第一篇　网络与网络信息战

以因特网为代表的各种信息网络的出现，是20世纪最伟大的科技成就。正是无所不在的信息网络，把人类紧紧地联系在一起，极大地改变着人类的生产和生活，使人类真正走向更加灿烂辉煌的信息时代。当我们尽情地享受着网络带来的无数便利和利益的同时，我们还会惊奇地发现，网络也正在改变着战争，网络不仅加速人类战争从机械化向信息化转化的进程，网络空间本身也正在变成人类战争的一个崭新作战空间。用键盘操纵的战争——网络信息战，已经成为人类战争的一个重要样式，由高知识、高智能的人员组成的网络战部队已经出现。

第一章　互联网——信息作战的新空间

公元 2000 年 2 月 4 日,中东地区大国 ×,试图迫使沙特阿拉伯减少其石油产量以提高原油价格。为达到保护盟友和石油供应的双重目的，华盛顿准备派部队去中东为沙特阿拉伯助威。× 国自知与美国进行直接武力对抗难以占到便宜，就选择了一种更隐蔽的方式——发动网络信息战，与美国实施对抗。于是，白宫接到一系列报告：北加利福尼亚和俄勒冈州的电话系统已中断了；就在总统国家安全委员会刚刚结束会议不久，一列时速 320 公里的客车在马里兰州撞上了一列被误导的货车。中央情报局认为可能是 × 国给他们的通信系统和铁路计算机系统注入了“逻辑”炸弹，并引发了这场灾难。与此同时，在沙特东北城市达兰附近，一家原油提炼厂遭受到通过计算机信息系统而发动的“攻击”，引起了爆炸和大火。在伦敦和纽约，三种不同的病毒同时向证券交易系统发动攻击。在一系列打击之下，纽约和伦敦的股票市场交易迅速下跌。

按照计划，美国开始派部队去中东。但是，通过计算机网络实施的‘电子进攻’,严重阻塞了派遣基地的军用电话系统,美国部队的调遣不能如期进行 由于软件中的‘蠕虫’病毒毁坏了数据,五角大楼用于部队调遣和装备、食品与油料配给的计划表变得杂乱无章；在佐治亚州，两家银行的自动柜员机突然狂躁起来，肆意在顾客的账目上增减数目；美国有线电视网的电视信号中断了 12 分钟,美国公众开始恐慌,纷纷提取大笔存款。

2 月 18 日，沙特两家政府电视台的新闻播音员的面孔，被电子技术替换成了伊斯兰复兴民主运动领导人的面孔，他号召发动

军事政变反对沙特皇室。在五角大楼，情报军官通报国防部长，一些不知名的计算机“黑客”已向美国发动了一场毫不留情的信息战：世界各地的大部分美军基地的计算机系统受到攻击而变得反应迟缓或失去联系，甚至已被破坏。更糟糕的是，美国空军引以自豪、用来跟踪敌方坦克和部队的“联合监视与目标攻击雷达系统”战场指挥机，也开始在屏幕上出现斑点和被电子感染的迹象。

2 月 19 日,华盛顿的所有电话系统,包括移动电话,全部停止了工作。总统试图召开国家安全委员会的紧急会议，但通信不畅使他们困难重重。最终，委员们来到白宫，在这里指导五角大楼坚持与伊朗打一场缓慢而不流血的战争……

展现在我们面前的这幅可怕的景象，不是好莱坞科幻电影场面，而是美国国防部委托兰德公司于 1995 年 1 月举行的一场‘信息战”演习。其目的不外乎为了迎接来自一种新的作战空间——网络信息空间的挑战。

在人类战争史上，随着技术的进步和战争工具的发展，作战空间也不断地拓展和变化，逐步地从地面延伸到水上，由平面拓展到立体，由有形变为无形。作战空间的每一次新的拓展和变化，都带来战争方式和方法的演进和发展。随着互联网的出现和迅速发展，计算机网络成为信息化社会人类生存和发展的又一崭新空间。而随着这一新的空间的出现，人类战争又被拓展至一个新的领域——计算机网络空间。

一、神奇的互联网

20 世纪最伟大的科学成就之一，就是网络的诞生。它使世界为之一变，使人类的生产和生活方式发生了根本的变化。

(一)“蜘蛛网”引发的灵感

历史不会忘记 1946 年 2 月 14 日，也就是第二次世界大战开始后的第二年，世界上第一台计算机埃尼阿克应急切的军事需求而问世。当时它仅仅是作为计算弹道的一个辅助工具，就像是厨房里的灰姑娘，又笨又粗。体积达 320 立方米,重量达 30 多吨,足有二层楼高。也许在当时，它的出现并不那么引人注目，可正是它真正开辟了计算机技术的新纪元，宣告了一个全新时代——信息时代的到来。

在埃尼阿克之后,第二代、第三代、第四代计算机相继问世,体积越来越小，功能越来越强。计算机不仅在军事领域发挥重要作用，而且广泛应用于社会的工业、农业、科研、医疗卫生等各个领域，渗透到人类生活的每一个方面。

然而,当计算机数量日趋增多,并通过线路、服务器、路由器等连接起来，且具有一定拓扑结构的时候，一个全新的东西——计算机网络就开始形成了。

20 世纪 60 年代末期，美国军方已研究出同时分享系统技术，军内的电脑系统可以实现多位用户同时分享一个电脑处理器所提供的信息资源。据此，美国国防部一些高层人士提出建立一个网络系统，这种网络系统类似蜘蛛网(WEB) ,用一个网络将分布在各地的指挥控制系统连接起来。 1969 年,美国防部为确保国家重要的计算机系统在核打击情况下仍能正常运作，下令国防部高级研究计划局 ARPA(Advanced Research Projects Agency)进行建立计算机网络的研究，最后导致了世界上第一个计算机网络——阿帕网的建立。

到 70年代末期，国防部高级研究计划局又建立了几个计算机局域网并投入运行。这些局域网的建立，对提高网内各个计算机系统的效能以及其安全性和可靠性发挥了积极的作用。

由于阿帕网运行良好，许多大学和科研学术机构纷纷加入该网络，这使阿帕网日益扩展。但随着越来越多的用户加盟阿帕网，也使阿帕网变得非常拥挤，管理也日益困难。为解决这一问题，研究人员将阿帕网分成两部分，即军事网络（MILNET)和民用阿帕网(ARPANET),两者之间用网络协议 IP(Internet Protocol)联接起来。网络协议在设计上允许成千上万的计算机进入，并且规定网络内的每一台计算机原则上都与其他任何一台计算机具有同样的能力，即网上的任何计算机之间都可以进行交流。为了解决网络之间的通信问题，国防部高级研究计划局研究了一种将不同的局域网连接起来形成广域网的新方法，建成了一个广域的计算机互联网络，这就是我们目前广泛使用的因特网的前身。互联网络在 80 年代虽然得到较大的发展，但应用范围还是十分有限，使用者只是美国国内的科学工作者、大学师生和有关人员。

1972 年，在阿帕网络内，实验人员首次成功地发送了第一件网络电子邮件(E—MAIL)。

1973 年，阿帕网络和其他非地面网络系统联结成功，其中包括通过人造卫星和海面舰船网络系统进行联结的 SAT 网络系统，以及通过电话系统和地面移动网络系统进行联结的 PR 网络系统。

1985年，美国国家基金会建立了自己的 NSF 网(National Science Foundation Network)，由骨干网、中级网和校园网三层网络组成，并建立了一批地区网络把每个地区的用户联结起来。到 1986 年，随着很多商业部门从使用阿帕网转移到使用 NSF 网，NSF 网取代阿帕网成为互联网的主干网。

随着互联网技术的成熟和用户的增加，互联网的商业化趋势越来越明显。世界各地也加强了网络技术的研究和网络系统的研究。

进入 90 年代以后，互联网络在世界范围得到快速扩展，已发

展成为一种影响十分巨大的全球性国际互联网络。随着以计算机技术为核心的信息技术的迅猛发展和广泛应用，计算机网络已开始向地球的各个角落辐射，其触角伸向了社会的各个领域。据有关资料介绍，当今全球最大的国际互联网络——因特网(Internet)已经有数千万台计算机与之相联，成为名副其实的国际信息网络。它已将世界上 170 多个国家和地区的计算机网络连为一体，用户达数千万。1997 年,仅在美国就有约 5468 万人上网;1998 年初,全球上网人数已超过 1 亿人。利用因特网，用户可以顺利进行信息收发及信息查询等信息业务。它已广泛应用于医疗、交通、金融、贸易、军事等各个领域，用户仍在以每月递增 10%～15%的速度扩大，预计 2005 年上网用户将达到 10 亿人；仅在美国,23%年收入超过 10 万美元的人和 60%的大中型企业已加入其中。随着新世纪的来临，因特网更成为各国注视的焦点。而各国正在加紧建设的国家、地区乃至全球信息基础设施，最终将建成使各国乃至个人都能互联互通的全球信息网络，形成完全超越传统地理空间概念的所谓“计算机网络空间”。

（二）贯通全球的信息高速公路

为了在激烈的信息技术竞争中保持其优势地位,1993 年 9 月 15 日,美国出台了《国家信息基础设施 行动计划》。1994 年 1 月 15 日,美国总统克林顿在《国情咨文》中称,要在 2000 年前在全国建成国家信息基础设施。实际上，美国的“国家信息基础设施计划”就是要在全国建立高速光纤通信网络。这一网络的末端将深入到每一个办公室和家庭等，在全国构成四通八达、无孔不入的信息“交通网”,以实现一般信息网络不能或很难提供的信息服务。不仅如此，国家信息基础设施的建立，将成为带动美国各种高新技术发展的龙头。在这个投资额高达 4000 亿美元以上的庞大高技术计划的牵引下，美国经济和科学技术将实现新的腾飞和发展，从而在政

治、经济、技术和军事上继续占据世界领先地位。美国人认为,国家信息基础设施计划的实施，将会像当年的高速公路计划一样，成为美国经济和科技腾飞的新支柱，因此形象地将其称之为“信息高速公路”。

美国政府提出信息高速公路即国家信息基础设施计划后，世界上立即兴起了一股建设信息高速公路的热潮。发达国家和少数经济实力较强的发展中国家计划在 2000～2010 年建立覆盖本国的计算机通信网络。1994 年 9 月，美国政府又提出了建设全球信息基础设施的倡议，即将各国信息高速公路联结起来组成全球信息高速公路，实现各国信息共享。世界上多数国家都承认，尽管各国经济基础、科技水平和社会发展程度存在明显差异，但在信息技术已发展到计算机网络化的新时代，建设本国的信息高速公路并将其联结成全球信息高速公路，是历史发展潮流之所向。面对全球信息高速公路的发展趋势，虽然各国在管理经济和社会生活的过程中将遇到一系列新的难题，国际关系也将受到影响，无论是发达国家还是发展中国家都将面临严峻的挑战。但是，全球信息高速公路的建立将有利于加强国际经济、科技和教育合作，推动文化交流，加快社会向更高阶段发展，为各国提高综合国力提供难得的机遇。这是一个挑战与机遇并存的发展和变革时代。

在未来信息社会里，信息网络将遍布地球的各个角落，渗透到人类生产的各个领域和生活的各个方面，成为信息社会的重要支撑。

（三）意义非凡的网络革命

网络给人类社会带来了强烈的冲击，引发一场深刻的社会变革。用美国人的话说：其变革之巨大犹如 10 次工业革命和基督教改革加在一起同时发生在一代人身上。

因此,如果说 19 世纪是火车和铁路的时代，20 世纪是汽车与

高速公路的时代,那么,21 世纪将是电脑同网络的时代。

在全球范围内，因特网正以一种不可阻挡的势头迅猛发展着，其发展普及的速度超过以往任何一种技术。我们知道，无线广播用了 38 年时间才拥有 5000 万听众，电视用了 13 年时间拥有 5000 万观众，而因特网仅用了不到 5 年时间便拥有了 5000 万用户。目前，几乎每隔半小时就有一个新的网络与因特网相联，每过一个月就有 100 万名新的因特网使用者加盟。目前，全球已有超过 1 亿人在因特网上工作、漫游和交流，网上每 24 小时的信息流量达到万亿比特，每个月的电子邮件突破 10 亿封。

因特网的发展极大地改变了人类生活和工作的方式，深刻地改变社会结构，解放社会生产力，使人们突破物质条件的束缚、时空的限制，获得更多更公平的教育、医疗、就业和施展才华的机会。

仅在美国，因特网的发展使其信息产业涌现了一批像雅虎这样的新的明星企业，产生了新的信息服务部门，增加了几十万个高薪工作职位,产生了 2000 亿美元的经济效益。

在社会经济领域普遍信息化和网络化的同时，以计算机为核心的信息设备也在军事领域得以大量采用，已成为军事现代化和武器系统先进程度的重要标志。利用各种军用计算机网络，不仅可以把各种信息获取、信息处理、信息控制、信息传输等军用信息系统联在一起，形成庞大的一体化 C^4I 系统,实现信息获取、处理、控制和传输的一体化和实时化，而且可以把各种由计算机控制的武器装备系统、各种不同的作战部队联成一个有机的整体，实现侦察—控制—打击—评估的一体化和各种作战部队的一体化，从而极大地提高军队的作战效能。正因为如此，世界各国在跨世纪军队建设中，都把信息化作为军队建设的重点，充分利用计算机网络技术来建立各种新型的作战部队。最典型的便是美国陆军从 1994 年开始实施的数字化部队建设，其目的便是通过电子纽带把战场上的单兵、单个作战平台和战场指挥控制系统联为一体，形成一个巨型

信息网络系统。

二、可怕的网络威胁

科学技术是一把双刃剑，它即能为人类造福，同时也可能给人类带来灾难。就在互联网极大地促进着人类社会经济、文化、军事等各个领域的飞速发展的同时，电脑病毒、计算机“黑客”等前所未有的威胁也随之向人类袭来。

（一）莫里斯的“蠕虫”

随着计算机网络而出现的最大威胁，莫过于计算机病毒。说起计算机病毒，就不得不谈及莫里斯的“蠕虫”。

1988 年 11 月 2 日下午 1 分 59 秒，一种名叫“蠕虫”的“病毒”突然发作起来，致使美国 15.5 万台计算机和 1200 多个连接设备突然进入“休克”状态。联接美国国防部、美军军事基地、宇航局以及多所大学和研究机构的计算机网络突然间大面积瘫痪，直接经济损失达 1 亿多美元，间接损失更是无法估量。

这一事件的始作俑者，竟然是美国康奈尔大学电子计算机专业的年仅 24 岁的研究生罗伯特·莫里斯。他看准了他父亲——一位电脑安全防卫专家在程序设计上的几个缺点，想跟他开个玩笑，将自己设计的软件程序“注入”电脑系统，未料该程序出现了毛病，竟以闪电般的速度复制起“病毒”来。结果，首先是美国国防部远景规划局的电脑网络告急，紧接着全国 8500 台军用、民用电脑陆续被感染，陷入瘫痪和半瘫痪状态。

莫里斯的蠕虫病毒事件就像是计算机世界的一场大地震，引起了巨大的反响，震惊了全世界，引起了人们对计算机病毒的恐慌，也使更多的计算机专家开始重视和致力于病毒与反病毒研究。

尽管如此，新的病毒仍发疯式地滋生，如“黑色星期五”病毒、

阿拉梅达病毒“米开朗基罗”病毒、“GPI”病毒……这些看不见摸不着的病毒，在遍布全球的计算机网络上肆意横行，给计算机网络和以此为基础的社会政治、经济、军事系统等等造成了极大的危害。

（二）布里顿的“嗅探器”

无独有偶，在莫里斯的“蠕虫”病毒开创计算机病毒侵害计算机网络系统的先例之后，一些所谓的“计算机天才”，又发明了另一种给计算机网络带来严重危害的“武器”——各种网络“黑客”程序和系统。英国 16 岁的少年布里顿，就发明了一个名为“嗅探器”的系统，专门破译和国际计算机网络并网的计算机用户的名称和密码。运用该系统，布里顿在国际计算机网络内“渗透”进了美国政府最为敏感的计算机系统，时间长达 7 个月之久，接触到了包括弹道武器研究报告、飞机设计材料、雇员名录、后勤供应、人员档案和电子信件等内容的大量机密。 1994 年春天，当朝鲜核检查问题最为紧张之时，他甚至进入美国情报部门的计算机，搞到了内部机要通信资料，并把这些资料下载后输入到国际计算机网络中 3500 万用户都能读到的电子通信栏里。 1994 年 3 月，也就是布里顿利用他的“嗅探器”进入美国政府的计算机网站 7 个月之后，美国空军特别调查处在对计算机系统进行安全检查时，才“偶然”发现布里顿这个“不速之客”。在这一天，粗心的布里顿将自己的计算机与美国国防部计算机接通后就睡觉去了，一夜未关机，因此才被跟踪上的。当美国情报官员“捕”他时，他说自己不是什么间谍，只是觉得这样挺好玩。可美国官员不得不承认，这是迄今为止最严重的计算机网络泄密事件，它已影响到了美国军队的战备状态。在长达 7 月的时间里，布里顿已经进入了他可以“进入”的美国包括国防部在内的几乎所有政府计算机网络之中，下载了大量的机密资料，布里顿的一位同伴还把从美国国防部计算机系统获得的机要资料写成

日记。由于布里顿的计算机渗透，美国国防部数以百万计的计算机密码都要重新编制。专家们称，如果布里顿不是毫无背景的少年，而是一名训练有素的谍报人员，那么他就绝对不会一夜不关计算机,美国军方的跟踪系统也就很难发现他的‘渗透’行为。

（三）无所不在的“黑客”

对于计算机网络系统而言，无所不在的“黑客”是最可怕的威胁之一。

“黑客”(hacker)，源于英语动词 hack ,因美国麻省理工学院一个学生组织的某些成员，不满当局对某个电脑系统的使用权采取的限制措施,因而非法闯入该电脑系统而得名。通常,电脑‘黑客’是指那些未经授权而侵入他人计算机系统的非法入侵者。目前，计算机“黑客”已经成为计算机网络的主要威胁。

在 90 年代初的海湾战争中，曾经有一批荷兰黑客向伊拉克政府建议，说他们可以利用计算机网络对美国军方实施攻击。因为在战争的进行过程中，美国军方曾经频繁地通过因特网进行大量的通信联系。黑客们保证，他们可以干扰多国部队在海湾地区的部署和军事行动，使之在军事对抗中处于不利地位。从 1990 年 4 月到 1991 年 5 月之间，这批荷兰黑客一共侵入了 34 个美国国防站点的计算机系统，并把大量的军事数据复制并储存在美国一些主要大学的计算机系统中。在袭击完成后，他们还修改了计算机工作记录,抹去入侵痕迹。

近年来,随着计算机网络的进一步发展,网络‘黑客’所带来的危害也越来越严重。美国军方在 1995 年的有关报告中曾指出，在计算机网络遍布全球的情况下，美国的对手们无须进入美国，就能通过国际计算机网络对美国的计算机网络系统进行攻击。据美国国会总审计署披露,仅 1995 年一年内，企图渗透到美国军用计算机网络的‘黑客’行为就达 25 万起，平均每天约 700 起，其中有

65%获得了成功。如此频繁的‘黑客’攻击,给美国包括军用计算机网络在内的许多计算机网络系统造成了极大地危害，有些甚至导致了十分严重的后果。

1996 年 8 月 17 日,为了抗议‘正派通讯法案”,黑客们破坏了美国司法部的网页，把司法部长的照片换成了希特勒的照片，并放上了两张黄色的照片，写了许多抗议美国政府压制言论自由和专制的口号。1996年 9月 18 日，在另一起极为著名的黑客入侵事件中，美国中央情报局的网页也遭到攻击，“中央情报局”(CM,Central Intelligence Agency,Intelligence 一词在英语中既可作“情报”讲,又有‘智力’之意)被愤怒的黑客改成了‘中央愚蠢局”,并写上了许多嘲笑和谩骂中央情报局的话。

全世界数以百万计的“黑客”们，对世界上发生的任何事件都会表示自己的立场和意见，甚至作出其过激的反应。 1998 年 6 月，印度不顾国际社会的强烈反对一意孤行进行核试验后，一群自称“千足虫”的青少年黑客宣布，他们成功地进入了印度国家安全的要害部门 ——设在孟买的“巴巴原子研究中心”的电脑网络，盗走了其中高度敏感的核武器机密，包括印度和以色列两位核专家之间的电子邮件及其他的绝密资料，并将该系统储存的部分资料清洗得干干净净，还在该网中心站的主页上留下了反核信息。他们说，侵入印度军事电脑系统是为抗议印度在此前接连进行的 5 次核试验。

在如此众多的‘黑客”们的‘光顾’之下,不仅像美国国防部这样的要害部门的计算机网站成为全世界黑客们竞相进攻的“众矢之的”,其他一些不知名的网站也可能随时成为‘黑客’们闲逛的场所，从而对计算机网络及其以网络为重要基础的社会政治、经济、军事、文化等系统造成极大的危害。

（四）并非偶然的“意外”

无所不在的计算机网络面临的另一种威胁，是不断增多的“意外事件”和有组织的计算机犯罪。进入 90 年代后，随着计算机的日益普及和计算机网络的不断延伸，一些意外事件和越来越多的针对计算机网络的犯罪活动不断出现。这种意外事件和犯罪活动所造成的严重危害是如此之巨大，即使是无意中对公共计算机网络的破坏，也可以轻而易举地使一个计算机网络较普及的国家难以招架，甚至产生非常严重的后果。例如，1991 年，美国一位农民在掩埋死牛时挖断了一条光缆，结果导致美国联邦航空管理局所属 4 个主要空中交通控制中心关闭达 5 个多小时之久，造成了巨大的经济损失。1994 年，美国最大的电信公司美国电话电报公司地区交换中心系统的一套软件出了一个小小的故障，结果导致其长途电话网中断了 9 小时。

至于针对计算机和计算机网络的有组织犯罪，给世界各国造成的损失则更加巨大。据 1996 年伦敦信息安全会议公布，1995 年全球计算机犯罪损失已达 150 亿美元，2000 年则达到 200 亿美元。美国硅谷一名技术权威指出，针对计算机和计算机的有组织犯罪，如果不严加防范和打击的话，将足以使一个国家的经济陷入停顿，甚至面临崩溃，其产生的后果不亚于核爆炸后产生的强大电磁脉冲。

三、崭新的作战空间

为了有效地对付上述这些潜在的并日益增大的威胁，确保计算机网络正常运行而不被破坏，维护网络稳定而免遭攻击等一系列网络安全措施也就被提上了日程。而这种进攻与防护的矛盾运动，直接导致了一种新的军事斗争方式——计算机网络信息战的

出现，计算机网络空间也就成为一种与传统的战场空间完全不同的又一新的作战空间。

（一）网络空间的激烈争夺

面对来自网络空间日益严峻的挑战，世界各国特别是一些发达国家充分认识到，在网络空间中所进行的激烈对抗，已经逐步演变成信息战的一个重要的有时甚至是主要的方面，是一种战略信息战。因此，许多国家都采取有效措施加强网络信息战的研究，进行网络信息战的准备，从而使得网络空间的争夺更趋激烈。

美国作为互联网的诞生地，首当其冲地受到各种网络攻击。也正因为如此，美国比任何国家都更关注网络空间中所展开的激烈争夺，力图在网络信息战中掌握主动，并把提高网络信息战攻防能力，作为其信息战发展的重点。

1996 年 6月 5 日，美国参议院调查委员会在充分调查的基础上,拿出了一份‘ 电子空间安全问题 ’的基调报告。报告提出 直到最近，人们才认识到用信息战方法破坏和保卫基础设施的重要性和严重性。中央情报局局长约翰·多依奇也提出,不仅美国,某些外国也已具备进行信息战的能力，美国应为此立即做好准备。司法部副部长杰米·哥瑞利克也鼓吹，要像当年发展原子弹的曼哈顿计划那样强化美国应付信息战的能力。基于此，美国国家情报委员会在原有的“ 外国信息战计划 ”的绝密报告中增加了这方面的内容,并于 1996 年年底完成一份更完整的情报评估。美国政府安全政策委员会的白皮书提出：通过网络尤其是因特网（国际互联网）对国家基础设施的攻击已是一个现实的威胁，它将造成大范围的社会瘫痪，这显然属于国家基础范畴的安全问题，联邦政府应改变目前各自为政的情况，成立统一的负责保障国家基础设施的管理局。美国防部提出,应把涵盖军民各方的‘ 综合信息战略 ’作为一项国家战略,并于 1997 年 6月 7 日成立了‘ 国家安全情报中心 ”,由

各军种信息战部门、情报单位和信息行业各大公司组成，增拨 3.7 亿美元用于网络安全计划。 1997 年 7 月 15 日,克林顿发布总统令,成立‘保护国家要害基础设施总统委员会”,这标志着美国为对付信息战，特别是网络信息战的实际威胁已在最高决策层采取了相应的措施。

在这段时间里，美国出台了三份有代表性的报告：一是兰德公司受国防部委托完成的《战略信息战——全新的战争手段》;二是克林顿政府负责安全事务的约瑟夫·奈完成的《美国的信息力量优势》；三是五角大楼战略评估助理查理斯·斯维特完成的《因特网的战略评估》。这三份报告，反映出美国信息战战略的一些新的观念和看法。其中最主要的成果之一，就是提出了“战略信息战”，亦称‘信息基础设施战争”(IIW)的概念。美国认为,信息基础设施战争是指以信息战武器，通过信息网络对一个国家的通信网、公路铁路网、空中交通网、电网、金融网、股票交易网、油气管网等基础设施进行软破坏或软摧毁。这些网络是国家赖以生存的基础设施和基本信息资源，对其破坏的后果不亚于实施核打击。因而，这种信息战就必然具有政治性、战略性，是一种战略性的信息战。这种战略信息战的实施既可借助于军事设施，也可以使用非军事设施；既可以来自境外，也可以发自境内。这样传统的前方与后方的界限、军用与民用的界限、战争与犯罪的界限都变得模糊了，而传统的战术警报和战略预警体系，传统的情报搜集分析方法也面临新的挑战。因此,美国专家认为‘战略信息战’是一个全新的概念,它的出现带来了一系列全新的问题。并认为，美国虽然首先开发了进攻性病毒、逻辑炸弹等软杀伤武器，具备了进行战略信息战的能力，但面对上述情况也还没有能保护自己的完整对策。

在 1996 年的国防报告中，美正式把信息战列为重要内容之一，并提出了计算机空间战(Cyber Space Warfare)的概念。其基本含义是通过计算机通信网络来影响对方信息与信息基础设施，保

护己方的信息与信息基础设施，以达到国家目的的行动。其主要内容是:通过因特网,截取、利用、篡改、破坏对方的信息,或利用病毒和虚假信息来影响对方的信息与信息基础设施。

美国防科学委员会认为，世界上有 100 多个国家具备信息战能力,有 50 多个国家以美国为作战对象进行了信息战的准备，一切信息领域的珍珠港事件或切尔诺贝尔事件迫在眉睫。因此，美国要像当年发展原子弹的曼哈顿工程计划那样发展大规模信息战技术。

（二）发生在科索沃的另一场战争

人们在对计算机网络空间中的激烈对抗进行理论研究和技术准备的同时，已经逐步将计算机网络信息战付之于实践，并发挥着越来越重要的作用。在 1999 年的科索沃战争中,交战双方在计算机网络空间展开了异常激烈的对抗，互联网变成了“硝烟弥漫”的战场，以至于许多军事专家将科索沃战争称之为人类战争史上第一场真正意义上的网络信息战。

从 1999 年 3 月 24 日开始，以美国为首的北约开始对南斯拉夫联盟共和国实施了代号为“盟军”的军事打击。战争爆发后不久，双方激烈的军事冲突就从地面、空中、海上等有形空间，逐步向因特网蔓延，把网络空间变成了难以捉摸的新战场。在这里，交战双方及其支持者利用电子图像、电子公告栏和黑客袭击作为进攻的武器,对敌方的计算机网络实施了大规模的‘进攻”。

面对北约部队的狂轰滥炸，在军事上处于劣势的南联盟另辟蹊径，利用计算机网络信息战向北约进行反击。一方面，他们通过网络系统广泛开展对外宣传，揭露北约的侵略行径，从而有力地打破了西方国家对科索沃危机的舆论封锁。随着北约空袭的继续，南联盟的普通平民纷纷进入因特网进行反对北约轰炸的宣传战。由于宣传作品在因特网上特别容易发表，电子通信又使人们可以采