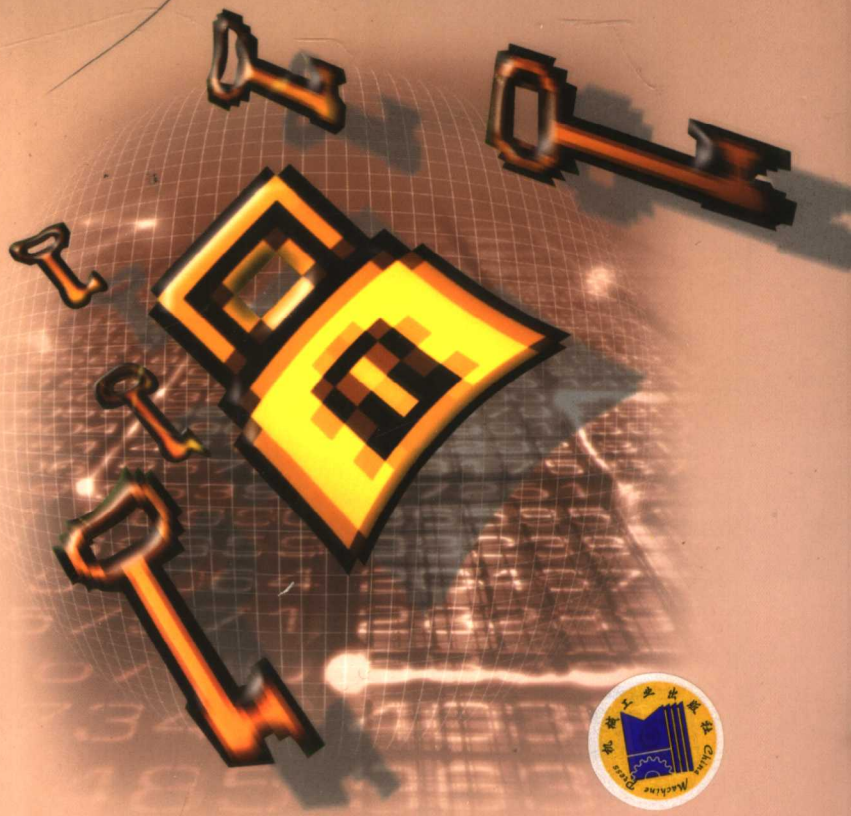
高等院校信息安全专业规划教材

网络信息对抗

- 信息对抗基本概念，TCP/IP中与网络安全相关的知识及网络风险分析方法
- 网络攻击的方法和各种网络信息对抗技术
- 网络基础设施的安全机制

提供电子教案

肖军模　周海刚　等编著



机械工业出版社
CHINA MACHINE PRESS

高等院校信息安全专业规划教材

网络信息对抗

肖军模　周海刚　等编著

机械工业出版社

本书在介绍信息对抗基本概念、原理与作用，TCP/IP 体系中与网络安全相关的知识以及网络风险分析方法的基础上，根据网络攻击的一般过程，详细地介绍了网络攻击的方法、步骤，并在合理分类的基础上介绍各种攻击手段，其中包括网络探测、扫描、口令破解、漏洞攻击、电子欺骗、窃听、木马攻击、路由器攻击和逻辑炸弹等手段的原理与实现技术；然后，根据网络边界防护与网络主机防护的要求，详细介绍了各种防护手段，其中包括路由器、防火墙、VPN、密罐、IDS 以及 Windows 2000 与 UNIX、IIS 与 Apache、病毒防护和应急响应等手段的原理与实现技术；最后介绍了网络基础设施的安全机制(PKI/PMI)。

本书可以作为信息安全专业、信息对抗专业、计算机应用专业或其他相近专业的教科书，也可以作为从事网络信息安全领域的研究生、科技人员与信息系统安全管理员的参考书。

图书在版编目(CIP)数据

网络信息对抗/肖军模等编著. —北京：机械工业出版社，2005.8

高等院校信息安全专业规划教材

ISBN 7-111-16740-6

Ⅰ.网… Ⅱ.肖… Ⅲ.计算机网络-安全技术-高等学校-教材 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2005)第 063689 号

机械工业出版社(北京市百万庄大街 22 号 邮政编码 100037)

策划编辑：胡毓坚

责任编辑：陈振虹 版式设计：霍永明

责任校对：申春香 责任印制：陶 湛

北京铭成印刷有限公司印刷

2005 年 8 月第 1 版第 1 次印刷

787mm×1092mm $^{1}/_{16}$ · 23.75 印张 · 583 千字

0001—5000 册

定价：33.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

本社购书热线电话(010)68326294

封面无防伪标均为盗版

高等院校信息安全专业规划教材

编委会成员名单

出版说明

信息技术的发展和推广，为人类开辟了一个新的生活空间，它正对世界范围内的经济、政治、科教及社会发展各方面产生重大的影响。如何建设安全的网络空间，已成为一个迫切需要人们研究、解决的问题。目前，与此相关的新技术、新方法不断涌现，社会也更加需要这类专门人才。为了适应对信息安全人才的需求，我国许多高等院校已相继开设了信息安全专业。为了配合相关的教材建设，机械工业出版社邀请了解放军信息工程大学、解放军理工大学通信工程学院、上海交通大学、西安电子科技大学、湖南大学、中山大学、南京邮电学院等高校的专家和学者，成立了教材编委会，共同策划了这套面向高校信息安全专业的教材。

本套教材的特色：

1. 作者队伍强。本套教材的作者都是全国各院校从事一线教学的知名教师和学术带头人，具有很高的知名度和权威性，保证了本套教材的水平和质量。

2. 系列性强。整套教材根据信息安全专业的课程设置规划，内容尽量涉及该领域的方方面面。

3. 系统性强。能够满足专业教学需要，内容涵盖该课程的知识体系。

4. 注重理论性和实践性。按照教材的编写模式编写，在注重理论教学的同时注意理论与实践的结合，使学生能在更大范围内、更高层面上掌握技术，学以致用。

5. 内容新。能反映出信息安全领域的最新技术和发展方向。

本套教材可作为信息安全、计算机等专业的教学用书，同时也可以供从事信息安全工作的科技人员以及相关专业的研究生参考。

机械工业出版社

前　言

实际上，在古代战争中，就存在着信息对抗。作战双方保守作战意图和行动秘密以及在作战过程中的斗智行为，都是信息对抗的体现。在19世纪末和20世纪初，无线电以及雷达的发明及其在军事中的应用，使信息对抗进入到了电子对抗的新阶段，并在战争中发挥着无法替代的重要作用。20世纪50年代后，信息对抗又扩展到红外、激光等光电对抗领域。1988年，当一个美国年轻人莫里斯把一个“蠕虫”程序放到了Internet上，导致几千台网上机器瘫痪的时候，又标志着信息对抗扩展到了计算机网络空间。在1991年海湾战争期间，美军及其盟军采用了各种电子对抗和网络对抗手段，摧毁了伊拉克军队的C^3I系统，致使伊军的作战能力完全丧失，这又使信息对抗发展到综合电子战阶段。

信息对抗先后在两次海湾战争中发挥了重要作用，在各国军队中产生了极大震动。现在，世界各主要强国都把发展自己军队与国家的信息对抗能力作为军队和国家安全策略的重要组成部分。人类社会已在向网络化、信息化发展，军队也要向信息化发展。未来的战场将是数字化战场，实现传感器网络、指挥控制网络和武器平台网络的有机互联，支持实施网络中心战。因此，我们认为信息对抗的主战场是计算机网络空间，谁能在信息对抗中取得主动权，谁就能在该空间中取得信息的控制权。信息对抗成败的关键在人才和先进的装备，我们应该加强这一领域中人才的培养工作和技术研究工作，这就是我们编写本书的主要目的。

本书围绕网络攻击与防护技术为中心的内容展开。第1章介绍信息对抗的发展历史及其内涵、功能和对抗的样式，使读者从较高层次去认识信息对抗。第2章从网络安全的角度介绍TCP/IP的主要有关内容。第3章介绍风险分析的理论与方法，介绍了主流操作系统UNIX和Windows 2000可能存在的安全缺陷。这三章的作用是为后续章节的学习打基础。第4章和第5章的内容，基本上是根据网络攻击的过程安排的，即按照网络探测与扫描、网络侵入、信息窃取以及网络破坏等的次序编写的。第6章主要探讨了网络边界防护的各种技术手段。包括路由器、防火墙、VPN、密罐、IDS等防护技术与方法。第7章主要介绍了主机防护的各种手段，包括UNIX、Windows 2000操作系统的安全配置、网络服务的安全防护、病毒防护与应急响应等方法或措施。第8章介绍有关网络基础设施的安全保护问题，主要介绍了PKI/PMI的原理与主要内容。虽然需要介绍的信息对抗技术还有很多，但受篇幅限制，本书只能介绍其中的主要内容，但已足以使读者了解与掌握信息对抗的基本内容与技术，为今后在该领域的发展打下扎实的基础。

本书第1、2、3、8章由肖军模编写，第5、7两章由周海刚编写，第4、6两章由肖军模、周海刚合写，最后由肖军模统稿、修改完成。参加编写工作的还有于振伟、戴江山、刘军、郭继斌、徐锐、刘晶，张增军、袁震等同志，张凯泽同志提供了第2章的主要内容。在编写过程中我们还得到解放军理工大学通信工程学院信息安全研究中心其他同志有益的帮助，并参阅了许多同行作者的著作，在此向所有为本书做出贡献的同志致以衷心的感谢。

由于信息安全与对抗技术是一个新兴的研究领域，而我们对这一领域的研究还不够深入，对于书中存在的错漏之处，欢迎读者和专家提出批评改进意见。

为了配合教学，本书还提供了与教材配套的电子教案，读者可在机械工业出版社网站 www. cmpbook. com 上免费下载。

作　者

目　录

第1章 概 述

信息对抗是伴随人类社会中不同利益的个人、组织或国家之间的竞争、对抗或战争等活动而产生的一种社会现象，都是通过争夺对信息的控制权和使用权达到在对抗中获胜而展开的斗争。由于军事斗争的需要，各个时期开发的信息对抗手段一般都最先应用于军事，因此，信息对抗在军事斗争中，尤其是战争中的应用是最广泛的和最鲜明的。本书将重点从军事应用的角度去介绍信息对抗的概念、手段与技术。信息对抗包括的内容相当广泛，除了电子对抗、网络对抗等样式外，实际上还包括心理、认知等层次上的对抗，所有这些对抗对决定战争胜负都发挥着十分重要的作用。由于篇幅原因，本书将重点介绍网络信息对抗的原理、技术与手段，简要介绍一些电子对抗的历史与知识，而对心理和认知层次上的对抗则不涉及。另外，目前关于信息对抗的资料与著作甚多，相关概念不尽一致，如信息战、信息对抗、信息斗争、信息作战、信息运作等，本书不想研究它们的概念定义与区分，或试图给出一个全面定义，但可能在适当的场合用到它们。

1.1 信息对抗的产生与发展

信息对抗行为是自古以来就有的，早在4 000多年前，古埃及人就开始使用密码来保密传递的消息。在进攻之前设法隐蔽自己的作战部队的行踪或对外释放假象，然后出其不意地实施突然进攻，往往是取得作战胜利的最好策略，古代的特洛伊木马的故事也描述了一种在现在仍然使用的十分有效的信息对抗手段。

在信息对抗过程中，对抗的一方会采取各种机制(方法、技术、手段与措施)来确保己方的信息安全，对抗的另一方则是通过破解对方的机制获取对方的秘密信息。信息对抗的目的则是确保己方信息的保密性、完整性和对信息利用的能力，获取信息的优势，达到对抗胜利的目的，同时设法不让对手拥有同样的能力。

但是，信息对抗技术的重大发展则是近代的事。19世纪末和20世纪初发展起来的无线与有线通信的远距离通信技术使信息对抗形式发生了重大的变化，使信息对抗成为决定战争胜负的最重要因素之一。随着电子技术、计算机技术、通信技术和网络信息技术的飞速发展，信息对抗技术得到了广泛的发展与应用，信息对抗的形式发生了革命性的变化，成为促成当前正在进行的新军事变革的发生与发展的重要原因之一。为了使读者对信息对抗的概念及其手段与技术有较全面的了解，下面分别简要介绍从无线与有线通信手段诞生以来的现代信息对抗概念、技术与手段的发展过程。从信息对抗的发展过程来看，可以大致划分为三个时期：古代信息对抗时期、电子对抗时期、综合信息对抗时期。

1.1.1 古代信息对抗时期

这个时期一直延续到19世纪末和20世纪初无线电通信在军队中正式应用时为止。从信息对作战作用的角度讲，古代战争中的探子、细作就是为了获取敌人行动信息的；烽火、鼓

与号角、信使、信号旗、驿站的主要任务是传递信息的；古代的信息处理主要靠指挥人员的大脑。信息的获取、传输与处理主要靠人的感觉器官、人工操作，有时也靠畜力和火光传递信息。由于信息的获取方式和传递手段落后，古代战场指挥人员很难获得全面而及时的信息，大大影响了信息在战争中的作用，但也有利用对信息的控制权取得战争胜利的范例。

“三国演义”中的东吴大将吕蒙通过控制关羽设在荆州附近的烽火台，使得在外地作战的关羽得不到荆州守军的求救信息，很容易地占领了荆州。荆州的烽火台是关羽的信号系统，吕蒙破坏了关羽的战场信息生成与传输系统，所以取得了胜利。

“四面楚歌”的故事是一次典型的心理战范例，项羽的楚军被韩信的军队十面埋伏于垓下，韩信令汉军士兵大唱楚国民歌，引起楚军士兵的思乡之情，楚军丧失斗志，大量逃亡，最后项羽自刎而亡。心理战通过散布虚假信息或夸大的真实信息来影响敌军的军心，尤其是指挥员的心理，使他们的心理防线崩溃，不战自败。

由于古代战争中信息的获取主要靠人的感觉器官的直接作用，作战双方控制信息的能力有限，信息作战的主要形式是指挥员之间的斗智行为。古代战争通常讲究斗智斗勇，斗智是双方指挥员之间的智力与指挥艺术的较量。哪一位指挥员有较高的聪明才智，掌握的信息多，而且能够综合应用，他就能够在战争中取得胜利。

1.1.2 电子对抗时期

这个时期包括从 1905 年的日俄海战开始到 20 世纪 90 年代初的海湾战争爆发前的整个时期，信息对抗主要在电磁频谱空间内进行。自 1896 年俄国波波夫发明了无线电报以后，无线通信技术很快就应用到军事领域中，最初形式的电子信息对抗也就开始了。电子信息对抗是指敌对双方在电磁空间中，围绕对电磁频谱的控制权与使用权展开的斗争，这种斗争常被人们称为“电子战”。电子战的样式与内容是随着用于军事的各种电子系统与设备(如无线通信、导航、雷达、敌我识别、计算机、制导武器等)的功能与技术的提高而发展与变化的。先后经历了无线电通信对抗、导航对抗、雷达对抗、武器制导对抗、电子毁伤和综合电子战等技术发展阶段，这些技术与手段的发展不是淘汰式的，而是增强式的和领域扩展式的。下面通过现代军事斗争史中的几个典型战例，说明电子对抗技术的发展与应用情况。

1. 初期电子对抗

为了加强远东海军针对日本海军的作战力量，俄国从其欧洲部分派遣第二太平洋舰队远征远东，准备进驻海参崴军港。日军联合舰队利用无线接收装置窃听俄军舰队的无线电通信，准确掌握了俄军舰队的航行路线，在预定海域等待俄军舰队的到来。1905 年 5 月 27 日日军舰队向毫无准备的俄军舰队突然开火，并干扰俄军的无线通信信道，使得俄军互相无法联络，无法互相支援，只得四处溃逃。日军又窃听到俄军残余舰队的集结位置，并迅速包围了他们，俄军残余舰队最终无法突围，只得向日军投降。这次日本海大海战俄军舰队全军覆没，共有 19 艘军舰被击沉，7 艘被俘获，伤亡 11 000 人。而日军损失很小。日军取得这样大的胜利，主要因为他们在两军无线通信对抗中，取得了控制信息的优势。这是人类历史上第一次以电子对抗的形式进行战场大规模信息战，体现了通过电磁空间远距离获取战场信息的巨大作用。

到了第一次世界大战，各帝国主义国家军队普遍使用无线电通信技术，各国军队为了防止无线通信失密，纷纷采用密码电报，同时也加强了破译通信密码的研究，使得以空间电子

战为主要作战式样的信息作战进入到破译与反破译、侦察与反侦察、欺骗与反欺骗的新阶段。1916 年 5 月底，英德海军在日德兰大海战中，德军强大的公海舰队以无线电静默方式隐蔽尾随在一小型舰队的后面，并让该小型舰队频繁发报故意暴露自己的位置，引诱英军主力舰队出航，德舰司令命令德国港口内的无线电台以公海舰队司令的呼号不断发报，制造主力舰队仍在港口内的假象，这一招果然使英军海军司令杰力克上当，结果英军遭到很大损失，英军损失 14 艘军舰，战死 6 000 余人，德军舰队损失也不小。这是一次近代战争史上人类利用电子欺骗取得战争胜利的电子战的战例。这一时期的电子对抗主要是为了侦察、破译对方无线通信的内容，是以获取情报为主要目的，干扰是次要的，因此，可以把这一阶段的电子对抗看作是一种初级的通信对抗。

2. 二战中电子对抗发挥了重要作用

电子对抗的作用在第一次世界大战中发挥的作用，引起了当时世界各军事强国的高度重视，许多国家研究了无线电导航、探测与测距等技术，研制成功了相应的导航系统和雷达系统。在第二次世界大战中，这些技术得到了广泛的应用，形成了电子导航对抗、雷达对抗等新的电子对抗形式。包括得到进一步发展的通信对抗技术在内，所有这些电子对抗的手段在战争中都发挥了重要作用，甚至影响了战争进程。

到了第二次世界大战后期，各种电子对抗手段得到了综合应用，使电子对抗达到很高的水平，在战争中发挥了极其重要的作用，这一作用充分体现在著名的诺曼底战役中。美、英等国为了开辟欧洲反法西斯第二战场，准备动用 300 万盟军、6 000 多艘舰船和11 000 多架飞机参战，计划跨过英吉利海峡，在法国北部的诺曼底登陆。如此大的军事行动如何能瞒住德军，减少登陆部队的损失呢？盟军方面采用了多方面的信息对抗手段欺骗德军。主要的手段有：盟军在远离诺曼底的法国加莱的海峡对岸的英国多佛儿地区设立了一个假司令部，由美军巴顿将军任司令，并故意拍发泄密电报，吸引德军的注意力；盟军指令法国抵抗力量破坏德军有线通信设施，迫使德军使用无线通信联络，而盟军已经掌握了德军的通信密码，可以掌握德军的动向；摸清德军在法国海岸部署的雷达、通信、导航等电子设备的位置、参数、使用规律等信息，在登陆作战开始时将它们绝大部分摧毁，对于残存的德军雷达站则实施强大的电子干扰，使得德军的警戒雷达、炮瞄雷达难以发现目标，德军的无线通信系统无法通信联络，德军的指挥陷于一片混乱，盟军仅以损失六艘战舰的战绩在诺曼底顺利登陆。整个战役盟军损失如此小，主要应归功于战前和战争过程中盟军对德军进行了强有力的信息战，通过信息欺骗、电子欺骗、电子干扰等手段使德军得不到真实信息，致使德军指挥官决断错误，最后导致失败。

3. 越南战争扩大电子对抗新领域

在越南战争中，在美军空袭和北越反空袭的过程中，双方都使用了新式武器和新的电子对抗手段，精确制导导弹或炸弹是这些新式武器中最突出的作战兵器，围绕如何对抗这些新式武器，使电子对抗水平上了一个新台阶。

为了对付北越使用苏制的精确制导的防空武器 SA-2 和 SA-7 地空导弹，美军在各种类型的作战飞机上相继安装了雷达告警接收机、有源干扰机与无源干扰投放器组成的电子对抗自卫系统，重点干扰地面或空中的各种制导武器。此外，美军还大力发展专用电子战飞机，如 EB-66 和 EB-6A，这些飞机安装的电子战设备比较完善，可以对地面各种警戒、引导、炮瞄和导弹制导的雷达实施全面的侦察与干扰。美军的这些措施显著地提高了自己飞机的生存

能力。

越南战争的一个更显著的特色是开拓了更多的电子对抗新领域，其中最重要的是展开了光电领域内的对抗，而且反辐射导弹也开始应用于实战。

随着光电技术的进步，利用光电技术作为制导控制的导弹、炸弹被制造出来，并在战场上得到应用。例如，在 1972 年春，越南使用前苏联提供的红外制导的单兵肩抗防空导弹 SA-7，在 3 个月内击落了 24 架美国飞机。美军很快研究出了与飞机尾喷口红外辐射特性相似的红外干扰弹和红外告警器(AN/AAR-43/44)，并迅速安装到飞机上，使来袭的 SA-7 导弹受红外诱饵欺骗而偏离目标飞机，SA-7 的作用因此大大降低。还有一个典型战例是，1972 年 5 月的一天，美军利用 20 枚刚研制成功的激光制导炸弹，在 2 个小时内就炸毁了包括清化桥在内的 17 座桥梁，而自己无一飞机损失。而在此之前，美军曾为了轰炸河内附近的这座清化桥，先后出动 600 余架次飞机，投弹数千吨，不仅未炸毁目标，而且还损失了 18 架飞机。激光精确制导武器在战争中的重要作用，又促进了对抗激光制导武器的技术的发展。这些战例表明，电子对抗除包括传统的通信对抗和雷达对抗领域外，又新增加了光电对抗领域。从此以后，各国军队都十分重视光电对抗技术的研究与应用，光电对抗系统成为高价值作战平台(如飞机、军舰、坦克等)必须装备的设备与系统。光电对抗领域也就成为电子对抗的最重要领域之一。

在面对越南方面强大的地面防空炮火威胁，美军认为破坏敌防空雷达系统是一种有效的压制地面防空火力系统的措施。为此，美空军研制出了针对各种辐射源的武器——“百舌鸟”导弹，并且组建了特种航空兵(野鼬鼠)部队，专门对付地面雷达等辐射源目标，取得了很好的实战效果。反辐射导弹的出现表明电子对抗已经由“软杀伤”发展到“软、硬杀伤结合”的阶段，反辐射导弹成为一种重要的电子对抗武器。对反辐射导弹及其对抗技术的研究从此成为电子对抗领域的一项重要内容。

1.1.3 综合信息对抗时期

进入 20 世纪 80 年代后，计算机技术、网络技术和信息处理技术迅速发展，人类社会快速进入信息化时代。尤其 80 年代末期后，计算机与网络设备进一步微型化、性能与可靠性又有很大提高。进入 90 年代后，Internet 走向了全世界。在 Internet 向商业化发展的同时，网络技术也在向战役与战术领域发展，C^3I 也随着向战场发展，向战斗指挥员、士兵个人，向武器平台方向发展。信息战已经从电子对抗发展成为整个 C^3I 系统之间的对抗，信息战的主战场也从纯电磁空间发展到光谱空间和计算机网络空间，形成光、电和计算机多种手段、多种样式的综合信息对抗。下面以海湾战争中的信息战与和平时期一些典型的“黑客”攻击事例，说明这一时期信息对抗的特点。

在海湾战争开始前的几个月时间内，美国通过自己在高科技方面的优势，利用各种手段，其中包括卫星、空中侦察飞机、无人侦察飞机、地面情报系统、船载电子侦察系统、雷达与战地传感设备等多种先进侦察手段对伊拉克军事行动与部署进行了详尽周密的侦察，同时也干扰伊拉克方面的侦察活动，所以在战争开始前美军已经控制了战场信息获取权。此外，在政治、外交方面，美国更是不遗余力的四处活动，大造各种舆论，充分利用各国人民痛恨侵略、爱好和平的愿望，最终获得了联合国的授权，既达到了自己对海湾石油资源控制的目的，又使自己对伊拉克的作战行动披上了合法的外衣。在美国有效的政治、外交与舆论

的攻击下和世界各国的反对下，战争还未开始，伊拉克已经完全处于孤立状态，失败已属必然。美国进行所有的这些努力，都属于它海湾信息战组成的一部分，都达到了它预期的目的。

在海湾战争正式开始后，美军空袭的首要目标是使伊拉克的军事信息系统 C^3I 全面瘫痪。他们把破坏伊拉克指挥控制设施、发电设施、电信与 C^3I 系统枢纽、一体化战略防空系统等目标列为 12 项重点空袭目标群中的前 4 位，而轰炸伊拉克军队地面有生力量仅被列在第 11 位。伊拉克的一体化战略防空系统遍布伊拉克与科威特领土，对美空军的威胁最大，美军破坏该系统时首先破坏其指控中心、雷达和通信枢纽，而不是防空导弹、高炮和战斗机等武器装备。在战争开始后的 24 小时内，美军又是重点破坏巴格达地区 40 多个领导指挥机构、防空和配电设施、C^3I 主结点等关键目标，使得战争一开始，伊拉克的首脑指挥机关全面陷于瘫痪，隔断了它们对自己作战系统的指挥控制权。由于伊拉克的所有的信息探测系统和信息传输系统不是被硬轰炸破坏了，就是被软干扰封锁住了，伊拉克的飞机、导弹、坦克、防空火炮和各种军事设施就变成了“聋子”、“瞎子”，成了美军各类高科技武器试验的靶子。在以后的 30 多天空袭中，美军继续对伊军实施电子侦察、电子干扰为主的强有力的电子对抗措施，干扰伊军残余的雷达与无线通信系统，使得伊军的坦克、飞机、导弹、自行火炮等武器找不到作战目标。

为了躲过伊拉克军队的雷达侦察，多国部队使用隐身飞机担任首攻任务。在战前充分详尽侦察准备的基础上，在开战第一天(1991 年 1 月 17 日)凌晨，美军派隐身效果极好、突防能力极强的 F-111A 隐身战斗轰炸机躲过了伊拉克雷达的监视飞到巴格达上空，利用精确的激光制导炸弹，首先炸毁了伊拉克的电信大楼，随后出动的 30 多架 F-111A 隐身飞机准确攻击了伊拉克的指挥设施、C^3I 枢纽、固定雷达、发电设施等要害部位，并且在这些隐身飞机的带领下，大批攻击机对巴格达实施了大规模空袭，使伊拉克防空系统与指挥系统立即瘫痪。事实证明，隐身技术是对抗雷达侦察技术的一种非常有效的技术，从此隐身与反隐身对抗技术的研究成为电子对抗的一项新的内容，成为各国军队十分重视的研究与应用领域。

在这次海湾战争中，多国部队几乎运用了所有先进的电子对抗技术与手段，使这次战争几乎成了多国部队电子战的实验场。仅电子战飞机就占作战飞机的总数的 10% 以上，电子战飞机的出动数约占空袭飞机的总出动数的 20%，正是因为美军完全取得了战场电磁空间的控制权，不仅使多国部队的空军损失微乎其微(仅损失 38 架飞机,战损率不到 4/1 000)，而且大大缩短了地面战争时间(仅 100 小时)，而伊拉克空军作战能力损失 90% 以上，伊拉克地面部队作战能力损失一半左右。在对垒的两军总兵力超过 150 万人的战场上，在不到半年的时间里造成如此大的胜负差距，地面进攻时间如此之短，在人类战争史上是罕见的。这一场战争标志着以消灭敌人有生力量为主要目标，以地面机械化部队直接对垒“拼钢铁”为主要作战样式的作战时代已经结束，代之以彻底压制或破坏对方信息系统、获取战场态势信息的控制权为主要目标、以两军 C^3I 系统对抗的信息战为主要作战形式的作战时代的开始。

经过这次海湾战争后，又经过十余年的经济制裁，伊拉克军队已经变得十分虚弱，C^3I 系统已经不健全，所以 2003 年 3 月在美英联军的打击下，伊拉克几乎没有任何招架之力，这次伊拉克战争并没有体现出激烈的电子对抗场面。但也有值得一看的亮点是发生 GPS 对

抗的精彩一幕。伊拉克利用从俄罗斯引进的 GPS 干扰设备，引偏了许多美军的巡航导弹与 GPS 制导武器，曾使美军头疼了一阵。但美军很快利用反辐射导弹毁坏了这些干扰设备，使伊拉克很快失去了对抗能力。但不管伊拉克的 GPS 干扰在这次战争中发挥了多大作用，GPS 对抗开辟了电子对抗又一新的领域却是不争的事实，已经引起了各国军队的高度重视，可以预见，GPS 的对抗与反对抗技术的研究将成为今后很长时间的热点，在下一场未知的战争中很可能成为双方对抗的主角。

1.2 信息对抗的内涵与模型

信息对抗作为一种新概念，有关理论还正在发展过程之中。有关信息对抗的实践还是处于初级和简单的阶段。虽然在 20 世纪 90 年代海湾战争及其以后的几场战争中，美军使用了信息战手段，取得了明显的信息优势，但总的说来，由于对手非常的弱，尤其是在电子信息技术方面的明显落后，真正的大规模信息对抗实际上并未发生。因此，下面对信息对抗概念与模型的探讨必然也是初步的，只是引玉之砖。

1.2.1 信息对抗的内涵

在军事上，信息对抗的本质是两个或多个敌对者在信息领域内，利用先进的电子信息技术和装备，使己方获取对战场信息的感知权、控制权和使用权而展开的斗争。由于斗争是限定在信息领域中进行的，因此信息对抗是围绕着信息的整个生命期过程(包括信息的获取、传输、储存、处理和决策、利用与废弃等阶段)而展开的。在计算机网络日益普及的今天，信息的储存、处理与利用都必须依赖于信息系统，信息的传输必须依赖于有线的或各类无线的网络系统，因此，信息对抗实际上是在保护己方的信息、信息处理、信息系统和计算机网络空间安全的同时，为破坏敌方的信息、信息处理、信息系统和计算机网络空间安全而采取的各种行动。

支持信息的产生、传输、处理和储存的设施称为信息基础设施，这就是说，信息对抗是在信息基础设施中展开的。广义的信息基础设施由数据、信息、设备、电信系统和人员等要素组成，信息对抗的目标就是要获取明显的信息优势，进而获取决策优势，最终使军队获取整个战场优势。信息对抗的战略目的是在保护己方信息系统安全的同时，通过利用、封锁及施加影响等手段，攻击对方的国家和国防信息基础设施，以夺取和保持决定性的优势。

信息对抗的概念同样也适合政治、经济及商务等领域，互相对立的或竞争的利益集团也同样为了获取对方的敏感信息，使自己在斗争或竞争中获得先机和处于优势地位。

在军事领域中，信息对抗争夺的焦点是信息的独占权、控制权和使用权，其攻击对象是敌方的军事信息系统或具有军事价值的民用信息系统，其中主要是敌方用于获取信息的探测系统、传送信息的通信系统、指挥控制系统(包括信息服务器、决策支持与指挥系统、计算机处理平台以及操作人员)等。因此，信息对抗的内涵包括：在准备和实施军事行动过程中，为夺取并保护对敌信息优势，按统一的意图和计划而采取的一整套信息保障措施，其中包括信息优势、信息进攻和信息防御(参见图 1-1)。

信息优势是指能够及时获取敌我双方准确而完整的信息，近实时生成战场态势，通过信

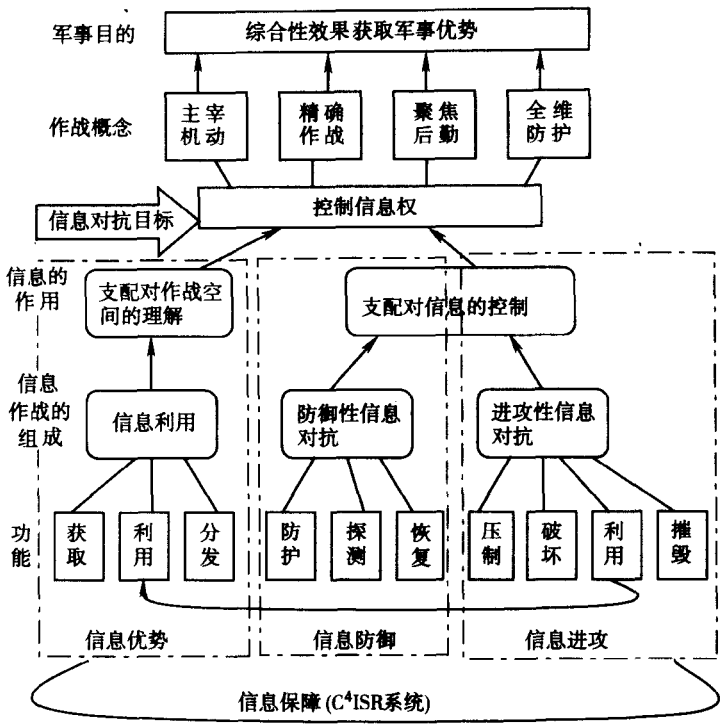


图 1-1　信息对抗的内涵

息分发，为各级指挥员提供可靠决策依据；信息进攻是使用各种软硬件(信息的或火力的)进攻手段，破坏敌方的信息保障能力和敌方的信息系统(如指挥自动化系统 C⁴ISR)等一整套措施；信息防御是在敌方对己方实施信息进攻的情况下，为确保己方信息系统的正常运转而采取的各种措施。

在战场上双方的 C⁴ISR 系统通过电磁空间互相交连，同时各自又与自己后方的战略网连接。C⁴ISR 系统是国防信息基础设施的基础部分，是双方实现各自信息保障，进行信息对抗的最主要的硬件基础与工具，这已得到各国军方的认同。因此要求 C⁴ISR 系统必须是具备信息攻防兼备能力的综合性军事信息系统，其作战职能包括探测预警、情报侦察、通信、指挥控制和电子战分系统。

按层次分，信息对抗可以分为国家信息对抗、国防信息对抗、战略信息对抗和战术信息对抗。按性质分可以分为进攻性信息对抗和防御性信息对抗。按杀伤机理分可以分为软杀伤类的信息对抗(如计算机网络攻击、病毒战、情报战、心理战等)，硬杀伤类信息对抗(如强力电磁炸弹攻击)和“软硬兼施”的信息对抗(综合利用火力打击与信息武器)。按时间划分，可分为和平时期的信息对抗、危机时期的信息对抗和战争时期的信息对抗。和平时期的信息对抗包括政治信息战、经济信息战、文化信息战、网络情报战、心理战等形式；和平时期信息战的样式基本上都可以应用于危机时期或战争时期，在平时与危机时期，信息对抗主要以获取各类情报为主，不会去破坏对方信息系统与网络的正常运行，但到了战争时期，由于双方已经处于敌对状态，对对方的网络及信息系统实施破坏战，甚至是瘫痪战可能会成为主要的信息对抗样式。