



“网络反导”：防御利器还是潘多拉魔盒

□ 刘杨铨 石海明

“网络反导”的构想并非凭空出现。近年来美国始终致力于包括网络武器在内的新技术研发，意图通过所谓“主动抑制发射”的方式，即在对对手战略导弹发射前侵入其指挥控制系统或核心部件，抑制导弹发射，达到事实上的反导效果。这一构想背后暗藏的危險信号，值得整个国际社会警惕和反思。

进一步加速战略疆域深度融合

随着网络攻防对抗从虚拟目标扩展到物理目标，网络与核、太空等战略疆域的相互关联和相互影响逐渐凸显。美国和以色列针对伊朗核设施发动的“震网”攻击，首次展示出网络武器干预核力量对比的潜在能力。由于网络攻击手段日益多样化，即使核武器指挥控制系统和民用核设施这类与外界高度隔离的平台，也存在一系列可能遭致网络攻击入侵的弱点。外层空间设施同样无法幸免。信息支援本身就是空间能力发展的重要功能，这意味着信息流动带来的安全风险亦会波及外层空间。现有的理论和实验证据已经表明，网络攻击能够干扰或阻碍卫星与地面的通讯联系，甚至能直接侵入空间设施的控制系统，造成其运转失灵或是偏离轨道。美国众议院一名议员直接表示，使用网络手段攻击卫星应被视为战争行为，这从侧面也反映出网络与太空愈发增强的联动性。

但战略疆域加速融合也会带来一系列安全挑战。首先，基于单一领域的战略威慑将难以为继，因为某领域内建立起的威慑平衡很容易被领域外的技术发展所抵消。其次，由于核、太空、网络等领域均具有鲜明的军民两用性，这些领域的安全联动将使用基础设施置于连带威胁之下，这将极大提高一国维护战略安全的成本和可能遭受不必要损害的风险。对于美国的网络反导来说，上述挑战意味着其意欲建立的单方面战略优势可能难以实现，因为其他国家同样可能发展

非对称的打击能力来破除美国的反导“神话”，而这将导致美国军用和民用关键设施的脆弱性不降反升。从这个意义上看，网络反导恐怕只会开启新的潘多拉魔盒，释放出扰乱新兴战略领域安全稳定的危险因子。

进一步刺激网络空间军备竞赛

从2015年乌克兰电力设施遭到网络攻击导致大范围断电，到今年美国大选期间出现针对选举系统的网络侵袭，网络攻防对抗已不仅仅是过去的黑客行为或政治宣泄，而是越来越多地与特定的战略目的联系在一起。美国网络反导的构想更是具有明确的战略指向，清晰地显示出将网络攻击手段作为有效军事工具的意图。近年来，美国已经通过一系列举措大力推进网络攻防向实战化战术化发展。建立网络司令部、组建网络任务部队、出台网络作战指导规划、开发网络武器集成平台，这些措施使得网络攻防能力逐渐嵌入美军作战力量体系，也加速了网络军事化的总体趋向。将网络攻击纳入全球反导布局只会使美国在网络军事化道路上越走越远。其后果必然会刺激各国加强网络军事能力建设，使本已硝烟渐浓的网络空间安全环境进一步恶化。按照英国一家智库开展的年度军力评估，截至2014年底已有大约35个国家建有不同形式的网络战力量。美国挑起的网络军事化浪潮必将使这一数字不断升高。随着网络空间军备竞赛加剧，各国在网络空间的安全互信无疑会受到严重削弱，针对他国开展的网络军备建设和力量部署可能会更为显著。如果一种朝向冲突演化的安全文化在网络空间国际互动中占据主导，安全困境将不断加深并为网络空间国际秩序带来普遍伤害。

进一步动摇全球体系战略稳定

冷战后美国在全球部署反导系统，意欲通过牺牲他国的安全来换取自身的“绝对安全”，这已经严重削弱



了冷战以来的全球战略稳定的基础。而网络反导还想将这种部署“更上一层楼”，无疑是极不负责任的火上浇油之举。不仅如此，网络反导构想本身也包含诸多不稳定因素。一是容易引发大国关系的紧张对峙。与传统的战略武器和常规武器不同，网络武器及其攻击方式更为隐秘，一国对他国网络武器的性质、规模、效果等要素难以做出准确评估，这使得网络条件下的战略互动关系将建立在极不透明的基础上，对战略能力和意图的判断很容易出现重大偏差。美国若将网络攻防介入战略互动体系，必然对其他国家的战略威慑能力构成新的挑战，从而引发后者新的不安和战略反制，损害新型大国关系的稳定基础。二是容易导致突发事件和危机升级。追踪溯源和身份识别是网络攻防中的重要难题。特别是由于各类非国家行为体同样具备一定的网络攻击能力，国家间网络安全互动将面临更多不确定性，突发事件导致的战略误判和冲突升级风险大大增加。三是容易成为发动先发制人打击的借口。网络反导并非在战略武器发射后进行拦截，而是要在发射前就加以破坏，这种先发制人的攻击方式本身就与《联合国宪章》中关于自卫权的规定相违背。霸权国有可能蓄意夸大现实威胁甚至捏造虚假信息，为自己发动预防性攻击遮掩粉饰，这一点在美国一意孤行的伊拉克战争中已经体现得淋漓尽致。对这类国家来说，发动网络攻击的道德约束

和成本压力显然小过常规战争，因而更有可能为霸权和侵略行径推波助澜。总之，美国构想的网络反导计划注定会开启一条危险的道路，其前景只会通向普遍的、愈发难以扭转的安全退化。

在这样的背景下，遏制网络空间军事化步伐应当成为国际社会的共识。但必须注意的是，减缓甚至扭转网络军事化进程并非易事，不仅需要综合施策，更需要科学辩证地看待网络能力建设与反对军事化之间的关系。事实上，力量制衡是阻止霸权国推进网络军事化的重要砝码。针对霸权国力量弱点的非对称制衡能够有效改变霸权国对于成本收益的战略认知，从而促使其转向协商治理和共同安全。因此，中俄等网络大国加强网络攻防能力建设，积极开展双边和多边安全合作，将是遏制美国网络军事化企图的重要战略举措。与此同时，国际社会亟需为网络空间安全互动建章立制。良好的行为规则是安全环境的稳定器。当前，国际社会对网络空间行为准则的基本价值和内涵尚未达成共识，中国应当进一步发挥积极引领作用，推进以非军事化为直接指向、以平等互信为基本理念、以共享安全为根本目标的网络安全国际行为准则。唯有此，才能将已然徐徐开启的潘多拉魔盒回归原位。



警惕大数据暗藏的“窃密通道”

大数据模糊了涉密与非涉密数据的界限，颠覆了数据垃圾无秘密的传统认识，打破了以客观存在为基础的定密习惯。因此，稍有疏忽便有可能引发泄密事件，保密工作者应高度警惕。

□ 傅 国 焦 艳

大数据暗藏“窃密通道”

从非涉密数据中发现涉密信息。大数据基本理论告诉人们：“如果将海量的碎片化数据汇集到一起，积少成多，形成大数据，然后通过数据分析，就可挖掘出隐藏在大数据表象背后的重要价值。”这一理论启示人们：如果将海量多元的非涉密数据通过大数据技术进行关联分析，在碎片化的信息之间建立某种整体联系，就可挖掘出隐藏在非涉密数据背后的重要价值。而这种“价值信息”因具有价值属性很可能涉及秘密范畴，从而使大数据具备了从非涉密数据中发现涉密信息的能力。比如，早些时候曝光的“棱镜”“X关键链”等美国网络监控计划已经充分表明，美国情报机构早已与“八大金刚”等网络巨头紧密合作，对全球通信系统和互联网进行大数据采集、挖掘和分析，从中搜集他国国家秘密和情报信息。因此，如果将非涉密数据置于一种失管失控的状态，就容易被不法分子轻易获取并从中发现有用情报。

使数据垃圾显现涉密价值。大数据基本理论告诉人们：“数据的价值并不仅限于特定的用途，它可以为了同

一目的而被多次使用，也可以用于其它目的；判断数据的价值需要考虑到未来它可能被使用的各种潜在方式，而非仅仅考虑其目前的用途。”比如，在英国学者舍恩伯格所著《大数据时代》一书中，有一则关于“莫里的导航图”案例，就是运用数据垃圾再利用的典型案列。该案例讲述的是年轻的航海家马修·方丹·莫里利用库房里存放的航海书籍、陈旧的地图和图表，以及多年前海军上尉写的大量航海日志制作全新航海图的故事。虽然莫里能够接触到的航海日志都是陈年旧货，内容上也无章可循，但莫里和他的助手硬是把看似垃圾的航海日志绘制成表格并重新利用，成功创建了一张全新的更安全、更有效的航海图，取得了空前成功。由此可见，大数据再利用技术能够使所谓的数据垃圾释放新的能量，重现新的价值，这种价值一旦具有涉密属性，就会使数据垃圾显现涉密价值。

提前感知涉密事项的趋势与未来。基于相关关系分析基础上的预测是大数据的核心。A增长的同时B也增长，A降低的同时B也降低，在拥有海量A数据的基础上，就可以利用大数据技术捕捉B的现在和预测B的未来。舍恩伯格在《大数据时代》中提到，麻省理工学院两位经济学家通过一个软件在互联网上每天收集50万种商品的价格信息，然后把大数据和好的分析法相结合，就能比官方数据提前一

步发现通货紧缩趋势。这种趋势涉及国家经济发展大局和未来走向，提前一步发现就是相当于掌握了核心机密。由此可见，大数据预测功能使人们有能力提前一步感知到涉密事项的发展趋势和未来状态，这一功能如果被不法分子利用，就可能演变为一种新型的窃密手段。

堵住大数据“窃密通道”刻不容缓

改变对待非涉密数据和数据垃圾的传统处理方式。大数据时代，非涉密数据、数据垃圾与涉密数据一样，具有特有的价值和可能的涉密属性。这就启示保密工作者不能再像以往一样把眼光局限在涉密数据上，而应在紧盯涉密数据的基础上，清醒地认识到非涉密数据以及数据垃圾存在的泄密风险。要充分认识到，包括数据坟墓、数据孤岛、数据垃圾、由涉密数据解密形成的非涉密数据、自然形成的非涉密数据在内的所有数据，都有其基本价值和潜在价值，都有可能是挖掘涉密信息、感知涉密事项趋势和未来的基础原料。保密工作者在处置非涉密数据和数据垃圾时，再也不能把非涉密数据绝对性地界定在涉密范畴之外，使其脱离了保密视线，也不能一味地把数据垃圾当作废弃物抛弃；相反，要采取有效措施，防范非涉密数据或数据垃圾成为失密泄密的新源头。

打破涉密数据以时长作为解密条件的传统标准。无论是《中华人民共和国保守国家秘密法》，还是《中国人民解放军保密条例》，对于秘密的管理都是以时长作为涉密信息定解密的一条主要标准。然而，在大数据背景下，涉密数据不仅具有基本价值，还

具有潜在价值，仅仅依靠时间来判断涉密数据是否仍有使用价值和保密需要是远远不够的，因为保密期限的届满并不能完全代表涉密数据已经没有任何使用价值。因此，要打破涉密数据以时长作为解密条件的传统标准，引入价值判断这一新标准，将两者有效结合起来。在传统时长标准的前提下，组织专业的大数据公司和数据科学家，依托科学合理的应用模型，审核即将到期解密的涉密数据，判断涉密数据的有用性和价值残留，在此基础上，再来确定涉密数据是否按期解密。

严格把控大数据的共享共用。2015年8月，国务院常务会议通过《关于促进大数据发展的行动纲要》，提出要推动政府信息系统和公共数据互联互通，深化大数据在各行各业创新应用。由此可见，在大数据时代，非涉密数据共享共用，充分挖掘数据价值将成为数据运用的新常态。但同时要看到，大数据模糊了涉密与非涉密数据的界限，并能运用预测功能从非涉密大数据中感知秘密的未来，这就要求将非涉密数据控制在一定的知悉范围内，防止过度扩散。这样做，又不可避免地会在一定程度上对数据运用产生反作用力。可见，恰当地平衡好两者的关系是必须解决的问题。保密工作者要认识到非涉密数据共享共用不是无原则滥用，共享是有条件的，共享共用的数据必须是非涉密或公开后带来的风险隐患是在可控范围内；而保密是无条件的，数据的共享共用必须确保其涉密内容的绝对安全。要做到既不会因为数据共享共用而降低保密要求，也不能片面追求绝对安全而阻碍了大数据应有作用的发挥。



气象对军事行动的影响，并未因军事技术的飞速发展和“全天候”武器的广泛运用而有所减弱，相反，随着武器装备的更新发展、战争行动联合化程度的不断提升，气象正以前所未有的深度和广度影响制约着现代战争的进程和结果。充分认清气象对高技术武器装备和军事行动的影响，更加积极主动地加以运用，对于夺取现代战争主动权具有重要意义。

气象对现代战争的影响

亘古以来，多少叱咤风云的将帅，因为不懂气象，陷入困境，毁于一旦，铸憾终生。又有多少借天公赐予良机，倚天作剑横扫千军的战例。古有黄帝乘雾胜蚩尤、曹操因火兵败赤壁、汉尼拔顺风胜罗马军、“无敌舰队”逆风葬火海；近有拿破仑因暴雨兵败滑铁卢、苏联凭酷暑扭转战局于斯大林格勒、日军逆天行事于中途岛惨败、盟军乘潮沙登陆诺曼底，等等。史实可鉴，气象同战争密不可分。

科索沃战争时，北约共出动飞机3.5万架次，受阴雨天气影响，仅有1万多架次的飞机进行了实际攻击。在许多情况下，因天气恶劣，北约飞机尚未到达目标区实施攻击任务便中途弹带返回。伊拉克战争中，一场强沙尘暴使美军飞机被迫降落或停止起飞，通讯网络装备被毁，2架直升机坠落。

在北约空袭南联盟的行动中，美军的精确制导武器因激光被云层、云雾等吸收或散射导致激光制导系统难以准确探测和锁定目标，武器效能发挥大打折扣。据美联社报道，美海军发射的“战斧”巡航导弹有五分之一的命中目标。而俄通社一塔斯社则称，美军空袭南联盟的巡航导弹的命中率仅为20%。相反，2015年10月，俄罗斯空军开始轰炸叙利亚IS组织前，预先对战场上空的气象条件，包括平均风速、云层分布、降雨周期、气温变化等进行了精密测算，选择最佳时机开展军事行动，从而使武器装备发挥了最大效能，取得了良好的轰炸效果。

此外，我们必须清醒的认识到的气象对战争乃至人类的负面影响。截至目前，人类对影响、改变天气的技术的研究还很有限。比如，人造酸雨、人造臭氧洞等，对环境的破坏力远远超出人类的控制范畴。从本质上讲，气象本身并没有价值判断的功能，这就决定了气象服务战争既可以被用于善的目的也可以成为恶的帮凶，只有武器与道德、法律和人文精神结合起来，才能真正体现气象服务战争的真正价值。

气象影响现代战争的途径

气象影响现代战争的途径，概括起来，一是通过气象武器影响战争，二是通过气象保障服务战争。

所谓气象武器，是指运用现代科技手段，人为改造战场环境，以实现军事目的的一系列武器的总称。这是一种既不是枪林弹雨，又不见刀光剑影，但却同样在特定的战场环境以致摧毁和打击敌方的特种“武器”。随着科学技术的的发展，人类已掌握了20多种人工影响天气的技术，其中可以引起气象武器作用的主要有人造干旱、人造洪暴、人造寒冷和酷热、人工引导雷电、人工影响电离层等。越南战争中，科学家就利用碘化银、碘化铅等化学物质作为“种子”，进行人工降雨，影响战争。1963年3月，“胡志明小道”上空每隔一段时间便有几架白色的美军飞机掠过，飞机离开半个小时后，该地区便会狂风大作、暴雨倾泻，道路变得泥泞不堪，给越南人民军行军和输送物资造成巨大困难。战后人们才得知，美军此举持续了长达7年之久。其作业方式主要是利用WC-130E气象侦察机和RF-4C侦察机，向作业地区的积雨云发射装有碘化银和碘化铅的烟弹，产生人工晶核，以达到催云降雨的目的。

气象保障是有别于气象武器而对现代战争产生影响的另一种途径。气象保障是指人类运用气象探测、气象预报和气象网络通信等手段预测气象服务战争的方式。近年

善用气象制胜现代战争

□ 吴洪林

来，美军利用先进技术，不断提升气象保障的信息化水平，逐步建立起与作战指挥体制相一致的气象保障体制。在气象探测方面，美军开发出气象影响辅助决策系统。这是一套将大气科学的基本原理及其物理模式应用于武器装备和描述战时军事行动的计算机系统。该系统能定量评估大气环境对武器装备和军事行动的影响程度，为指挥员和作战人员在指挥决策和作战行动中提供气象影响的定量化信息，并提出如何利用有利气象条件和避开不利气象条件的建议，为指挥员和作战人员作出正确决策提供保障。在气象预报方面，研究建立了综合化的多种尺度的气象预报平台，用于战时气象预报。美国空军已经装备了全球战区天气分析和预报系统，可有效提供战场目标区的天气预报。美国海军的全球大气业务预报系统，至今已发展到第四代模式，该系统能够实时为美军提供天气气候分析和预报产品。在气象通信网络方面，美军采用多网络、多信道和安全保密技术，以确保军事气象信息传输的准确性时效性安全性。

两点启示

高度重视，全面准备。气象服务战争，是现代战争发展趋势所需，我们要作好全面准备。首要的是，把气象的军事功能放到战略位置，从思想认识、组织架构、军民融合等加以体现。在观念形态上，不仅把陆、海、空、天等物理空间的有形气象考虑在内，也把电磁、网络等领域的无形“气象”考虑进去；在军事条例、战斗条令编制中，适当扩大气象测控队伍的规模，提高专业化水平；在军民融合中，建立军民兼容的气象水文和空间天气服务综合保障系统，特别是应对突发事件的军民联动保障协调机制，为国防安全和重大军事行动提供有力服务。

充分适应，主动谋划。即能主动而不是被动地、灵活而不是僵化地依据气象条件谋划和应对现代战争。牢固树立气象力就是战斗力的意识，无论研制部署运用武器装备还是组织开展军事行动，都把气象作为一个重要的制约因素来运筹考虑；不仅高度重视有形的气象信息，也密切关注无形的气象资料；着力提高武器装备、人员、技术、军事行动的抗“天候”能力，尽量把气象的影响降到最低；开展武器装备影响和重大军事行动适应性评估，提高军事气象研判应用和战场环境影响辅助决策水平和能力。

