高等学校规划教材·电子、通信与自动控制技术

PROGRAMMING TEXTBOOKS FOR HIGHER EDUCATION

信息对抗理论与技术

王 成 牛奕龙 编

西北工业大学出版社

信息对抗理论与技术

王 成 牛奕龙 编

西北工业大学出版社

【内容简介】 信息对抗技术是一个多学科相结合的专业，主要涉及计算机科学与技术、信息与通信工程、电子科学与技术、控制科学与工程、光学工程等学科。

本书分为上、下两篇。上篇全面介绍了信息对抗的作用、信息对抗技术、信息进攻和信息防御的内容。同时，以雷达对抗和水声对抗为例，介绍了有源对抗和无源对抗技术。下篇主要是网络对抗部分的内容，介绍了网络攻击的基本概念和各种网络攻击技术，详细介绍了信息安全工程、信息交换安全技术及网络系统安全技术。

本书可作为高等院校计算机类专业、信息对抗专业本科生的教材，也可以供初学者和相关技术人员参考。

图书在版编目(CIP)数据

信息对抗理论与技术/王成，牛奕龙编. —西安：西北工业大学出版社，2011.1
ISBN 978-7-5612-3003-9

Ⅰ.①信… Ⅱ.①王…②牛… Ⅲ.①计算机网络—安全技术 Ⅳ.①TP393.08

中国版本图书馆 CIP 数据核字(2011)第 015825 号

出版发行：西北工业大学出版社
通信地址：西安市友谊西路 127 号 邮编：710072
电　　话：(029)88493844　88491757
网　　址：www.nwpup.com
印 刷 者：陕西天元印务有限责任公司
开　　本：787 mm×1 092 mm　1/16
印　　张：8.75
字　　数：206 千字
版　　次：2011 年 1 月第 1 版　2011 年 1 月第 1 次印刷
定　　价：20.00 元

前　言

信息对抗技术是一个多学科相结合的专业，主要涉及计算机科学与技术、信息与通信工程、电子科学与技术、控制科学与工程、光学工程等学科。

本书在内容选取上，既注意到理论的系统性，又顾及选材的多样性，突出了理论与实践的结合。本书还在传统信息对抗的基础上加入了水声对抗内容，彰显了该专业的特色。

本书分为上篇(1～7章)和下篇(8～13章)。内容安排如下：

第1章：介绍信息对抗的基本概念、基本样式和作用；

第2章：介绍信息进攻的概念和常见的4种信息进攻方式；

第3章：介绍信息防御的概念和常见的4种信息防御方式，以及信息安全保密措施；

第4章：介绍雷达对抗技术的分类、特点，以及雷达告警技术、雷达情报侦察技术、无源定位技术及有源干扰技术；

第5章：介绍雷达无源对抗技术的分类、特点及发展趋势；

第6章：介绍水声对抗技术，包括水声对抗的重要性、作用及任务，并介绍水声探测设备及水声对抗器材；

第7章：介绍水声反对抗与目标识别技术；

第8章：介绍网络安全威胁的基本概念，包括ISO定义的安全威胁、网络安全服务、网络安全机制、网络安全管理、网络安全系统结构、信息安全交换技术、网络安全交换技术；

第9章：介绍常见的网络攻击技术，包括分布式拒绝服务攻击、缓冲区溢出攻击及IP欺骗攻击；

第10章：介绍密码技术内容，包括对称加密算法、非对称加密算法、数字签名算法、单向散列函数、身份认证技术等；

第11章：介绍信息安全工程，包括信息安全工程基本概念、信息安全标准化、信息安全评估标准、信任度评估方法及信息安全准则的应用；

第12章：介绍信息交换安全技术，包括数据链路层安全协议、网络层安全协议等；

第13章：介绍网络系统安全技术，包括基本概念、网络防护技术、网络检测技术等。

由于水平有限，书中难免存在缺点和不足之处，敬请广大读者和同行批评指正。

编　者

2010年11月

目　录

上篇　电子对抗

下篇 网络对抗

上篇　电子对抗

第1章 绪 论

1.1 基本概念

1.1.1 信息的基本定义

“信息”一词有着很悠久的历史，早在两千多年前的西汉，即有“信”字的出现。“信”常可作消息来理解。作为日常用语，“信息”经常是指“音信、消息”的意思，但至今信息还没有一个公认的定义。

信息是物质、能量及其属性的标示[2006年，医学信息(杂志)]。

信息是确定性的增加。

信息是事物现象及其属性标识的集合。

信息以物质介质为载体，传递和反映世界各种事物存在方式和运动状态的表征。

信息是物质运动规律总和，信息不是物质，也不是能量！

信息是客观事物状态和运动特征的一种普遍形式，客观世界中大量地存在、产生和传递着以这些方式表示出来的各种各样的信息。

信息论的创始人香农认为：“信息是能够用来消除不确定性的东西”。

信息是抽象于物质的映射集合。

信息是有价值的，就像不能没有空气和水一样，人类也离不开信息。因此人们常说，物质、能量和信息是构成世界的三大要素。所以说，信息的传播是极其重要与有效的。

信息是事物的运动状态和过程以及关于这种状态和过程的知识。它的作用在于消除观察者在相应认识上的不确定性，它的数值则以消除不确定性的大小，或等效地以新增知识的多少来度量。虽然有着各式各样的传播活动，但所有的社会传播活动的内容从本质上说都是信息。

1.1.2 信息对抗的分类

信息对抗可分为广义信息对抗和狭义信息对抗两类。

1. 广义信息对抗

广义信息对抗指双方(敌对)在政治、经济、外交、军事、科技和文化等领域运用信息技术手段而进行的(秘密或公开的)有控制的、破坏性或毁灭性的对抗。

广义信息对抗的内容涉及军事和民事两大领域，包括：

(1)为维护国家的安全和利益，对于信息技术和系统所进行的研究、生产、装备、使用活动。

(2)对于其他国家上述活动所进行的侦察、干扰、破坏和技术上的对抗与竞争，以及其他运用信息技术手段为本国安全利益所进行的斗争。

广义信息对抗的基本特点：

(1)军事与民事领域,平时与战时、战场内与战场外均可进行;

(2)在战争中发挥主导作用的能量形式有了突破性转变;

(3)战争手段创新,进行战争的手段主要是技术高密集的信息化装备和数字化部队。

(4)攻击的目标,主要是敌方的信息系统和认识体系等要害。

2. 狭义信息对抗

狭义信息对抗指在情报支援下,综合运用军事欺骗、作战保密、心理战、电子战和实体摧毁等手段,攻击包括人员在内的整个敌信息系统,破坏信息流,以影响、削弱和摧毁敌指挥控制能力,同时保护己方的指挥控制能力免遭敌类似行动的影响。

从狭义的军事领域来说,信息对抗的内容包括:

(1)使用信息技术手段进行的探测、侦察、引导、指挥、控制、通信、信息处理、伪装欺骗和打击杀伤等作战行动。

(2)对敌方上述活动所进行的电子对抗侦察、干扰、破坏和反利用而采取的对抗措施等。军事领域的信息对抗是在电子对抗的基础上发展起来的,其主体仍然是电子对抗,信息对抗是电子对抗的发展和升华。

1.2 信息对抗的基本样式

1.2.1 指挥控制战

指挥控制战是在军事领域内实施信息对抗的最主要形式。

美国在1996年3月31日颁发的《3210、03号参联主席指令》给指挥控制战下的定义是:"在情报的支援下,综合利用作战保密、军事欺骗、心理战、电子战和物理摧毁等手段,在使己方指挥控制能力得到严密防护的同时,使敌方得不到信息,并影响、削弱或摧毁敌指挥控制能力"。

指挥控制战的实质是通过对敌方信息系统实施物理或电子(包括有害软件程序)攻击,来阻隔敌军部队与指挥员的联系,破坏其指挥能力,干扰指挥员决策。

在实施指挥控制战中,选择攻击敌人部队"技术结合部",可能更有效地破坏其指挥控制系统;选择攻击敌人最高指挥层,可使敌人受到更大的伤害。

1.2.2 电子战

电子战是信息对抗的重要组成部分,也是实施信息对抗的重要作战样式。电子战包括电子进攻、电子防护和电子支援三部分。

电子战是在雷达、声呐、通信、导航等无线电及光电领域内实施的电子及光电侦察与反侦察、干扰与反干扰、欺骗与反欺骗(目标识别)等方面的斗争。

1.2.3 情报战

实施信息对抗时,极其重要的是要能得到情报信息。人造卫星技术和成像系统的进步,使侦察能力和监视能力有了很大的提高。

使用红外线、紫外线、地表震动、声像、嗅觉等探测装置,采集和利用数据融合技术,可及时

向用户提供可靠的信息。未来，由于小型高效计算机和传感器的使用，各国将部署更多的战术情报系统。这些情报系统的信息将由部署在太空、空中、近海和陆地上的传感器通过滤除系统和提示系统提供给战场指挥官，以帮助他们打赢信息战。

1.2.4 经济信息战

目前世界各国的经济贸易走向全球化，一个国家想要达到本国利益目标，就要经常有计划有组织地实施“黑客行动”和投机活动。计算机黑客或投机商们利用股票及银行等要害部门的电子信息系统来改变股票市场和银行现金流量来攻击一个国家的经济，或者在网上发出某一敌对国的货币即将贬值的暗示，而引起敌对国金融市场的混乱。

1.2.5 “黑客战”(计算机战)

这是一种崭新的攻击方式，是针对计算机和计算机使用者的，目的是破坏或者利用敌方的信息系统。“黑客战”的主要武器是计算机。它是由熟谙计算机及网络技术的高手，通过软盘、终端、通信网络或者其他方法进入计算机系统，进行情报信息窃取、破坏等恶意活动。“黑客”可以利用一条电话线、一台计算机对敌方信息系统输入有害的软件程序，以瘫痪敌信息系统，或迫使敌方信息系统周期性关闭，另外还可以大量偷窃敌方信息数据。除了向计算机网络注入“病毒”外，还可以向敌方计算机系统注入“微生物”，这种“微生物”能吞噬电子系统，使计算机系统长时间无法运行。

1.2.6 计算机网络战

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。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、瘫痪、控制敌方的商务、政务等民用网络系统。

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。网络战分为两大类，一类是战略网络战，另一类是战场网络战。

战略网络战又有平时和战时两种。平时战略网络战是在双方不发生有火力杀伤破坏的战争情况下，一方对另一方的金融网络信息系统、交通网络信息系统、电力网络信息系统等民用网络信息设施及战略级军事网络信息系统，以计算机病毒、逻辑炸弹、黑客等手段实施的攻击。而战时战略网络战则是在战争状态下，一方对另一方战略级军用和民用网络信息系统的攻击。

战场网络战旨在攻击、破坏、干扰敌军战场信息网络系统和保护己方信息网络系统。其主要方式有：利用敌接受路径和各种“后门”，将病毒送入目标计算机系统；让黑客利用计算机开放结构的缺陷和计算操作程序中的漏洞，使用专门的破译软件，在系统内破译超级用户的口令；将病毒植入计算机芯片，需要时利用无线遥控等手段将其激活；采用各种管理和技术手段，对己方信息网络系统严加防护。当然，战场网络战的作战手段也可用于战略网络战。

早在1991年的海湾战争中，美军就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成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都有增无减。南联盟使用多种计算机病毒，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，北约的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注入南军计算机网络系统，致使南军防空系统陷于瘫痪。

1.2.7 心理战

心理战即运用心理学的原理原则，以人类的心理为战场，有计划地采用各种手段，对人的认知、情感和意志施加影响，在无形中打击敌人的心志，以最小的代价换取最大胜利和利益。通过宣传等方式从精神上瓦解敌方军民斗志或消除敌方宣传所造成的影响的对抗活动。它通常分为政治心理战、经济心理战、外交心理战和文化心理战等。

我国古代的《孙子兵法》很大一部分讲的是心理战，海湾战争以及美英联军攻打伊拉克的战争均成功地使用了心理战。

心理战告诉我们，一个军队的心理被击垮了，那么这个军队肯定会吃败仗。对于我们自己来说，如果我们被自己固有的心理劣势打倒了，我们的人生也一定会是失败的人生。

心理战的目的有 3 个：一是最大限度地争取盟友，孤立对方，置对方于心理弱势和劣势；二是在本民族、本国家内部赢得民心民意，形成同仇敌忾的强大气势；三是以正义之师的形象激励参战人员斗志和士气，造成官兵的战场心理优势。

心理战常用的手段有声音、光线、形象、传媒、宣传、恐吓、威慑、欺骗、诱惑、诡诈、怀柔以及收买等方面。

心理战在国外早不是新词，而且许多国家对内对外、对敌对友、对中立都用。可不是所有的人都对心理战有好感，苏联就认为“心理战是帝国主义的卑鄙、伎俩”，他们研究和运用心理战，但就不叫它心理战，而称之为“意识形态斗争”。最近，随着朝鲜半岛紧张局势的加剧，朝鲜指责韩国使用边境地区高音喇叭搞的广播等煽动宣传为“心理战”，强烈要求拆除并扬言必要时给予摧毁。

第二次世界大战后，心理战的地位得到迅速提升，西方大国将其列为国家安全战略的四大支柱之一，把心理战视作“执行国家安全政策的一种战略手段”。“像台湾就非常重视心理战研究，并有专门的部队，他们叫政战部队。”

“心理战的魅力在于它只要针对对手的心理，遵循科学规律，使用一定的方法，就能玩对手于股掌之间。这种被称为不花钱的战争样式比流血、摧毁更吸引人。许多时候，它能解决兵战解决不了的问题。”

1.3 信息对抗的作用

1.3.1 信息侦察的作用

信息侦察是指利用情报人员及各种侦察设备和器材（如侦察卫星、无人驾驶飞机、雷达以及无线电监视器等），采取全方位探测、全领域侦察和全过程运作，搜索、截获、监视、收集、分析和识别敌方信息，以获取情报的一种手段。

1.3.2 信息进攻的作用

信息进攻由信息干扰和破坏、“硬”武器的打击两部分组成，包括偷窃数据、散播错误信息、否认或拒绝数据存取、从物理上摧毁作为数据存储和分发的部分磁盘及武器平台与设施。

信息进攻是指为削弱、破坏和摧毁敌方获取、处理、传递、使用信息的能力而实施的主动攻击行动。

1.3.3 信息防御的作用

信息防御是指针对敌人可能采取的信息攻击行为，采取强有力的措施保护己方的信息系统和网络，从而保护信息的安全。

信息防御体系由信息保护、电磁防护、物理防护三大方面组成，通过使用病毒检查、嗅探器、密码和网络安全系统抵御敌方的进攻。

严密的信息防御，可保护己方情报不受控制和破坏；保证指挥、控制、通信和计算机、情报网络系统的安全生存，并在通过频谱封锁之后仍能恢复原有功能；保证依赖于信息的武力支援和武器系统能够有效发挥作用。

第2章 信息进攻

信息进攻是指在联合(合同)作战指挥员和信息作战指挥机构的统一指挥下，围绕夺取和保持制信息权，由专业信息进攻力量和非专业力量，采用电子干扰、电子欺骗、计算机病毒攻击和网络渗透、兵力破袭和火力摧毁、心理攻击等综合措施，最大限度地削弱、破坏、瓦解敌方信息系统的主动攻势作战行动。

信息进攻的方法有两类：

一是采用非常规的电子和信息的渗透技术，通过有意地渗透到敌方的信息和控制系统，干扰或欺骗敌人，使之无法或错误地决策。

二是采用常规的精确攻击、实体摧毁，破坏敌方的信息搜集、处理与分发系统、指挥控制系统，削弱其情报搜集和指挥控制能力。

2.1 电子干扰

电子干扰是指为使敌方电子设备和系统丧失或降低效能所采取的电波扰乱措施。电子干扰是电子对抗的重要组成部分，是具有软杀伤特征的电子进攻手段，是电子对抗的组成部分。其目的是削弱或破坏敌方使用各种电子设备和系统执行战场侦察、作战指挥、通信联络和兵器控制与制导的能力，为隐蔽己方企图和提高己方飞机、舰艇的生存能力创造有利条件。

2.1.1 电子干扰的分类

通常按产生的方法、作用的性质和作用的对象进行分类。

(1)按产生的方法可将电子干扰分为有源电子干扰和无源电子干扰两类。

有源电子干扰是用专门的干扰发射机发射或转发某种形式的电磁波，使敌方电子设备和系统工作受到扰乱或破坏。发射的干扰信号载频、功率和调制方式(干扰样式)是根据欲干扰的电子设备的类型、工作频率和技术体制等确定的。

无源电子干扰是用本身不发射电磁波的箔条、反射器或电波吸收体等器材，反射或吸收敌方电子设备发射的电波，使其效能受到削弱或破坏。这类干扰，主要用于干扰雷达、激光测距装置等以接收反射电波来工作的电子设备。

(2)按干扰的作用性质可将电子干扰分为压制性电子干扰和欺骗性电子干扰。

压制性电子干扰是指造成电子设备的接收系统过载、饱和或难以获取有用信号的干扰。

欺骗性电子干扰是以与有用信号相同或相似并含有假信息的信号，使电子设备或操纵人员真假难辨，造成错误的识别和判断的干扰。

(3)按干扰的对象可将电子干扰分为无线电通信干扰、无线电导航干扰、雷达干扰、无线电遥控干扰、无线电遥测干扰、红外干扰、激光干扰等。一些国家还将对声呐等水声电子设备的干扰也列入电子干扰的范围。

2.1.2 电子干扰的实施

电子干扰的实施，通常是按统一的电子对抗计划，同部队战斗行动协调地进行。由于陆、海、空军的作战特点不同，它们对电子干扰的战术应用也不完全相同。在航空兵突防作战中，一般有远距支援电子干扰、近距支援电子干扰、随行电子干扰和自卫电子干扰4种基本战术。

(1)远距支援电子干扰，即用电子干扰飞机在作战地域(敌地面防空武器有效射程)以外，对目标附近的主要电子设备和系统施放大功率综合电子干扰，掩护攻击机群的战斗行动。

(2)近距支援电子干扰，即电子干扰飞机作为攻击机编队的先导机随编队一起突防，并在距目标的一定距离上盘旋飞行，施放电子干扰，掩护攻击飞机执行作战任务。

(3)随行电子干扰，即电子干扰飞机在突防和作战过程中，在编队中施放电子干扰，掩护攻击机群作战。

(4)自卫电子干扰，即作战飞机自身携带电子干扰设备和器材，在执行任务中施放电子干扰，保护自身安全。水面舰艇、潜艇作战，偏重于自卫电子干扰。地面部队作战，不论是进攻还是防御，都强调合理配置电子干扰群，干扰压制敌方通信指挥系统。

2.1.3 电子干扰的发展趋势

电子干扰的发展趋势是：不断探索新的电子干扰技术，发展新型电子干扰设备和器材，扩展干扰的电磁频谱范围和增大干扰有效性，提高干扰过程的自动化程度和对复杂的新型电子设备的干扰能力，以及广泛采用模拟设备研究发展电子干扰战术。

2.2 网络攻击

计算机网络进攻主要用于进攻性信息作战。

计算机网络进攻的主要战略目标是敌方的军事、金融、电力、电信等系统中以计算机网络为核心的信息基础设施。

2.2.1 计算机病毒攻击

计算机及其网络已越来越成为各种军用电子设备和高技术武器系统不可缺少的组成部分。计算机的信息需要存取、复制、传送，病毒作为信息的一种形式可以随之繁殖、感染、破坏，并且，在病毒取得控制权后，它们会主动寻找感染目标，使自己广为流传。

计算机病毒的结构和特点：

1. 计算机病毒的结构

计算机病毒是以计算机系统为环境而存在并发展的，所以，可以认为计算机系统的硬件、软件环境决定了计算机病毒的结构，而这种结构是能够充分利用计算机系统资源进行活动的最合理体现。

病毒的主要组成部分是传染模块和表现及破坏模块，每个模块又有两个程序段：条件判断和实施段。

(1)计算机病毒的传染模块。计算机病毒的传染模块是计算机病毒由一个系统扩散到另一个系统、一个网络传入另一网络、一张软盘传染另一张软盘的唯一途径。它担负计算机病毒

的扩散任务。

(2)计算机病毒的破坏及表现模块。一个特定的计算机病毒的编写,体现了这种病毒设计者的目的,不仅可以通过传染方式粗略地判断病毒设计者的目的,还可以通过计算机病毒的破坏和表现模块来判断计算机病毒设计者是否为恶意攻击者。

2. 计算机病毒的特点

(1)计算机病毒是一种可执行的计算机程序。

(2)计算机病毒的广泛传染性。传染性是衡量一种程序是否为病毒的首要条件。

(3)计算机病毒的潜伏性。计算机病毒潜伏性是指它具有依附于其他媒体而寄生的能力。

(4)计算机病毒的可触发性。计算机病毒一般都有一个触发条件,如在一定的条件下可激活一个病毒的传染机制使之进行传染。

(5)计算机病毒的破坏性。

(6)计算机病毒的针对性。现在世界上出现的计算机病毒,并不是对所有计算机系统都进行传染。

3. 计算机病毒的分类

计算机病毒种类有很多,但根据其性质、功能和造成的危害,大致可分为 6 种类型。

(1)定时炸弹型。这种病毒进入敌方计算机系统后,并不立即影响敌方计算机系统的正常工作,等到预定时间和特定的事件发生后,便突然被触发,发挥其破坏作用,毁坏计算机系统内的有关数据或破坏系统的正常运行,其特点是隐蔽性好。

(2)暗杀型。它是专门用来销毁敌方计算机系统内的某种特定文件和数据,并且不留任何痕迹。

(3)强制隔离型。这种病毒能自动地将计算机系统关闭,中断计算机系统的工作。迫使敌方的信息系统陷入瘫痪,使其无法发挥其应有的作用和作战效能。

(4)超载型或复制型。这种病毒进入敌方信息系统中的计算机系统后,便可以大量复制,大量占据计算机系统内的存储器,覆盖其作战数据和文件,使计算机系统因其存储器超载而无法工作。

(5)间谍型。这种病毒能按攻击者的要求,自动寻找所指定的数据、信息和文件,并将它们转发到指定的地点。

(6)矫令型。这种病毒可以将敌方下达的命令接收下来,然后增加错误指令再传送给敌方,扰乱敌方的行动。

4. 计算机病毒攻击的对象及方法

计算机病毒攻击的主要对象是敌方的各种信息系统,如指挥控制与通信系统、计算机网络系统、雷达情报网络系统、各种传感器等,以及各种武器控制系统,如现代飞机、舰艇、坦克、导弹等的自动驾驶、火控和制导系统,这些系统都是以计算机为核心的。

这些信息系统大致分为三类:

(1)全封闭型系统。这类系统一般是由专用单机或专用计算机局域网络组成的,它们与外界无任何数据、程序、指令的通信联系。

(2)有线与无线兼有的半封闭式系统。这类系统一般是带有无线链路的区域网络,它们与外界无任何信息联系,只是在本网络系统内存在信息流动(网络通信链路是由有线和无线两种方式组成的)。