编者按：美国对伊拉克战争已呈剑拔弩张、一触即发之势，战争阴云笼罩着巴格达。布什政府何时下达战争令、战争何时爆发我们无法得知，然而作为现代战争的一种重要的作战样式——网络战，却早已是不宣而战。本期刊载两篇介绍网络战的文章，希望对读者了解在这场可能爆发的战争中将会出现的一种全新的网上战争有所帮助。

美国开始制定网络战战略

2月7日《华盛顿邮报》，赫然刊出一条消息，据称美国总统布什已于去年签署一项密令——“国家安全第16号总统令”，要求美国国防部牵头，组织中央情报局、联邦调查局、国家安全局等政府部门制定一项计算机网络战战略，以便在必要时，在确保美国军民网络信息系统安全的情况下，攻击和破坏敌方的网络信息系统。

网络战关乎国家安危，是类似于核战的战略战

美国兰德公司认为，战略战是一种破坏性极大的“顶级”作战形式，它实施的成败关系到国家的安危与存亡；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。

有鉴于此，美国的军事战略就像核武器诞生后出现了“核化”趋势一样，现在又出现了“信息网络化”趋势。目前，美国军事领导人和军事理论家已经把一些军事战略术语中的“核”换成了“信息”，如“信息优势”、“信息威胁”、“信息垄断”、“信息攻击”、“信息防护”、“信息威慑”、“信息保护伞”、“信息保障”等，网络战已成为极其重要的战略战。

美军已经具备了很强的网络进攻能力

美军非常重视网络战进攻能力建设，已经具备很强的网络进攻能力。其举措有三：

一是大力开发计算机网络战武器。在软杀伤网络战武器方面，美军已经研制出2000多种计算机病毒武器，如“蠕虫”程序、“特洛伊木马”程序、“逻辑炸弹”、“陷阱门”等。在硬杀伤网络战武器方面，美国正在发展或已开发出电磁脉冲弹、次声波武器、激光反卫星武器、动能拦截弹和高功率微波武器，可对别国网络的物理载体进行攻击。

二是创建“黑客部队”。据悉，美军通过在国内外招募计算机高手，已经建立起一支“黑客部队”。这支部队训练有素，接到命令后随时可发起信息网络攻击，侵入别国网络，进行破坏、瘫痪甚至控制。

三是组建信息网络战进攻部队。美国空军正在建立一支专门负责实施信息网络进攻的航空队——第8航空队。该航空队由9个不同类型的空军联队组成：第67信息战联队和第7情报联队于2001年划归第8航空队，第55联队、第9侦察联队、第93和552空中控制联队、第41和42电子战联队于2002年10月归建，第11侦察联队将于2003年10月纳入第8航空队建制。

美国军方一直在研究网络战战略

对于网络战这样一种重要性日益凸现的作战样式，美国军方十分重视，已将网络战纳入各种重要作战条令。例如，在参联会1998年10月颁发的《联合信息行动条令》中，就用一定篇幅论述了如何实施信息战中的计算机网络攻击。又如，美国陆军部于2001年6月发布的新版《作战纲要》中，又重点规范了陆军部队如何实施“信息行动”中的计算机网络防护。

近年来，美国军事理论界和研究军事问题的民间思想库，乃至工业和商业界，也把网络战作为重点研究课题。2002年7月，美国加特纳技术研究所和海军军事学院联合召开了“计算机网络战研讨会”，79%的与会者认为两年之内很可能发生恐怖分子袭击美国重要军用或民用网络信息系统的事件。今年1月，50多名美国科学界、工业界和政府部门的专家在麻省理工学院召开会议，深入探讨了平时和战时战略网络战涉及的各种问题。

尽管美国各界都很重视计算机网络战研究和网络战能力建设，但是美国联邦政府还没有制定出全国统一的、跨部门的、军民通用的网络战战略规划。特别是在美军已经具有强大的网络进攻能力的情况下，这种能力的使用由于影响巨大而涉及到很多战略、法律、道德问题，必须全面考虑、周密筹划，明确网络战战略指导就成为当务之急。布什总统就是在这种形势下下令制定网络战战略的。

美国政府准备拟定攻防兼备的总体网络战战略

全新的网络战已经拉开帷幕

军事科学院　栾大龙

据《华盛顿邮报》2月7日报道，美国总统布什去年7月就签署一道密令，下令制定一个网络战略，以便在必要的情况下对敌人的电脑系统发动袭击。

有迹象表明，在可能爆发的对伊拉克战争中，美国有意对巴格达发动一场全新的网上战争。

透析网络战

网络战，是一场在有限的作战空间内、以进攻性行为夺取和达成信息优势，从而影响、破坏敌方的信息站、信息系统和计算机网络的一种作战方式。网络战以武器控制、C4I等系统中的核心设备——计算机为主攻点，力图瘫痪对方、同时保护己方的“心脏”安全。科索沃战争，使神秘的网络战从虚拟走向现实。

在未来网络战中，每个芯片都可能是一种潜在的战争武器，每台入网的计算机都将可能成为一个作战单元。任何一个拥有一台计算机和入网线路的人，只要熟悉网络配置情况，掌握一定的计算机理论和操作技能，就能够上网运作、发布与传递信息；就能够攻击装有芯片的系统，就能够介入网络作战，成为一名“网络战士”，在网络战场“冲浪”。

在未来网络战中，由于信息技术的广泛运用，各种战场传感系统、侦察系统能够全方位、大范围、全天候地探测、监视、侦察瞬息万变的战场情况；特别是无人驾驶飞行器、无胶片摄像机等，能够精确地对敌战场态势乃至战斗过程中的行动进行探测、识别、跟踪攻击，进一步提高了战场信息的“透明度”。

在未来网络战中，由于战场网络是一个由通信情报网络、计算机、战场数据库以及各种用户终端等组成的综合网络，它不仅可以真实及时地传输图像，而且还可以真实及时地传输话音、文字、数字等信息，这样整个战场信息的循环，就构成了实时的、有效的“回路”，作战空间广阔且时间无限。

未来网络战，将不受局部的陆、海、空交战空间的任何束缚。对于美国来说，由于拥有先进的电子技术优势，它可以在平时预先有准备地将计算机病毒芯片插入可能卖给的控制国，或者将这种病毒芯片预设在敌国的武器系统中，或者把病毒编制到软件中。一旦需要，既可以在平时直接激活这些潜藏的病毒实施攻击，也可以在战时予以点击，从而使战前、战中、战后的时间观念淡化。平时也就是战时，网络作战时间跨度将无始无终，不受限制。

未来网络战攻击手段多样，可以是黑客攻击，也可以采用计算机入侵，还可以利用其他方式。未来网络战无论在作战力量、战场信息，还是在作战时空、攻击手段、打击精度上，都将显现出与以往战争迥然不同的特征。海湾战争中，以美国为首的多国部队充分发挥网络优势，利用激光制导炸弹实施精确攻击；特别是美军的“斯拉姆”导弹，能准确地从前一枚导弹打通的墙洞中穿过，进而攻击预定目标。

美、俄、印和台湾地区的网络战准备情况

美军《2010年联合作战构想》和《2020年联合作战构想》均将信息优势看成是联合作战的主要因素。因此，美军十分重视计算机网络的攻防研究与建设，以求夺取未来信息作战的主动权。

网络战分为两种基本类型，即网络进攻战和网络防御战。

布什总统下令制定网络战战略的另一个重要原因是，为美国政府拟定总体网络防御战略，使政府各有关部门协调行动，保护民用和军用信息网络系统。

众所周知，美国是世界各国中社会信息化程度最高的国家。美国社会已经是一个高度一体化的网络社会，社会的各个单元都是这个大网络的节点，国家运转、社会生产、商品交换、人民生活都高度依赖计算机网络。信息网络系统是一把双刃剑，它可以给作战、工作、生产、生活带来巨大效益，但一旦受损又会导致灾难性后果。而信息网络系统又不可避免地具有脆弱性，“就是上多少道锁也难以保证它的绝对安全”。所以，美国总统网络安全顾问克拉克惊呼：“美国是一个最容易受到网络信息攻击的国家！”事实也是如此，在美国政府组织的、由兰德公司和国防信息系统局分别实施的对民用和军用信息网络系统的攻击实验中，有近70%的攻击获得了成功。（摘编自《解放军报》王保存“美国开始制定网络战战略”一文）