的多重威胁与安全压力。这些压力加速推动了英国网络安全力量的壮大与成熟。

这支国家网络部队的核心是英国陆军第6师下辖的第77旅，号称“网战007”。但正如英国防务战略的整体面貌一样，这支部队也非“独行”，而是牢牢地依托并服务于北约。在2011年发布的战略文件中，英国便强调自身的网络力量建设要与2010年北约的“战略概念”保持一致。乌克兰危机发生后，网络攻击行为是否适用于集体防御范围，成为北约近年来重点研究的课题之一。英国在此方面的立场十分积极。在2019年底的北约峰会上，防务大臣本·华莱士公开表态，英国将做第一个向北约提供网络进攻能力的盟国。

在实践中，英军第77旅已经实施了相关行动。据俄罗斯媒体透露，在2018年底俄乌关系紧张之际，这支部队曾前往乌克兰培训当地军事部门使之避免遭受网络攻击，并从事信息战。当然除了重点防范俄罗斯以外，英国家网络部队还将全力应对各类极端组织发起的临时网络攻击行动，以及涉及武器、人口和毒品走私的犯罪网络。

英国国家网络部队的职责范围预计将相当广泛，其对国家安全的重要性可想而知。然而，这支部队仍将面临一系列困难。首先，这支部队的财力支撑相当有限，不够充裕。其第一年的预算仅有7600万英镑，与2018年美国用于网络空间的80亿美元国防经费相比，这点预算可谓杯水车薪。财力的不足将严重制约国家网络部队的能力发展与人员招募。其次，英国近年来在脱欧的道路上一波三折，在这一漫长过程中，相关政府主管机构领导人的频繁更迭，导致国家网络部队的组建与成军一再被推迟。最后还有一个问题不容忽视，即英国需要将其国家网络部队的作战行动，与其更大范围的外交行动协调起来。

在此情况下，英国将如何应对，这是摆在国家网络部队乃至英国更高层决策者面前的一道难题。

（作者单位：国防科技大学）

贾巴尔空军基地——

美在波斯湾的“战场前哨”

■刘磊娜 初颖

兵史地志

在美国和伊朗关系持续紧张之际，有外媒报道称，美国海军陆战队第251战斗机攻击中队的12架F/A-18C“大黄蜂”战斗机，日前已部署至科威特贾巴尔空军基地。该基地是美军西南亚联合特遣队“大本营”，曾在海湾战争和打击“伊斯兰国”行动中充当联军战斗机前沿基地。美此番增兵让中东局势更趋复杂，贾巴尔空军基地也成为美在波斯湾空中军备力量的重要枢纽。

贾巴尔空军基地位于科威特城西南56千米处，临近波斯湾，距离伊拉克南部边境线仅120千米，拥有两条3500米长的机场跑道，因身处沙漠地带，又被称作“沙漠机场”，是美扼控战略通道的重要空中力量驻扎地。部署此处的西南亚联合特遣队，由第332远征大队、第332远征空中支援行动中队、第4406作战大队、第4406空中支援行动中队和第9情报中队组成，总兵力约1500人，以3至4个月为周期实施人员轮换，常态化负责叙土边境—伊拉克—沙特阿拉伯—波斯湾一带空域的战备警巡，具备丰富的地区行动经验。

贾巴尔空军基地是美军中东整体战略的一个“缩影”。1992年8月，美国等在伊拉克南部地区划设“禁飞区”，并依托贾巴尔空军基地实施代号“南方守望”的监视行动，在随后的对伊拉克军事打击行动中，大批战斗机也由此起降完成作战任务。1998年底，美在此组建第332空中远征部队，进一步强化地区存在。

2003年10月，美在强化中东地面力量基础上，对空中兵力进行整合，贾巴尔空军基地的大部分资产被转移到邻近的萨利姆基地，仅保留维持日常运营的部分管理人员。2014年10月，美以“反恐”、“维持地区秩序”之名重返该基地，并邀请盟国力量加入，包括丹麦皇家空军的7架F-16、意大利空军的1架KC-767，该地成为美携欧洲盟友联手介入中东局势的重要支点。

2016年10月，美展开对“伊斯兰国”大规模军事打击行动，贾巴尔空军基地再次成为重要依托。美西南亚联合特遣队以此为驻地展开精确打击、空中搜索与救援、侦察监视、运补保障等行动。这里充当起美国和盟国反恐的中转与后勤中心。

在此轮中东局势升级背景下，贾巴尔空军基地被西方媒体视为美在波斯湾的“战场前哨”和空中战力集结地。去年9月，为因应伊朗封控霍尔木兹海峡的军事示强，美曾从卡塔尔调派F-22隐形战机部署至贾巴尔空军基地予以应对。

此外，贾巴尔空军基地与卡塔尔乌代德、阿联酋达哈夫拉和约旦姆瓦法克空军基地，形成方向上互为策应、战机谱系多元、处置响应灵活的空中军备布势，共同构成美在波斯湾西侧空中战场力量网络。此次，美高调派遣战机助阵中东，且选择贾巴尔空军基地为临驻点，突显出美军的威慑策略，也显示出贾巴尔空军基地在美中东战略“网格”里的重要地位。

下图：贾巴尔空军基地俯视图。

资料图片