信息战与信息安全战略

国家保密局
国务院发展研究中心国际技术经济研究所

金城出版社

信息战与信息安全战略

国家保密局
国务院发展研究中心国际技术经济研究所

（内部发行）

金城出版社

图书在版编目（CIP）数据

信息战与信息安全战略/付德棣主编．-北京：金城出版社，1996.12

ISBN 7-80084-149-9

Ⅰ.信… Ⅱ.付… Ⅲ.信息-安全-研究-世界 Ⅳ.D526

中国版本图书馆CIP数据核字（96）第21410号

金城出版社出版发行

（北京市劳动人民文化宫内 100006）

北京昌平兴华印刷厂印刷

850×1168毫米 1/32 8.125印张 210千字

1996年12月第1版 1996年12月第1次印刷

印数：1—5000

ISBN 7-80084-149-9/D·34

定价：16.00元

（内部发行）

《信息战与信息安全战略》编委会

序　言

随着冷战时代的结束，世界格局正朝着多极化方向发展，综合国力竞争已成为各国竞争的主流，而高新技术竞争则成为决定胜负的关键。电子信息技术及其产业化建设的发展水平和规模已经成为衡量各国综合国力的标志，它关系着现代科技的发展，成为现在和下世纪争夺国际地位的焦点。自1993年9月美国正式提出兴建国家信息基础设施（NII）计划以来，西欧、日本、亚洲“四小龙”以及南亚、南美一些国家也相继提出了自己的NII计划。1994年9月，美国又提出了建立全球信息基础设施（GII）计划的倡议，以实现全球信息共享。尽管GII有利于加强国际经济、科技、教育合作和文化交流，但它也将为美国等一些国家向各国进行经济扩张、政治渗透和文化入侵提供最快捷、最方便的途径。目前全球已有不少的国家制定了计算机间谍计划。正因为如此，目前世界各国都在抓紧研究开发信息安全保密技术，组建信息安全保密工作机构，提出信息安全保密方案和实施措施，以保护国家秘密信息的安全。

为此，国家保密局、国务院发展研究中心国际技术经济研究所联合编写了《信息战与信息安全战略》一书，力图使领导同志和决策部门重视信息安全保密工作，加强信息安全对策研究，促使建立我们的信息安全防范体系，以求在今后的国际竞争中立于不败之地，保障“九·五”计划和2010年远景目标的胜利实现！

由于时间仓促，水平有限，书中存在着一些缺点和错误在所难免，请同志们批评指正。

国家保密局局长　戴生龙

1996年10月5日

目　录

前　言

公元2000年2月4日，伊朗试图迫使软弱的沙特阿拉伯减少其石油产量以提高原油价格，华盛顿准备派部队去中东为沙特阿拉伯助威。为了打击美国，伊朗选择了一种更隐蔽的方式——发动信息战。于是，白宫接到报告说北加利福尼亚和俄勒冈州的电话系统已中断，陆军在华盛顿州路易斯堡的重要基地的电话系统也中断了。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，中央情报局认为罪犯可能是伊朗特务，他们给铁路的计算机系统注入了“逻辑炸弹”并引发了这场灾难。在沙特东北的城市达兰附近，一家原油提炼厂遭受到通过计算机信息系统发动的“攻击”，引起了爆炸和大火。在伦敦，银行已检测出用来破坏证券交易的三种不同的病毒。受到一系列事件打击，纽约和伦敦的股票市场交易迅速下跌。

2月15日，美国开始派部队去中东。但是，因计算机化的“电子进攻”阻塞了派遣基地的军用电话系统，美国部队的调遣不能进行；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燥起来，肆意在顾客的帐目上增减数目；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，纷纷提出大笔存款。

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，情报军官通知国防部长，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，甚至已被摧毁。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，在那里指导五角大楼坚持与伊朗打一场缓慢而流血的战争……

展现在我们面前的这幅可怕的景象，绝不是好莱坞科幻电影的场面，而是1995年1月，美国国防部委托著名的战略研究智囊团兰德公司举行的“信息战”演习。

信息战这一战争新概念，在国外，尤其是在科技最为发达的美国也是处于萌芽状态，对信息战的理解众说纷坛。我们认为，所谓“信息战”就是以计算机为主要武器，以覆盖全球的计算机网络(如Internet网)为主战场，以攻击敌方的信息系统为主要手段，运用高精尖的计算机技术（如计算机病毒），破坏敌方所有的信息系统，不仅破坏军事指挥和武器控制系统，而且广泛破坏敌方的银行、交通、商业、医疗、通信、电力等民用系统，这样，不仅造成军事行动的混乱和失败，而且造成全社会的恐慌和不安，甚至使整个国民经济处于瘫痪状态，从而达到付出极小代价，甚至不费一枪一弹，夺取战争胜利的目的。

五角大楼把信息战定义为在一场冲突中控制电子信息系统的行动。信息战的鼓吹者非常具体生动地描述了信息战的各种手段：军事“黑客”(Hacker)从世界任何地方随时在敌方的计算机网络

中打入“软件钉子”，使之无法正常工作；外交官向驻在国的电话交换机散布病毒，使之频频出错，甚至设法关闭国际电话线路；无线电干扰仪使敌方的军用无线电系统完全失灵；电磁脉冲武器烧毁了敌方的电子设备；高灵敏度的窃听设备使敌方的指挥通信暴露无遗；……五角大楼的战略家们认为只要暂时地控制敌方的部分信息流就足以使敌人变成瞎子、聋子，受骗上当，乱作一团。

1995 年 5 月，美国中央情报局局长 William Studeman 在一次情报官员会议上承认，信息战的目标可以包括美国的通信系统、金融系统、股票交易所、税务局系统、社会保险系统、银行、战略重点公司、研究开发机构、空中交通管制系统和高技术数据库。目前这些系统都是易受外部攻击的薄弱环节。

早在 1991 年海湾战争时期，美国军方就已开始在实战中运用“信息战”这一被人们称为“第三次战争”的新的战争手段。

据美国报刊报导，海湾战争爆发前，美国获悉伊拉克将从法国购买一批用于防空系统的新型计算机打印机，并且获悉该批设备将经由约旦首都安曼运抵伊拉克。于是美国派遣潜伏在安曼的特工人员偷偷地把一套带有计算机病毒的芯片换装到这批打印机中去。这样，当伊拉克军方安装使用这批打印机后，计算机病毒就顺利地侵入了伊拉克防空指挥中心的主计算机。当海湾战争爆发、美国空军开始空袭伊拉克时，美军用无线遥控装置将隐藏在计算机中的病毒激活，致使伊拉克的防空系统陷入瘫痪，从而使美军长达 40 天的空袭行动大获成功。

海湾战争结束后不久，美国国防部的官员在庆贺信息战的胜利之余，不禁想到了美国自身的计算机网络系统的安全。他们扪心自问，如果敌方对美军发起类似的信息战，美军能经受得住吗？

事实上，美国军方拥有世界上最庞大的计算机网络系统，被称为“国防信息基础结构”的这一庞大系统是由 210 万台计算机、1 万个局域网、100 个广域网、200 个指挥中心和 16 个大型计算机

中心组成的。美国军队是世界上最依赖计算机网络的军队，从军事指挥、武器装备，直到人员调动、发放军饷，哪一样都离不开计算机。因此，信息战是一把双刃剑，美国可以利用它来攻击别人，其它国家同样也可以“以其之道，还治其身”。尤其是进入90年代以来，计算机通信技术不仅在发达国家广泛普及，而且在新兴发达国家，甚至在一些发展中国家都正在推广使用。以计算机技术为核心的信息战基本上是一场智力的较量，而不是象常规战争那样，是综合国力的较量。因此，在这场以信息为主体的战争中，发达国家与不发达国家的差距远远小于他们在常规战争中的差距。可以说，信息战是一场低成本的战争，谁都打得起。美军在武器装备上的优势恐怕已不是信息战中的重要因素。

信息战是以计算机网络为战场的，因此，在这场战争中已经没有国界之分、前后方之区别了。遍及世界各地的美军计算机网络（包括美国国内的计算机网络）随时随地都可能成为被攻击的目标。攻击者并不需要从自己的国家对美国发起攻击，他可以在世界上任何一个网络入口处对美国的计算机网络发起攻击。例如，一个携带着一台便携式计算机的伊朗特工人员可以从容地在荷兰阿姆斯特丹宁静的豪华旅馆里向在千里之外的美军信息中心发起攻击。因此，从这个角度来说，高度依赖于计算机网络的美国军队反而显得十分脆弱，对它的攻击已经不再受时间、空间、甚至经济实力的限制，而且一旦攻击得手，它的损失也远远大于其对手。

事实证明，美国国防部官员们的担心并非是杞人忧天。

1994年12月，国防部信息系统局所属的国家通信系统（National Communication System）撰写的一份报告透露，至少有30个国家正在研究开发信息战技术。该报告得出结论说：“一个决心利用信息战技术来伤害美国的敌人完全可以不考虑军用计算机系统，因为攻击民用计算机系统同样可以取胜。攻击敏感而不保密

的信息系统，如电力、电子资金划拨系统、电话网和全国空中交通管理系统等均可引起美国社会的大混乱。”

1994 年，为了测试国防部的计算机网络抵御信息战的能力，美国国防信息系统局特意组织一批“黑客”，让他们从 Internet 网向国防部的计算机系统发起攻击。结果十分令人吃惊。在被“黑客”攻击的 8900 台“五角大楼”的计算机中竟然有 88%被“黑客”掌握了控制权，而这么多攻击行动中仅有 4%被国防部的计算机管理人员发现。这两个反差极大的百分比确实使“五角大楼”的将军们吓出了一身冷汗。

然而，事情并未到此为止。随着计算机技术的突飞猛进，攻击计算机的技术不仅越来越高级，而且越来越普及。过去智商极高的“黑客”们才能掌握的“攻击术”，而今一般的计算机发烧友也能“驾驭自如”了。据美国总审计局 1996 年的一份调研报告透露，1995 年，美国国防部计算机系统总共受到了 25 万次攻击，其中有 60%左右的攻击行动得逞。1994 年 1 月至 1995 年 6 月期间，美国军方自动化系统安全事故支援小组在这 18 个月内接到了世界各地美国军事计算机网络操作人员 2.8 万次求援电话。他们也截获了数以千计的“黑客”程序。

在美国的盟国，同样的情景也时有发生。最令人震惊的是英国于 1994 年 11 月破获的一起重大的计算机泄密事件。英国电信公司一位短期合同计算机操作员，借助于公司职员提供的计算机密码“闯入”公司内部数据库，获得英国政府防务机构和反间谍机构的电话号码与地址，并通过 Internet 网将这些机密传给苏格兰的一位新闻记者。当时 Internet 网已拥有大约 2500 万个用户，他们只需花费打一次电话的费用就可以从网络里获得这些机密。被窃机密包括英国情报机构、政府的核地下掩体、军事指挥部以及控制中心的电话号码。同时泄密的还包括英国情报机关军情 5 处和军情 6 处的电话号码，英国导弹基地和军事指挥中心以及一

些高级指挥官的家庭地址和电话号码，甚至还有首相梅杰的住地和白金汉宫的私人电话号码，英国政府在发生核战争时设在某郡的核地下掩体也在此次暴露之列。

法国国防部最近证实，法国海军行动力量参谋部的计算机中储存的军事机密于1995年7月底被盗。这些机密包括几百艘盟军军舰的声音识别密码，即海军情报部门分类保存的每艘军舰的特殊的声音，这些声音可以保证情报部门准确地判定每艘军舰的航行方位。被盗的还有舰只航行图。

严酷的现实向美国政府提出了新的挑战：要打赢这一场信息战，关键在于如何有效地保障自身信息系统的安全性。制定信息安全对策成了当务之急。

其实，美国政府早在80年代末对信息安全问题已开始加以重视，尤其是对于非保密（但又是敏感的）的民用信息系统给予相当的关注。1987年，美国政府制订了“计算机安全法”。这部法规要求美国所有政府机构凡存有敏感信息的信息系统必须制订完善的信息安全计划，要求政府各机构从政策、制度、经费、人员等诸方面充分重视信息安全工作。这部法规还落实了负责全国信息安全工作的具体单位——国家标准与技术局(NIST)，明确了它的职责范围。

以这部根本大法为依据，从80年代末到90年代，美国政府以政府通告、总统训令等形式不断推出信息安全政策方针和各类规章制度，逐步形成了一整套信息安全防范体系。然而，计算机技术的飞速发展，使这些政策方针、规章制度没隔多久便显得过时，甚至失效。因此，美国政府已明文规定每隔数年就必须重新审定信息安全政策方针和规章制度，以及时适应日新月异的高科技发展形势。

进入90年代以后，信息战的理论与实践，使美国政府把信息安全提高到了“国家安全”的战略高度加以重视。美国国防部和

陆海空三军在1995年相继成立了专业化的信息战中心。信息战也成了美军军事理论界的热门课题。1995年6月，第一批16名攻读信息战专业的军官悄然从美国国防大学毕业。在过去几年内，本文开头所描绘的那种惊心动魄的信息战演习已经进行了几十次之多。目前，五角大楼的军官们正在分析这些秘密演习的结果，以期制订未来的军事战略。

1984年，邓小平同志敏锐地洞察了现代社会发展过程中信息的巨大作用，明确提出了“发展信息产业、服务四化建设”的重要论断。此后，国家计委成立了国家信息中心，全国各省市、自治区的中心城市，150个地区和近80个县市都相继成立了信息中心。这些信息中心拥有计算机专业人员2万多人，各类计算机数千台套，使我国基本上形成了一个以电子计算机为基础的信息系统。近十几年来，我国重点建立了经济、科技、统计、银行、邮电、电力、铁路、民航、海关、气象、人口等12个计算机化的信息服务系统，建成了国家公用分组交换通信网，覆盖了31个省市自治区，服务对象已延伸到了一些地、县。同期，我国建立了800多个数据库，其信息内容涉及国民经济和社会生活的方方面面，用户可以通过计算机终端从远离中心的地区超越时空的限制来获取自己所需的信息。

1993年美国克林顿政府提出了建设信息高速公路的宏伟计划。我国政府也不失时机地在1994年提出了“国民经济信息化”的奋斗目标。作为国民经济信息化的起步项目，我国推出以“金桥”（经济信息）、“金关”（外贸管理）和“金卡”（电子货币）为代表的金字系列工程。这些工程将使我国已建成的信息系统加快实现网络化。近年，我国又实施了与世界上最大的计算机网络——Internet网的互联工程，使我国的科技人员、商贸企业和广大信息用户可以通过自己办公室或家中的电脑与全世界100多个国家的6000多万个用户交流和共享信息。

庞大的信息网络将给中国的现代化建设带来巨大的利益，大大加快我国现代化建设的步伐。然而，现代化的计算机信息网络也向我国信息安全工作提出了新的挑战。如果我们的安全保密工作还停留在传统的思维模式上、停留在传统的工作方式上、停留在传统的业务内容上、停留在传统的管理体制上，那么，我们将被时代所淘汰，在新兴的“信息战”面前，我们将束手无策。研究信息时代的新动向，分析国际社会的最新发展的前沿技术，借鉴发达国家成功的做法和经验，提出我国的发展战略和实施措施，无疑对于建立起与国际信息安全工作的新形势相适应的、符合中国国情的信息安全新思路和新体制，提高我们的信息安全防范能力，将起到积极的促进作用，从而使我国在世界多极化格局的竞争较量中，占据有利地位，使我国的信息安全工作迈上一个新台阶。

第一章　信息战与信息安全

近年来，信息与信息技术的重要战略地位已被世界各国日益深刻地理解和认识。尤其在美国，特别强调信息与信息技术同国家安全的密切关系，并且认为未来国与国之间的斗争主要是信息斗争，即信息战。美国著名作家托夫勒也认为，当第三次浪潮兴起时，即人类社会进入信息时代时，所进行的战争将是信息战争。目前，美国军界已把信息战作为未来作战的主要样式开展广泛的研究。然而，要打赢一场信息战关键在于如何保护自身系统的信息安全。

1.1　信息战

1995 年 1 月，美国国防部组建了信息战执行委员会，其目的是为确定和实现国家信息战目标创造条件，并使各有关方面结成一个整体，齐心协力达成共识。为支持这个委员会的工作，国防部办公厅还要求兰德公司协助研究下列问题：界定信息战的主要特征；强化高级官员的信息战意识，使其了解信息战对国家安全的意义；发现问题并协助确定信息战的政策方向；使国家安全首脑及社会各界注重参与信息战事务；同工业界就与国家安全有关

的信息系统未来发展方向问题进行协调。

由此可见，美国国防部是想通过各方面的工作来促使政府及社会各界统一认识，以提高信息战的地位，协调在信息战问题上的行动。目前，信息战已成为美国国防部及其他有关部门关注的焦点。关于信息战的含义众说纷纭，至今尚无定论。为使我国有关部门了解并重视这方面的发展动向，现将其部分观点简介如下。

1.1.1 信息战即攻心战

美国空军大学教授乔治·斯坦认为信息战主要是心计的角逐，攻击的目标是对方决策人的心理。

一、信息战的定义

斯坦认为，从广义来说，信息战就是利用信息来实现国家的目标。信息也像外交、经济竞争和使用武力那样是综合国力的主要方面，而且它日益成为保障外交、经济竞争和有效使用武力的国家重要资源。从这个角度观察，也可以把信息战看成是社会集团之间或国与国之间通过全球信息和通信网络所进行的战争。这就是说，信息战是即将出现的“战区”，未来极可能在这个“战区”爆发国与国之间的战略性冲突。信息战还可能是实施行动，而不是战争的战场，因为信息战可以使美国不向前沿部署其军队即可达到某些重要的国家安全目标。

二、信息战的目标

信息战是针对人的思想方法或更为重要的是针对人的决策方法所进行的作战。信息战的目标是人的心理，特别是在战争与和平问题上进行关键性决策的决策人的心理。从军事方面来说，它的目标是在是否使用战略部队、何时使用以及如何使用等问题上