战略纵横

信息化时代，网络安全的较量已上升为国家层面的对抗，需要军地一体合力集中统管——

打造军民融合的网络长城

■周鸿祎 张春雨

要点提示

●推动网络安全军民融合，需要在国家层面统一整合、优化配置，促进技术、人才、资源等要素双向流动转化。

●无论是网络安全分析、态势研判、应急处置，还是网络防护硬件、软件的研发，都需要大量的信息科技人才。

习主席深刻指出，没有网络安全就没有国家安全。数字化时代，网络空间已渗透到政治、经济、军事、文化等各个领域，具备军民一体的天然属性，是新时代军民融合发展的重要方面。当前，我国正向网络强国迈进，打造军民融合的网络长城，既是建设网络强国和信息化军队的基本制度设计，也是推动军民融合深度发展的重要驱动力量。新形势下，积极推动网络安全军民融合深度发展，亟须破解体制性障碍、结构性矛盾、政策性问题，不断提高融合水平、提升联合防护能力。

网络安全事关国家整体安全，需军地走开全面融合之路

信息化时代，网络空间安全已经成为国家战略新的制高点。去年全球爆发的“永恒之蓝”勒索病毒、乌克兰电网遭攻击、美国大选“邮件门”等事件表明，网络安全事关国家安全、社会稳定和战争胜败。网络安全的较量已上升为国家层面的对抗，超出军地各自管理控制的范畴，需要依靠军地一体合力集中统管才有可能管得住、管得好。

网络安全事关国家利益。由于网络触角延伸到经济、社会、文化等各个领域，其安全必将影响到经济安全、社会安全、文化安全、信息安全等。2017年5月，“永恒之蓝”勒索病毒席卷150多个国家和地区，包括政府、银行、通信公司、能源企业等重要部门机构基础设施陷入瘫痪，在全球引起轩然大波。早前，沙特的基础设施遭网络攻击，仅仅数分钟内，计算机硬盘就被破坏，所有数据被清空，攻击者还试图引发爆炸，如果得逞无疑会造成十分严重的后果。

网络安全事关战争胜负。信息化战争中，网络空间已成为新维战场空间。当前，美国、英国、日本等都已建立网络作战部队，并大力研发各种网络武器。伊拉克战争中，美军首先摧毁了伊军非常关键的5个指挥与雷达设施，并使用电子干扰等方式牢牢掌握信息优势，使伊军又盲又聋，防御体系迅速瘫痪。随着战争形态的加速演变，信息优势争夺日益成为战争胜负的核心内容，网络空间作为信息控制的“主战场”，日益成为战争博弈的制高点。

网络安全军民一体是世界普遍做法。当前，世界很多国家都将军民一体看作是提升网络空间安全的重要途径。例如，美国就将网络安全作为国家安全的重点，白宫和五角大楼指定波音、洛克希德·马丁等公司为网络安全国家队，指定微软、英特尔、思科、苹果、谷歌等信息技术巨头为网络安全的专业队，指定赛门铁克、迈克菲等网络安全防护企业为网络安全的特种队。在以色列，许多以军网络安全部队的军人退役后，成为地方高科技企业的精英，并创办多家网络安全公司。这些公司回过头来与以军在网络安全领域展开全方位合作，提升以军网络防护能力的同时，推动整个网络空间安全的发展。

网络安全资源分散多元，需军地强化顶层设计统筹

推动军民融合发展是一个系统工程，要善于运用系统科学、系统思维、系统方法研究解决问题。目前，我国各类信息网络系统高速发展，不同功能、类型的网络安全设施陆续配套投入使用，网络安全防护系统的总体框架基本建立。但网络安全资源广泛分布于军队和地方，推动网络安全军民融合，提高协同防护能力需要强化顶层设计统筹，打破体制壁垒和部门利益，在国家层面统一整合、优化配置，促进技术、人才、资源等要素双向流动转化。

构建完善网络安全组织领导体制。应加快建立军地一体具有中国特色的网络安全工作组织领导机构，确保层级清晰、分工协作。国家网络安全领导机构的工作重点是加强网络安全军民融合的顶层设计和宏观管控，制定发展战略和规划计划，履行军民融合中的统筹协调职能，负责国内网络安全的防御与应急反应，打击网络犯罪和网络恐怖主义等；军队网络安全主管机构侧重于拟制军队网络安全的整体规划和建设，将可以实施军民融合的领域纳入国家网络安全发展全局，做好与国家网络安全发展规划的相互衔接，明确军地协调的相关流程和管理办法，健全军地定期会商、重要情况通报、重大行动协同等工作制度，形成网络空间安全的联防、联管、联控。

统筹军地网络安全建设规划标准。以有效应对当前和未来一段时期网络攻防手段为目标，科学制定军民网络安全建设总体框架，分类确立建设模式，明确近期和长远建设目标，确定完成任务的配套措施。一是坚持统一标准。积极推动自主可控的安全操作系统、安全数据库系统等网络安全基础产品的技术标准统一，关键时刻能实现各系统的全面融合，打造坚固可靠的网络安全防线。二是坚持统一评估。加强网络安全建设评估和网络安全产品的技术风险评估，明确评估程序和环节，采取科学有效的评估方法，确保网络建成后防得牢、控得住。

建立网络安全军地资源共享机制。实现军地网络安全资源共享，关键是建立军地需求共提机制。应及时发布军民两用技术成果信息，实时对表“战场需缺”与“市场所有”，实现军地双方需求、技术、标准、产品等信息资源充分共享；加快构建军地信息融合共享平台，拓展联通渠道，规范互通标准，实现军地信息资源充分互补共用；建立网络安全准入制度，明确划定保密等级范围，军队业务主管部门与“民参军”企业定期会商、信息通报、需求对接和协作攻研，防止民用网络安全力量技术研发丢了目标、少了靶子，防护战术失去对手、缺乏指向；建立网络威胁信息互通机制，及时互通国内外网络安全最新动态和重大事件通报，鼓励民营企业与政府、军队实时共享网络安全威胁信息，提高研究分析的专业性和实时响应能力。

网络安全实质是人才的较量，需军地树牢联合思想

网络安全的本质是网络对抗，实质是人才的竞争较量。无论是网络安全分析、规划、态势研判、响应和处置，还是网络防护硬件、软件的研发，都需要大量的信息科技人才。为满足军地网络安全人才巨大需求，需要牢固树立联合思想。

联合培养人才。近年来，国家网络安全人才培养取得重要进展，网络空间安全被国务院学位委员会和教育部增设为一级学科，每年网络空间安全领域毕业生近万名。但与打造网络强国和强军兴军需求相比还存在较大差距，存在人才队伍缺口较大、培养体系有待完善、实践型人才储备不足等问题。应积极探索军队、地方高校、科研院所和网络安全企业开展人才联合培养渠道，共建师资队伍、共搭实验场所、共设实习基地，实现课堂教学、实习实践的有机结合，通过网络安全训练营、安全运维人才培养等，提升网络安全从业人员的专业能力，完善快速化、规模化、实战化的安全运维、分析响应、攻防渗透等网络安全人才联合培养机制。

联合运用力量。应统筹军地各种力量的运用，加强行动协同，建立较为完善的网络安全联防联控机制。一方面，充分发挥地方网络安全人才的作用，开放军队网络安全顶层设计、核心技术研发、网络安全整体建设等领域，以满足军队网络安全对人才的需求；另一方面，充分发挥军队网络安全需求的助推器作用，利用军方先进的网络技术，测试核能、通信、交通、金融等国家关键基础设施网络的安全性，检验应急响应体系的有效性。

联合研发技术。军民协同创新是实现网络防护技术创新突破的重要途径。应围绕发挥军事需求对前沿创新的牵引带动作用，聚力突破关键网络技术，促进基础平台军民共享，大力推动军民技术相互转化；鼓励高校、科研院所、军工企业和优势民营企业强强联合，集中军地人力、物力和财力，对关键芯片、核心器件、操作系统等领域集智攻关；探索军民融合网络安全装备技术创新模式，研发新一代防火墙、入侵检测、信息加密、信息隐藏、反窃听等防护技术，共同培育自主化网络安全产业生态链。

此外，由于网络安全具有综合性复杂性，还需军地合力来强化法规政策保障。制定网络安全军民融合的法规体系、支撑网络安全军民融合的相关政策，以及网络安全军民融合重点保障领域的相关文件，确保网络安全军民融合的措施落地生根，形成军地联合支撑体系。

高端走笔

在常态落实上下功夫

■范承才

习主席强调指出，虽然我军在不同时期担负的具体任务不同，但作为战斗队的根本职能始终没有改变。在各种风险挑战充满广域性、多元性和不确定性的今天，军队必须强化“战斗随时打响”的紧迫意识。练兵备战要摒弃“临阵磨枪、不快也光”的思维，彻底改变“一阵风、运动式”的模式，全面消除年年“一年级”、次次“炒冷饭”的现象，真正统筹好常态化与体系化、实战化、精细化的关系，在不断思战研战练战中，探索特点规律，加快人装结合，提升胜战能力。

常态探索完善体制机制。驾驭部队建设这艘航船，首先应学懂弄通体制编制这一龙骨。新编制为战而设、为训而立，对强化领导指挥、深化备战打仗起着重要的支撑作用。应加紧搞清变革变化，真正悟懂架构机理，尽快融入角色，在常态学研新编制、掌握新编制、运用新编制中，开创备战打仗的新格局。

常态研究作战问题。研战知战方能胜战。无论是指挥员还是战斗员，无论是领导机关还是基层部队，都应该把研究作战、思战谋战作为一种常态，把钻在作战室、身处演训场作为一种常态，紧盯作战任务、作战对手、作战环境，大兴作战问题研究之风，把现代战争制胜机理搞清楚，把将来要打的仗弄明白，不断推动作战研究成果进入方案计划、进入演训实践、进入战法训法。

常态落实按纲施训。言武备者，练为最要。真打实备必须落实到实战化训练上。要坚决克服“调门喊得高、实际不作为”的空谈主义，通过学研军事理论、学研武器装备、学研战法训法，练硬指挥本领、练精基本技能、练强基础体能，真正把“岗位必需、战位必备、能力必要”的素质练过硬。树立“常态化”抓训指导，保持“常态化”施训状态，不仅严格落实训练总时间，更要调控部队像组织作战一样训练，制定计划详细具体，组织实施严格严密，跟进保障到底到位，效益调控经常经济，促进部队训练全面靠拢实战。

常态完善能力指标。完善的作战能力指标体系，不仅能够常态引领发展，更能始终明晰方位。在部队重组重塑刚刚到位之际，无论是传统力量，还是新质力量，都需要尽快构建基于不同任务、不同环境和不同行动，覆盖各层级、各领域和各类型部队，延伸至单兵、单装、单平台的作战能力指标体系，形成明确、具体、量化的建设指向，彻底打通作战能力向战备建设和备战训练转化递进的桥梁路径，常态牵引战斗力标准落地落实。

常态强化监督监察。坚持战斗力标准，既需要官兵自省自觉，也需要外部用策用力。保持备战练兵的常态化，必须建立党委监督、纪委监督、业务机关监督和官兵群众监督的闭合回路，通过上下合力，反复纠治那些游离中心、背离主业，与战斗力建设争地位抢资源等问题，严肃查处那些作战准备不经常、实战练兵不惯常的人和事，将全面从严治党、依法从严治军向战斗力建设各领域延伸，保证一切工作向备战打仗常态聚焦。

常态保持高度戒备。中华民族伟大复兴绝不是轻轻松松、敲锣打鼓就能实现的。军人必须丢掉幻想，时刻准备斗争。任何部队都需要基于出门就能作战、开拔就能打仗，能够从野外训练场直接走向战场，加速补齐战备建设短板，全面落实全装满员训练，时刻保持高度戒备状态，即使部队在外，该带的物资必须带上，该备的弹药必须备齐，该建的要素必须建立，该联的系统必须联通，确保任何时候任何情况下，都能拉得出、上得去、打得赢。

（作者单位：中部战区陆军）

切莫忽视偶然现象

■张西成

群策集

●变革大潮起于青萍之末的时候，其端倪常常是以偶然现象示人。

提起珍珠港事件，很多人认为它是美国海军核心军事能力转变升级的诱因和起点，让美军决策者看清了打赢未来海战的方向和关键。那么，这个转型是如何发生与发展的呢？

1941年，珍珠港遭到日本偷袭，美太平洋舰队损失了7艘战列舰，在战事吃紧的情况下，他们只能转而倚重侥幸生存下来的航空母舰。当时，美国海军舰炮的有效射程最远不过40多千米，俯冲式轰炸机的作战半径却能达到战列舰的10倍，一下子使攻击距离得到惊人提高。珍珠港事件发生数月后的中途岛之战，美军的数艘航母战胜了规模远胜于己的日本联合舰队，并最终改变了太平洋战争的总体进程。

战争实践表明，没有空中掩护，水面舰艇在作战中几乎没有获胜的希望。美军决定立即减少战列舰的生产，加快航母的建造速度。战争结束时，美国已经建造了近百艘航母，而新建的战列舰仅有8艘。如果美国海军没在珍珠港事件中损失多数战列舰，这些战舰的牢固地位很可能会继续保持，航空母舰的“转正”恐怕也就不会那么快。

很多学者在研究美军时，认为其军事变革无不是“走一步、看两步、想三步”，始终长于计划、富于前瞻性，事实上并非如此。就像二战中美海军核心军事能力的转型，并不是有预谋地为之，而是偶然得之；并不是预先看到了海战变革的方向，某种程度上还是一种“无奈之举”。这也提醒我们，推进以信息技术为核心的军事变革，既不能把希望全然寄托在侥幸的偶然因素上，但也不能忽视偶然性在历史进程中所发挥的积极作用。

据美国一家咨询公司对世界500强企业信息化项目连续6年的调查数据显示，只有26%的项目完全成功，28%的项目完全失败，其余46%则超过了预算或工期。之所以如此，盖因世界充满了种种意外和不确定性，计划永远赶不上变化，没有谁的预言能够言出必中。历史经验表明，很多突破性的科研成果，靠的就是“有心栽花花不发，无心插柳柳成荫”的意外；许多事业的成功，一开始并非来自周密的计划，却常常来自实验和摸索，甚至还有那么一点点运气。

变革大潮起于青萍之末的时候，其端倪常常是以偶然现象示人。然而，偶然并非都能成为必然。没有敏锐的嗅觉，即使偶然的机遇撞到鼻尖上也抓不住。只有时刻关注事态的最新发展，认清偶然事件可能昭示的发展趋势，并勇敢积极地实践，才能成为时代变革的捷足先登者。

当然，就如硬币有正反两面一样，偶然现象也有利与害之别。对于后发者来说，既要重视偶然，善于挖掘偶然背后的必然规律；同时也不要迷信于偶然，防止被某一孤立的偶然现象牵入死胡同。如此，方能觅得转型先机，走好变革之路。

观点争鸣

洞悉信息化作战新变化

■高东广

●随着信息化作战的发展，快速处理数据、深度挖掘信息、获得信息优势的能力变得越来越关键。

近年来，随着信息技术的深入发展，大数据、云计算、物联网等新兴技术获得广泛运用。从军事领域来看，一方面，信息化作战的不断发展，越来越需要借助新兴技术，推动信息化作战能力获得升级；另一方面，这些新兴技术的运用，会进一步改变信息化作战的面貌。对信息化作战的新变化，我们应密切关注，及时了解掌握其特点。

信息优势的重要性更加凸显。大数据时代，夺取信息优势变得更为重要。美国学者布鲁斯认为，美军在过去20年中取得的所有军事胜利都有一个共同点，即达成了对敌人的信息优势。对于占有信息优势的一方，山那边、海对面的“战场迷雾”被驱散，指挥员能及时了解整个战场情况，实施高效指挥和快速打击。信息化作战，机动和信息两个要素变得异常关键，反映在信息维度，就是战场信息急剧攀升。据专家分析，美军一次小型战术作战行动，陆基、空基、天基等全方位侦察情报系统，全天候运转一天会产生近60TB的数据。一次分队级行动，就需要庞大的数据支撑，可见，随着信息化作战的发展，快速处理数据、深度挖掘信息、获得信息优势的能力变得越来越关键。

新兴信息技术影响日渐加深。战争总是打着时代的烙印。20世纪的两次世界大战，动辄数十万、上百万兵力交战，战场从欧洲到亚洲、从大西洋到太平洋，规模十分庞大。进入信息化时代，网络化部队分散配置和态势感知共享，使得兵家们历来想达成的“精兵破敌”“以快制胜”目标更易实现。据统计，美军完成一个“发现—定位—瞄准—攻击—评估”打击链所需时间，海湾战争为100分钟，到伊拉克战争缩短至30分钟以内，到了空袭利比亚时，已经近乎发现即摧毁。在这样的背景下，大数据等技术对信息化作战的影响越来越深。一方面，战争需要精心设计、精准筹划、精确指挥，这些都离不开大数据。数据承载着信息，信息越多，越需要从海量、繁杂的信息中，提炼出优质、高能的信息，并据此进行科学决策。另一方面，大数据与云计算、人工智能等深度融合，能够挖掘出隐藏在海量数据背后的作战规律，从而使作战运筹科学化、高效化，有效地回避了经验化、盲动化。

“制脑权”争夺变得尤为激烈。在人工智能、物联网等技术的影响下，信息化作战日益呈现出智能化特点，“制脑权”成为未来战场全新的制权争夺点。“制脑权”是指在人脑的智力空间激烈较量，会对其他空间制权产生倍增效应。“制脑权”的核心是对认知优势的争夺。认知过程包括感知、理解、推理三个阶段。“制脑权”争夺，首先在感知阶段展开，从传统隐蔽伪装、电磁静默到网络对抗，都是军事感知对抗的组成部分，目的是让对手只能感知虚假信息，确保己方准确、快速地感知对手和战场。在认知的理解和推理阶段，“制脑权”争夺则主要是在智能化手段辅助下通过战术与谋略运用，让己方科学高效制定决策计划，使对手难以准确判断、理解我方行动意图。甚或可以通过对脑机能干扰来影响人员思想意识、心理情绪等，扰乱、破坏对手的认知。在争夺“制脑权”的过程中，应着力追求“脑机有效融合”。把高层决策、总体规划等谋略性强的工作交由人脑来处理，需要大量、精确、高速的数据信息记忆、计算、管理任务交给机器，充分发挥脑机两者优长、弥补短板。