美军网络战司令部成立评析

□ 魏　都

随着全球化的不断深化，非传统安全逐渐成为人们关注的焦点。冷战后，各国将更多的注意力转移到非传统安全上来，如经济安全、金融安全、生态环境安全、信息安全、资源安全、恐怖主义、武器扩散、疾病蔓延、跨国犯罪和海盗等。进入21世纪以来，美国一方面维护传统安全的霸权，同时也在探索如何取得非传统安全的霸权。这对美国是一个新问题。这次美军组建网络战司令部再一次表明，美国已经拉开争夺非传统安全主动权的序幕。

美军成立网络战司令部

2009年6月23日，美国国防部正式宣布创建网络战司令部，成为第一个组建此类司令部的国家。这表明，美国在对付网络安全或者说非传统安全威胁方面又先人一步。美国防部长盖茨在签署的备忘录中写道："我们对网络越来越多的依赖以及面临的一系列网络威胁给国家安全增加了新的风险"，网络战司令部的建立将帮助美国国防部"确保在网络空间的行动自由"。这也意味着美国正式将传统的战争空间由真实的陆海空天延伸到虚拟的网络空间，意味着网络战将作为一种国家层面的战争形式走入人类历史。新建的网络战司令部也可以被认为是美国继非洲司令部之后第二个重点对付非传统安全威胁的专门司令部。

美军认为，网络战是为干扰、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。作为全球最早把网络用于实战的国家，美国打造网络战部队的历史，远远早于互联网在全球的普及。早在1988年11月2日，美国康奈尔大学计算机系的研究生莫里斯，对美国防部战略C^4I系统的计算机主控中心和各级指挥中心实施病毒攻击，共约8500台计算机染毒，其中6000台无法正常工作。这让美军初步感受到了网络攻击的威力。而美军首次将网络战用于实战的战争是1991年的海湾战争。海湾战争中，美国通过情报系统，在伊拉克的防空系统中植入电脑病毒，在美军空袭前用遥控手段激活这些病毒，导致美空军飞临巴格达上空时，伊拉克防空系统已经瘫痪。

因此，美军组建网络战总部并不是其重视网络战的开始，更不是简单地只求拥有这一结果，而是在其多年信息战理论和实践的基础上，经过慎重考虑的结果。其目的只有一个，那就是在有形战争中保持绝对优势的前提下，在无形战场上也占据有利先机，以达到控制虚拟世界的目的。当然，从其一贯实用主义的立场考虑，组建网络战司令部的好处则远远比其称霸世界的目的要丰富得多。

美军宣布网络战总部的成立，也相当于同时宣布网络战已经成为信息时代战争的重要样式，甚至首选样式。它可以兵不血刃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，从而达到不战而屈人之兵。

毋庸置疑，随着计算机网络在军事领域应用的普及，网络已经成为提升军队作战能力的"倍增器"。美军网络战司令部的正式组建，为把军事霸权从陆地、海洋、天空和太空延伸到网络空间夯实了基础，使以往只是存在于传说和电子游戏中的网络战，变为步步逼近的现实。

美军网络战力量构成

什么是网络战？简单来说，就是利用各种信息手段掌握对手一切信息、阻止对手获取己方信息的军事行为。网络战的实施主体为网络战部队。

美国在加强计算机网络安全技术和发展网络攻击手段和工具的同时，也加强了网络攻击人才的训练和培养。继1995年美军第一代"网络战士"从美国国防大学信息资源管理学院毕业后，又有一定数量的网络战人才相继完成学业，其中还包括一部分信息战指挥军官。此外，美空军军事学院也开始系统培训空军信息战专业军官。

美军还组建了世界上第一支具有实战意义的网络信息战部队，即第609网络信息战中队。它由计算机专家、电子学工程师、航天技术专家、通信工程技术人员、通信保密技术人员及其他专业人员组成，主要任务是保护美国中央总部空军的关键性计算机网络的安全，主要采用软件技术手段实施网络防御，并完全具备向敌方的

计算机网络系统发动进攻性信息战的能力。为应对敌对力量的挑战，美军还将陆续组建类似于609的信息战部队。

根据对美军网络战项目跟踪多年的防务专家乔尔·哈丁评估，美军涉及网络战的军人已经增至5到7万人，其中网络战专家3000至5000人，加上原有的电子战人员1.5万人，总数已接近9万人，这意味着美军网络战部队人数已经相当于7个101空降师。但美军并不满足此，网络战部队还在不断扩充。美军战略司令部司令奇尔顿对媒体透露：美军计划增加一支“网络特种部队”，还要招募2000至4000人。这支部队不但要承担网络防御的任务，还将对别国的网络和电子系统进行秘密攻击，获取美国所需要的各种情报信息。目前，美军网络作战指挥权分属战略司令部下辖的两个网络战中心。一个是指挥网络防御的“全球网络联合特攻队”，主要负责保护美国本土和全球范围内的网络系统，应对试图攻入美军网络的攻击。另一个是负责网络进攻的“网络战联合功能构成司令部”，主要职责是对敌人发动网络攻击，以在战时快速侵入敌方网络系统，瘫痪敌方的指挥网络和依靠电脑运行的武器系统。随着网络司令部的组建，这两个构成美军网络战攻防指挥体系的盾与矛的部门，将尽快合二为一。正如奇尔顿在接受采访时所说：“在不远的将来，这两个部门将合并为一个更有效的机构。”

美军遂行网络战的主要手段

网络战部队的主要任务是渗入敌方网络系统窃取绝密数据，在对方网络内植入程序，以便在战时摧毁敌方指挥控制系统。网络战的主要手段：硬摧毁与软攻击相结合，在网络空间展开进攻对抗。通过电子系统攻击、电磁系统阻断与攻击、网络攻击和基础设施攻击作战，以阻止、降低、破坏、摧毁或欺骗敌人。攻击目标包括敌人领土、空中和太空网络、电子攻击和网络攻击系统以及敌人自身。

硬杀伤网络战武器方面，美军已经发展出电磁脉冲弹、次声波武器系统、动能拦截弹和高功率微波武器，能够对别国网络的物理载体进行攻击。特别值得注意的是一种机载系统，通过空降侵入并操纵敌方网络传感器，使敌方丧失预警功能。

在软杀伤网络战武器方面，目前，美军已经研制出两千种以上的计算机病毒武器，如“逻辑炸弹”、“陷阱门”、“蠕虫”程序、“特洛伊木马”程序等。从媒体报道来看，早期的进攻战术有“后门程序”、“炸弹攻击”等，近年来又研究了“僵尸网络”、“广泛撒网”等。既可以在对方毫无察觉的情况下，利用网络战手段窃取有价值情报，又可以利用特殊工具软件，在短时间内向目标集中发送大量垃圾信息，使对方出现超负荷、网络堵塞等状况，从而造成系统崩溃。美军感到这些软硬件装备和各种战法分散在各军种，没有发挥出整体优势，今后要依托新组建的网络战司令部，进一步完善装备，并加快战法研究整合步伐。

网络战漫谈

□ 守　磊

互联网技术的突飞猛进给社会生活带来便利，同时，信息革命也带来了深刻的社会变革，由于其与政治、经济、文化、军事等领域的联系越来越紧密，也使之成为可用以达成战略目的的利器。事实上，制网权，也成为继制海权、制空权、制天权之后国际竞争的又一重要领域。

网络战的实质

网络的威力与核武器相比，既存在相同之处，又有明显区别。同核武器一样，网络战产生的破坏力巨大。网络战一旦全面展开，受到攻击并被击败的一方有可能遭受国民经济全面崩溃的危险，而获胜一方将彻底破坏敌人发动和维持战争的战略资源。如同核武器通常可以产生巨大的心理震撼效果，网络战也可以崩溃敌人的战斗精神和意志。核武器一旦使用，战争后果具有不可控性，网络战也是如此，像病毒之类的作战武器在释放之后，将无法被控制，可能带来“双刃剑”效果。就二者的区别而言，网络战与核武器最大的不同在于网络战的胜利不是以大量的生命伤亡为代价，战争的附带毁伤小于后者。

美国早已把网络战地位提高到战略层面。美军方重要智库——兰德公司指出，工业时代的战略战是核战争，信息时代的战略战主要是网络战。美政府内人士透露说，美总统奥巴马本人对网络安全问题十分重视，早在竞选时就曾承诺将把网络安全的重要性视为等同于大规模杀伤性武器的国家安全问题。

网络战争，虽然形式上是虚拟世界的竞争与对抗，实质上更多的是思想文化的较量。占据互联网优势，就是占据传媒优势，占据文化优势。控制互联网就是控制思想，控制观念，控制文化，进而控制世界。美国哥伦比亚大学国际事