军事战略

加快推进网络立法进程

□ 邬贺铨

信息技术是双刃剑。信息技术的应用越深入，社会经济和人们生活对信息技术的依赖越多，信息技术产品的可靠性和可信性带来的安全问题影响就越严重。黑客利用软件设计的漏洞植入病毒和木马，盗取有用信息或谋取经济利益。目前针对智能手机有3000多种病毒和5万多种恶意应用软件，而移动智能终端因功耗限制无法像PC那样内置功能完善的防病毒软件。云计算和大数据中心会成为集中攻击的对象。我国在自主可控的大数据分析技术与产品方面与发达国家相比有不少差距。如过分依赖国外的大数据平台，难以回避信息泄密的风险。《中国互联网发展报告（2014）》报道，我国面临大量境外地址攻击威胁，国家互联网应急中心监测发现在2013年计境内1090万余台主机被境外服务器控制，其中美国占30.2%。我国境内6.1万个网站被境外控制，较2012年增长62.1%。2013年针对我国银行等境内网站的钓鱼页面数量和涉及的IP地址数量分别较2012年增长35.4%和64.6%。信息技术被用来作为国家间政治、经济与军事竞争的手段，斯诺登事件就是一例。受美国标准委员会NIST批准，美国家安全局（NSA）和加密公司RSA达成了价值超过1千万美元的协议，在移动终端所用的加密协议中放置后门，使NSA通过随机数生成算法Bsafe的后门程序破解各种加密数据。一些国家刻意准备网络战，目的是破坏对方的信息系统并进而摧毁能源、交通等基础设施，著名的案例是2010年9月伊朗的铀燃料浓缩设施被“震网”病毒攻击而瘫痪。



从国家战略高度认识网络安全。2011年以来，美、英、法、德、俄、澳、加、韩等国纷纷制定国家Cyberspace战略或Cyber Security战略。Cyberspace（赛博空间）包含网络基础设施、数据内容和控制域，即覆盖传输层、认知层和决策层，其范围还将从目前的互联网拓展到各类网络、各类数据链和所能链接及管控的各类设备。Cyber Security（赛博安全）的含义不仅是传统的网络基础设施安全，还包括信息层面即数据或内容的安全以及对被控制或被影响对象的执行决策层面的安全，即与信息化有关的非传统安全的综合。

美国发布的《Cyber空间国际战略》声称如其网络受到侵犯将视为对它领土的攻击，美国将保留使用一切必要手段打击网络威胁的权力，包括外交、信息技术、军事和经济。我国也需要制定有关网络安全的国家战略，从核心技术研发和管理协调等全方位提升网络安全防御能力。

习近平总书记在2014年2月中央网络安全与信息化领导小组成立大会上强调：“网络安全和信息化对一个国家很多领域都是牵一发而动全身的，要认清我们面临的形势和任务，充分认识做好工作的重要性和紧迫性，因势而谋，应势而动，顺势而为。”“没有网络安全就没有国家安全，没有信息化就没有现代化。”

加强网络治理，保障信息安全。互联网作为一种信息传播工具，是宣传社会主义文化的阵地，也是不法分子或居心叵测的人散布谣言煽动事端或欺诈的角落，要严厉打击网络犯罪，同时还要加强引导和治理，净化网络空间，维护网络秩序，保护网民和企业的利益。习近平指出：“做好网上舆论工作是一项长期任务，要创新改进网上宣传，运用网络传播规律，弘扬主旋律，激发正能量，大力培育和践行社会主义核心价值观，把握好网上舆论引导的时、度、效，使网络空间清朗起来。”

重视网络和信息安全产业的发展。习近平总书记指出：“信息掌握的多寡成为国家软实力和竞争力的重要标志。信息技术和产业发展程度决定着信息化发展水平，要加强核心技术自主创新和基础设施建设，提升信息采集、处理、传播、利用、安全能力，更好惠及民生。”我们不可能等待安全再推广信息化，没有永恒的安全，总是魔高一尺道高一丈，安全问题需要依靠发展来解决，我们要加大对网络与信息安全技术的研发和产业发展的支持力度。网络与信息安全产业占软件和信息服务业的比重在欧美国家达到8%~12%，我国目前仅1.5%。我国信息安全产业整体相对弱小，关键产品和服务依赖进口，高端信息安全人才缺乏。对信息安全产业也需要提升到国家战略高度来认识，加大扶持力度，力争实现《信息安全产业“十二五”发展规划》的目标，即到2015年产业规模突破670亿元。

我国网络立法存在的问题。互联网是现实社会的映射，适用传统的法律体系与法律关系，但它的出现也在部分环节和部分领域改变了传统法律关系要素的内容。互联网犯罪成本低而惩治成本高，出现了很多基于互联网的新的犯罪行为，Cyber空间扩大了国家安全的维度，互联网的虚拟性使主体的真实性识别发生困难，互联网上虚拟货币等新的财产形态难以认定，互联网多点接入的跨界性对行政属地管理原则形成挑战。尽管在过去十多年中，我国已经相继出台各类与网络相关法律、法规、规章200多部，但与发达国家和一些发展中国家相比，我国在信息化方面的立法仍明显滞后，不适应互联网发展的需要。我国网络立法的效力层次较低，部门规定多难免带有部门利益的色彩，着力管制多，关注发展少，对个人权利保护考虑不足，甚至上位法规定的权利被下位法剥夺的情况在中国互联网的管理中时有出现，本意要净化网络空间，结果却抑制了创新、阻碍了互联网产业与应用的发展。

尽快补足我国网络立法的短板。美国国会及政府各部门通过与网络相关的法律法规数量高居世界之首，主要涉及未成年人保护、国家安全、保护知识产权、计算机与网络安全等四大领域，在“9·11”事件之后，美国加强了信息安全的立法，先后推出了联邦通讯法、联邦监听法、对外情报监视法、执法通信辅助法、爱国者法、国土安全法、互联网情报分享与保护法和信息安全与互联网自由法等，既明确网络安全的要求，又为信息监管给出法律保障。我国的基础设施基本上都有一部行业基本法，如邮政法、铁路法、公路法、民航法、电力法等，但缺电信法和广电法，当前尤为需要网络与信息安全法和个人信息保护法。需要为信息安全和隐私保护立法。大数据挖掘需要有法可依，要明确数据的所有权，提倡数据共享又要防止数据被滥用，要区别个人数据与隐私，前者强调归属于本人的可识别性，后者强调与公共事务无关的私密性，要在保护隐私的前提下鼓励对用户数据的挖掘。信息安全的监管也需要有法律来界定，明确规定信息监管的适用对象，把监管纳入法治轨道，既要打击网络犯罪，又要保障公民的言论自由。要塑造一个良性有机的立法环境，在立法层面需要考虑如何让社会各类主体参与到网络社会的管理和建设。

军队建设

维护国家安全离不开实力支撑

□ 肖天亮

有效维护国家安全，必须坚持以总体国家安全观为指导，围绕实现党在新形势下的强军目标，加强国防和军队现代化建设，不断提高我军应对多种安全威胁、完成多样化军事任务的能力。

构建中国特色现代军事力量体系。我国传统的军事力量体系是一个陆战型、国土防御型的体系。新形势下维护国家安全，必须着眼新的国家安全需求，构建中国特色现代军事力量体系。从力量更新看，要构建新型作战力量与传统作战力量有机融合的力量体系；从能力结构看，要构建陆、海、空、天、网、电一体的力量体系；从安全重心看，要构建立足本土、倚陆向海、辐射利益攸关区的力量体系；从作战效能看，要构建精干、联合、多能、高效的力量体系；从中国特色看，要构建具有防御性、地区性、人民性的不对称力量体系。从总体国家安全观的要求看，在加强军队自身能力建设的同时，还要重视军事力量对其他领域安全的支撑保障能力。

加强新型安全领域力量建设。根据总体国家安全观的要求，要特别重视加强海洋、太空、网络等新型安全领域能力建设。海洋关系国家长治久安和可持续发展，必须建设与国家安全和发展利益相适应的现代海上军事力量体系，维护国家主权和海洋权益，维护战略通道和海外利益安全，参与海洋国际合作，为建设海洋强国提供战略支撑。太空是国际战略竞争制高点，应密切跟踪掌握太空态势，加强太空力量建设，应对太空安全威胁与挑战，保卫太空资产安全，服务国家经济建设和社会发展，维护太空安全。网络空间是经济社会发展新支柱和国家安全新领域，应加快网络空间力量建设，提高网络空间态势感知、网络防御、支援国家网络空间斗争和参与国际合作的能力，遏控网络空间重大危机，保障国家网络与信息安全，维护国家安全和社会稳定。

积极推进军民融合深度发展。习近平主席指出，把军民融合发展上升为国家战略。这是我们长期探索经济建设和国防建设协调发展规律的重大成果，是从国家安全和发展战略全局出发作出的重大决策。总体国家安全观也强调，要统筹安全和发展问题。因此，以军民融合为途径加强国防和军队建设，是总体国家安全观的内在要求。新形势下加强国防和军队建设，要注重将国防和军队建设规划融入国家经济社会发展总体规划，将军队信息化建设融入国家信息化建设体系，将国防科技和武器装备发展融入国家科技创新体系，将战场建设融入国家基础设施建设体系，将军事人才基础教育培养融入国民教育体系，将军队生活服务保障融入社会服务保障体系，将国防动员体系融入国家应急动员体系。通过军民融合的深度发展，加快国防和军队现代化建设步伐。

新概念新法则

网络空间作战走向前台

□ 姜连举　王永华

当下，正值网络潮起云涌的时代，一个与战争绕不开、躲不过的热点焦点话题——网络空间作战，正走入人们的生活，走向战争的前台。随着“网战”“网络司令部”“网军”等一个个军字号的作战实体露面，网络军备竞赛已战鼓声声，由暗到明，传统战场被罩在一张张看不见、摸不着的网络之中。虚拟的网络，真实的战争。一个国家若把不住“网络安全”的大门，一个小小芯片都可能成为敌人的“轰炸机”，国家安全和发展就无护航之盾；如不注重网络强军，“能打仗、打胜仗”就不可能落实到位。

“网战”左右战争胜负

网络在政治和经济领域具有超强的扩张性和渗透性，在军事领域的延伸更是张力凸显，网络空间正迅捷成为“网战”的大舞台。网络自诞生就紧连战争，现代网络的鼻祖“阿帕网”，实质上是军用实验网络。从网络到“网战”，演绎的是战争活剧，牵引的是国家安全战略脉动。美军首任“赛博空间司令部”的司令基思·亚历山大上将，曾一针见血地指出：网络是继海洋和太空之后的“新军事前线”。的确如是，网络已经成为国家军事机器的“中枢”，“网战”正逐渐撑起战争胜负的“大旗”。

网络向战场的不断延伸，使“网战”成为战争发展的必然，网络空间作战在战争中的作用也越发显现。“网战”能够左右战争胜负，是因为信息化战场上，各种作战要素都通过网络“相知、相融”，凝结成高度一体化作战体系，作战行动呈现空前的体系性，这使“破网瘫体”成为信息化战场上一种新的制胜定律。正如美国军事预测家杰姆斯·亚当斯在《下一场世界战争》一书中预言：在未来战争中，计算机本身就是武器，前线无处不在，夺取作战空间控制权的不是炮弹和子弹，而是网络里流动的比特和字节。

从机理上讲，网络空间作战的根本目的是破坏战场网络的核心属性，降低网络对敌联合作战行动的支持作用。作为联合作战重要手段，网络空间作战主要围绕联合作战目的，对敌指挥控制网、预警探测网、情报侦察网、通信网、业务保障网等节点进行入侵、破坏，使其无法稳定运行、发挥应有功能，破坏敌作战要素的信息共享和功能互补，瘫毁敌作战体系。战场网络通常与互联网物理隔绝，高度机动性却决定其具有无线传输特点，这就为网络空间侦察、入侵和破坏开启了一扇窗。分布式配置的网络侦察设备可以自由截获目标网络信息，分析研究其网络协议及密码，一旦成功，就能以无线方式入侵目标网络，尽情实施网络窃密或病毒攻击。即使无法掌握其协议和密码，也可利用强烈的干扰信号压制其无线信道，扰乱网络稳定运行。还可以通过特种行动在网络设备中预埋病毒，战时根据需要触发病毒，造成系统瘫痪。高功率微波武器、电磁脉冲武器也是网络设施的终极杀手，传统精确打击、兵力袭击也能在关键时节达成网络实体瘫痪目的。

有人说信息化作战“无网不胜”，但有网未必就能取胜。因为，从制胜的因素上讲，网络只是作战之“器”，决定作战胜负因素的则是运用武器之人和创新的作战之“术”。网络时代的战争，更注重人与武器的结合，强调人与网络空间的融合。“器”、人、“术”三位一体，构成网络空间作战的有效“组合拳”，“无网不胜”才会成为可能，“网战”左右战争胜负才有立论基础。网络空间作战平战界限模糊，要打赢“网战”，必须深入研究平战特点，准确把握作战规律，不管是平时还是战时，都要注重发挥网络的作战效能。在“器”的发展上，打造具有自身特色的网络制胜利器，为战争胜利创造条件；在人才队伍建设上，注重培养人掌握信息技术和网络思维能力，依靠人才精英方阵，决胜“没有硝烟”的网络战场；在“术”的创新上，确保网络空间作战指导的科学性，全面推进战法创新，以“术”制胜。

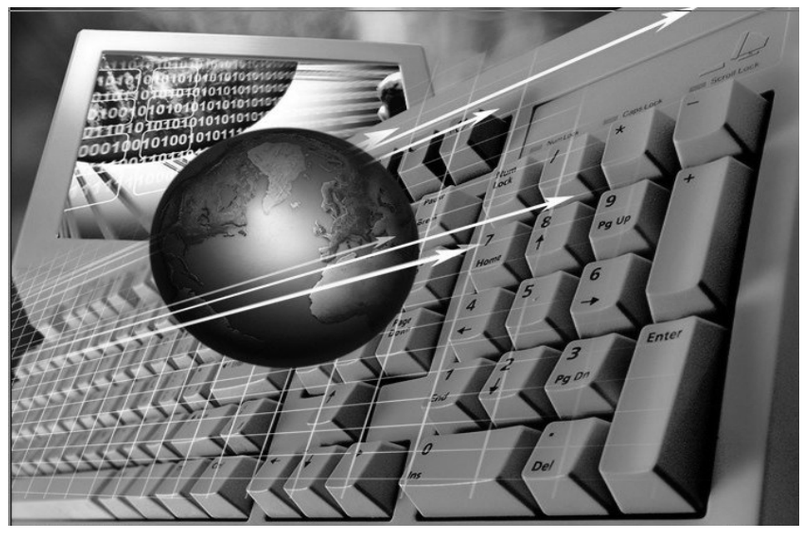
“网军”整装跑步入列

“网战”的号角召唤网络时代新的军旅尖兵，“网军”不仅应运而生，而且已经整装上阵，快速加入兵种行列。“网军”的入列，是人类战争史上又一次质的飞跃，今日看似稚嫩的“列兵”，演绎的将是全新的战争神话。

杜黑曾说过，胜利总是向那些能预见战争特性变化的人微笑，而不是向那些等待变化后才去适应的人微笑。面对战争硝烟日益弥漫的网络空间，怎样做好预见性的准备？什么样的准备具有胜算？“网军”建设给出了答案。美国是网络大国更是网络强国，美军对此做出的准备是，2009年率先成立赛博空间司令部，“网军”随之诞生，彰显了谋求网络空间主动权的决心和意志，为打赢“网战”做足了功课。其后，韩国、英国分别公开宣布建立网络空间作战司令部和网络安全业务中心，日本也高调成立网络防卫队。世界主要国家都在积极筹建网络攻防部队，全力抢夺网络空间的战略优势，这就是打赢网络空间作战的胜算准备。虽然和平利用网络是人类的共同愿望，但当战争依然是解决国际争端和利益纠纷的重要手段，当军事领域被网络“捆绑”的越来越紧，被信息“淹没”的越来越深的当口儿，当一只U盘便可“攻陷”五角大楼不再是“传说”，“网军”建设就成为各国竞相发展的焦点，是实现军事创新和作战胜利的战略选择。

“网军”作为战略和战场两级网络空间作战力量，既肩负着维护国家网络安全和主权的时代使命，也承担着决胜战场、打赢战争的重任。平时，“网军”需要为国家和平看家护院，时刻应对各种潜在的网络威胁和恶意攻击，适时显示自己的“肌肉”和能力，通过威慑遏阻各种敌意行动；战时，“网军”则根据作战需求，灵活实施各种网络攻防行动，渗透到各种作战样式之中，为夺取战场网络空间的控制权，遏制敌方网络空间的自由行动，夺取战场主动权创造有利条件，成为出奇制胜的战场“奇兵”。

“网军”能够走进信息化军队大家庭，成为军队作战的重要力量，是信息时代军事发展大势使然。如今，“网军”建设已不是讳莫如深的话题，而是军队力量建设的时代命题。如何使“网军”这支新生力量迅速成长壮大，更是世界各国军队都需要认真研究的重大课题。“网军”强，则国防强。面对“网军”急速而来的现实，既不能无动于衷，坐以论道，错失良机，也不能人云亦云，随之起舞，盲目发展。正确的选择是，认清历史方位，明确目标，理清思路，稳妥应对，以宽广的视野和创新的思维，走自己的“网军”发展之路。尽快形成能够遏制网络空间对抗危机、控制网络空间对抗战局、赢得网络空间对抗胜利的实战能力。



“网权”攀升至国家主权

网络空间虽然是虚拟世界，但在虚拟之中却有国家主权的“身影”。国家主权存在于网络空间，就如同一个国家的陆地、海洋、空中和太空主权一样真实，并非虚拟幻存。“网权”的出现，也产生了新的国家主权观，为维护网络空间的权益，一些网络大国已经把“网权”视为国家安全重心，纳入到军事战略的高度，将对网络空间的恶意入侵和严重攻击定性为战争行为。俄罗斯已将网络攻击视为大规模杀伤性武器攻击，美军也有专业人士指出，对网络攻击应与大规模杀伤性武器同等看待。维护“网权”，已成为“网战”的重要内容。

相对于维护领土、领海和领空等实体主权，维护网络这个虚拟空间的主权更为困难。因为，入侵和攻击网络，其隐蔽性、突然性和技术性强，网络空间主权更容易丧失，造成的危害更大，防范的难度也更大。一架飞机、一艘舰船对一国实体领域的入侵，很容易被发现、监控，造成的破坏与伤害也是直观可见的；网络空间则无形无疆，拥有网络技术优势的一方，可以悄然无声、多渠道、多形式地破坏目标国关系国计民生领域的核心网络，甚至中止对方网络使用权。主导网络技术优势的国家，可以建立自己的一片新的“网络领土”，拓展自己的疆界，别人进入这片“领土”，必须向其“申请护照”，遵循其主导的网络“游戏规则”。伊拉克战争期间，伊拉克顶级域名（IQ）的申请和注册工作被终止，相关后缀的网站全部从网络中消失。还有，从伊朗大选到俄格冲突，再到近期中东和北非的突尼斯、埃及、利比亚政局突变、动荡，围绕“网权”的殊死对抗从幕后走向前台。通过网络可轻而易举进入他国腹地直至“心脏”部位，践踏别国的主权，“网权”已经成为维护国家统一、稳定和完整的新权益。

时代催生了“网权”，就需正视和捍卫“网权”，全面更新主权观，增强“网权”意识，将网络空间摆到与陆地、海上、空中和太空同等的战略地位。大力发展自主知识产权的核心元器件和软件系统，从源头上消除潜在的主权入侵。制定网络空间突发事件有效的监测、预警和封堵的行动方案，形成高效、可行的网络空间安全应急处理预案。在军事上做好网络空间作战准备，确保“网战”出手即能打赢。