网络战与美国网络司令部

□ 本刊编辑　张敏钰（摘编）

一、网络战的定义

网络战是信息化条件下以计算机及其网络为基本工具、以网络攻击与防护为基本手段的一种全新的作战样式。网络战正在成为高技术战争的一种日益重要的作战样式，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、控制敌方的商务、政务等民用网络系统，不战而屈人之兵。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。

不同的国家和地区，在军事领域推行网络战的空间各有不同：一些国家和地区的作战系统部分运行于互联网络，部分通过专用网络，还有一部分为战场空间即时组网；另外一些国家和地区在军事领域则完全不接入互联网络，只通过专有网络和战场空间即时组网实现基于网络的作战。各国家和地区在政治、经济、文化等领域的应用系统基本上连接在互联网络上，少数运行在专用网络中。网络世界的战争，既针对互联网络，也针对各种专用网络和战场空间即时组建的作战网络。就是说通过现代高科技手段在网络战场这样一个虚拟空间进行的一些作战行动，这个基本上都叫网络战。网络世界的战争，主要在以下四个层面展开：一是信息基础设施，也就是计算机和通信设施的联网，包括有线、无线通信设施、通信卫星、计算机等硬件设备；二是基础软件系统，包括操作系统、网络协议、域名解析等；三是应用软件系统，包括金融、电力、交通、行政、军事等方面的软件系统；四是信息本身，针对在网络中流动的所有信息。

严格来说，对信息基础设施的打击应归为广义上的网络战，它针对的是网络运行的基础。各国家和地区在定义网络战概念时并没有将信息基础设施完全纳入网络战的范畴，但是，现代战争一旦打响，对信息基础设施的打击却是第一位的。

今天网络战最常见的是围绕秘密资料的窃与防。虽然主要国家和军队都会把机密信息储存在与互联网断开的电脑系统里，但庞大的系统难免有疏忽的人或硬件通过复杂的间接渠道错误接入民用网络。攻击者就是要找到这些漏洞，破解密码，把机密信息偷出来。有时这种收获会比派“007”式的间谍到敌人总部里偷到的情报还有价值。

其次是网络舆论战。这种战法考验的不是网络技术，而是心理战水平。攻击者会运用新闻传播规律和对敌方社会心理的了解，编造谎言、制造恐慌和不团结等。与早期阵地喊话式的舆论战比起来，有了互联网的帮助，这种作战的效果被放大数倍。在民心士气上的破坏力不容忽视。

第三种网络战是充满血与火的，这是军方网络战的核心。目前美军陆、海、空、天、电磁系统是一个大的网络，而美军作战力量又遍布世界各地。各种情报侦察、战场感知、指挥控制信息结成信息网；各种导弹、火炮、枪弹的火力结成火力网；各种参战力量、补给物资、弹药、设备等通过陆、海、空渠道形成后勤运送网。三种网络支撑着美军作战，美军最核心的网络战也在这三个网上，依靠这三个网的力量，先由实体作战部队实施突破、占领，或在较近距离实施电磁侵入和对抗，然后再实现进一步的瘫痪敌方系统、获取情报、施放假指令等网络战。所以，第三种

网络战将是网络战中最惨烈的一环。

网络战是在看不见的战场上进行的“软”较量，它充分利用计算机网络的开放性、便捷性和即时性等特点实施网络攻防，具有平时和战时一体化的特点，不仅战时是配合陆、海、空、天、电各个领域作战的重要作战手段，在平时也可独立实施并可随时发动网络攻击。

二、网络战真实案例

早在1979年，年仅15岁的美国少年“黑客”米尼克运用他破译密码的特殊才能，成功地打入美国军方的“北美防空指挥中心电脑系统”，在美国军方毫无察觉的情况下，其指向前苏联的所有核弹头数据资料均一览无遗，然后又悄无声息地复制传给其少年朋友，这给美军开了一个天大的玩笑。

在1991年的海湾战争中，美军对伊拉克实施了网络战。开战前，美国中央情报局派特工到伊拉克，将其从法国购买的防空系统使用的打印机芯片换上了含有计算机病毒的芯片。在战略空袭前，又用遥控手段激活了病毒，致使伊防空指挥中心主计算机系统程序错乱，防空C3I系统失灵。

在1999年的科索沃战争中，网络战的规模和效果更是有增无减。南联盟使用多种计算机病毒和组织“黑客”实施网络攻击，使北约军队的一些网站被垃圾信息阻塞，一些计算机网络系统曾一度瘫痪。北约一方面强化网络防护措施，另一方面实施网络反击战，将大量病毒和欺骗性信息送到南军计算机网络和通信系统。从高技术战争向信息化战争过渡的过程中，网络战的规模和强度将越来越大，作用日趋上升。

2003年年初，美国“黑客”们在因特网上筹划“倒萨”行动计划，并对伊拉克进行大规模的心理攻势。

俄罗斯的黑客举世闻名，在2008年8月的俄、格冲突中，俄罗斯可以说创造了一个网络战的经典案例。在军事行动前，俄罗斯控制了格鲁吉亚的网络系统，使格鲁吉亚的交通、通讯、媒体和金融互联网服务瘫痪，从而为自己顺利展开军事行动打开了通道。尽管俄罗斯的网络战实力不俗，但由于网络核心技术掌握在美国人手中，俄罗斯的网络战并没有经受真正的考验。这也是为何俄罗斯积极主张制定网络战国际条约的一个原因。

2009年1月，法国海军内部计算机系统的一台电脑受病毒入侵，迅速扩散到整个网络，一度不能启动，海军全部战斗机也因无法“下载飞行指令”而停飞两天。仅仅是法国海军内部计算机系统的时钟停摆，法国的国家安全就出现了一个偌大的“黑洞”。设想，如果是一个国家某一系统或领域的计算机网络系统出现问题或瘫痪，这种损失和危害将是不可想象的。

三、美国成立网络司令部及当今各国网络军备概览

在美军正式成立网络司令部之前，美军已建立了若干负责网络作战的机构和部队，如“全球网络作战联合特遣部队”（JTF—GNO）、“网络战联合职能组成部队司令部”（JFCC—NW）。美军网络司令部是在整合这些机构的基础上成立的，现已将总部设在马里兰州的乔治·米德基地，由国防部国防信息系统局提供技术支持和信息保障。网络司令部隶属美国战略司令部，基斯·亚历山大为司令官，编制近千人。网络司令部将整合全军网络资源，统一管理，强化对策，以应对军事网络系统所面临的不断增长的威胁。按照计划，网络司令部在2010年10月全面运作。美国组建网络司令部对美军具有里程碑意义，这表明美军能在新的网络领域推行全面攻防作战，标志着美军网络战实现了统一指挥，使网络战成为一种独立的作战样式。

美军网络司令部的职能是计划、协调、组织和实施各类网络空间作战行动，包括指导国防部信息网络的防御行动，准备和实施军事网络空间的全谱作战行动，确保美军及其盟国在网络空间的行动自由，剥夺敌人在网络空间的行动自由等。网络司令部一位高级官员认为，较之以往的网络作战机构，“网络司令部任务并没有更新，只是在原有基础上进行了扩充

和重组”。

目前，美军庞大的国防系统有700万台电脑，运营着1.5万个计算机网络，重要网络包括海军网、空军网、陆军网、后勤网、仿真互联网、巡航导弹网、医疗网等170多个，此外，美国国防部还有95%的数据通信使用公用电话系统。因此，美军十分重视网络的进攻与防御。

2005年3月，美国国防部公布的《国防战略报告》，明确将网络空间与陆、海、空和太空定义为同等重要的、需要美国维持决定性优势的五大空间。2009年5月美国政府公布的《网络安全评估报告》也认为，来自网络空间的威胁已经成为美国面临的最严重的经济和军事威胁之一。为此，自去年以来，美国加快网络战的准备，大幅度增加网络攻击武器的投入。

美军网络司令部拥有千余名信息战专家，包括工程师、物理学家、分析家、数学家、语言学家、计算机专家和数据流专家等。它由诸军种联合司令部、下属各军种网络司令部和作战部队共同组成，其中包括陆军的第9司令部和第1信息战司令部（地面）、海军的网络防御作战司令部和信息战司令部、空军的第67网络战联队和第688信息战联队、海军陆战队的网络空间司令部等。

美军网络司令部还制定了保护网络空间的“交战规则”，即网络战部队的作战条令，并准备与其他国家进行网络空间军备控制谈判，推广美军的网络战理念，形成网络作战共识。

美军网络司令部的成立在美国国内引起了不小的争议。一是有民众担心会侵犯个人隐私。信息时代，网络与人们的生活密切相关，从购物、存款到付账、纳税，样样都离不开互联网。美国的政治生活、经济运作、商业活动和文化娱乐，也都依赖庞大而复杂的网络系统。由于网络司令部汇集各种信息情报专家，可以通过先进的技术手段掌握丰富的网络资源和信息，如果再假以国家安全的名义，那么民众的个人隐私就有可能受到侵犯。

二是国土安全部担心军队的网络司令部会抢占它的地盘。美军网络司令部主要负责国防部的网络系统，美国国内民用网络安全工作由国土安全部负责。国土安全部的一项重要职能，就是收集并评估威胁美国民用网络的各种情报，并及时发布公告，采取适当的预防和防护措施。军方网络司令部成立后，与国土安全部难免要争夺网络空间的领导权和控制权。

三是对网络司令部司令基斯·亚历山大的争议。亚历山大此前曾任国防部国家安全局局长。这个局控制着整个美国的间谍卫星网和设在世界各地的监听站，其职能是负责收集外国通讯信号，监听范围包括电台广播、电话通讯、互联网，甚至是军事和外交的秘密通讯，为美国联邦调查局、美国中央情报局等政府机构提供可靠情报。选择亚历山大出任网络司令部司令，也加剧了人们对美军网络司令部日后行为的担忧。

美国成立网络司令部的绝对优势：

计算机芯片、操作系统、网络协议、路由、域名解析等，是绝大多数国家和地区的绝大多数网络运行的基础，它们大都打上了“美国制造”的标签。因为最了解系统中存在的漏洞，甚至是“制造”出来的漏洞，美国利用漏洞实施攻击或控制的能力世界第一。控制了全球13台域名根服务器中的10台，美国有条件“封杀”一个国家的网络。虽然美国不断强调网络上存在的风险，不断渲染各种针对美国计算机网络的攻击事件，但是，通过多年发展和网络攻防的实战及演练，不论是网络运行的稳定性、可靠性和安全性，还是锻炼出来的人才队伍水平，培养出来的网络安全意识水平等，美国都超过其他国家。

虽然各国家和地区在互联网络上拥有各自的应用软件系统，安全性各不相同，但是，再高的应用软件系统安全性，面对上述两个层面的攻击，也是无能为力的。也就是说，如果对方只是要达到摧毁或瘫痪的目的，在应用软件系统安全性上投再多的钱也还是温室花朵，无根浮萍。

如果信息基础设施还存在，也没有被引爆芯片、操作系统中可能存在的“致命炸弹”，只是在互联网络中演练入侵系统，“黑掉”网站、窃取数据等技术，那么，俄罗斯尚有和美国一搏之力。在专用网络和即

时组网方面，俄技术专家正在研制各种计算机病毒武器，特别是“远距离无线注入病毒武器”，可对敌方指挥控制系统产生直接威胁。

各国网络军备概况：

英国 早在2001年就秘密组建了一支隶属军情六处、由数百名计算机精英组成的“黑客”部队。2009年6月25日出台首个国家网络安全战略，并宣布成立两个网络安全新部门，即网络安全办公室和网络安全行动中心，分别负责协调政府各部门网络安全和协调政府与民间机构主要电脑系统安全保护工作。

俄罗斯 20世纪90年代就设立了信息安全委员会，专门负责网络信息安全，2002年推出《俄联邦信息安全学说》，将网络信息战比作未来的“第六代战争”。俄罗斯已经拥有了众多的网络精英，反病毒技术更是走在了世界的前列，在遇到威胁或有需要时，这些人才和技术将能很快地转入军事用途。

印度 基于对网络技术的精通和利用网络能够达到何种战争效果的认识，坚持自主研发、军民合作的原则，投入大量人力物力，力求在网络技术、密码技术、芯片技术以及操作系统方面自成体系。“闪光信使”高速宽带网络以及被称为“第三只眼”的海军保密数据信息传输网络的建成使用，将进一步增强印度军方应对未来网络战争的不对称优势。除完善防御体系外，印军一方面将网络进攻写入作战条例，明确指出要建立能够瘫痪敌方指挥与控制系统以及武器系统的网络体系，在陆军总部、各军区以及重要军事部门分别设立网络安全机构；另一方面通过吸纳民间高手人伍和对军校学员进行“黑客”技术培训等方式，逐步完成未来网络战的人才储备。

日本 其重要作战指导思想是通过掌握“制网权”达到瘫痪敌人作战系统的目的。日本在构建网络作战系统中强调“攻守兼备”，拨付大笔经费投入网络硬件及“网战部队”建设，分别建立了“防卫信息通信平台”和“计算机系统通用平台”，实现了自卫队各机关、部队网络系统的相互交流和资源共享；成立由5000人组成的“网络空间防卫队”，研制开发的网络作战“进攻武器”和网络防御系统，目前已经具备了较强的网络进攻作战实力。同时，日本注重与美国联合发展，在引进先进技术的基础上不断完善自身建设，不断提升“网战”能力。

韩国 在1999年提出了未来信息建设的总体设想，2009年宣布将组建“网络司令部”，并于2010年正式启动。目前，韩国已经拥有了约20万接受过专业训练的庞大的人才队伍，而且每年国防经费的5%被用来研发和改进实施网络战的核心技术。

以色列 在1998年就将成功入侵美国国防部的青年招入部队，并开始加大对网络作战的研究力度。在巴以冲突、黎以冲突中，以色列利用网络进攻的方式篡改网页、攻击电视台，以达到影响舆论导向的目的；侵入军方电脑窃取机密，以确定火力打击的重点目标和精确坐标；阻断敌人通信指挥系统，以掌握最佳的作战时机，这一切都是以军进行网络战真实写照。

2008年5月14日，北约7个成员国爱沙尼亚、拉脱维亚、立陶宛、德国、意大利、西班牙和斯洛伐克签署协议，将共同出资建立一个反网络攻击研究中心，以提高防御网络攻击的能力。由此可见，“网络军事化”已经渐渐走向战争舞台的最前沿。BMS

参考文献：

[1]《美军网络司令部引发争议》作者：陈翌春、赵小卓，中国人民解放军军事科学院研究生部、世界军事研究部研究员，出处：《人民日报》2010年6月17日.

[2]《网络战，威胁超越虚拟现实》作者：祁永强、王宁夏，国防大学军事后勤与军事科技装备教研部教员，出处：《人民日报》2010年6月17日.

[3]《多角度解读网络战》作者：陈小虎，国防大学军事后勤与军事科技装备教研部教员，出处：《人民日报》2010年6月17日.

[4]《各国网络军备概览》作者：袁轩、赵德喜，中国人民解放军军事科学院战略部研究员，出处：《人民日报》2010年6月17日.

[5]《世界网络战部队的发展现状》作者：吴清丽、王君学，石家庄陆军指挥学院，来源：《红旗文稿》2010年第21期.

[6]《网络战争》作者：张召忠，解放军文艺出版社，2001年1月.