可下载教学资料

http://www.tup.tsinghua.edu.cn

高等学校教材

计算机科学与技术

信息对抗与网络安全

贺雪晨 陈林玲 赵 琰 编著

清华大学出版社

高等学校教材

计算机科学与技术

信息对抗与网络安全

贺雪晨 陈林玲 赵 琰 编著

清华大学出版社
北京

内 容 简 介

本书主要介绍信息对抗与网络安全的基本概念、密码技术、通信保密技术、计算机网络安全技术和日常上网的安全防范等内容。在讲述密码技术时，融入了基于生物特征的密码技术、数据库加密技术、光盘加密技术等内容，并结合实例实现文件的加密与破解；在通信保密技术中，包括了信息隐藏技术、无线通信保密技术、数字水印技术等新技术；在讲述计算机网络安全技术和日常上网的安全防范时，不过多讲述原理，而是结合常见的安全问题，使读者能够使用各种防范手段，保护自己的系统。

本书可作为计算机类、电子信息类、通信类等专业相关课程的教材，也可作为从事网络安全、计算机安全和信息安全领域相关人员的技术参考书。

图书在版编目(CIP)数据

信息对抗与网络安全/贺雪晨，陈林玲，赵琰编著. —北京：清华大学出版社，2006.7

(高等学校教材·计算机科学与技术)

ISBN 7-302-12879-0

Ⅰ. 信…　Ⅱ. ①贺…　②陈…　③赵…　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(2006)第 036788 号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦

http://www.tup.com.cn　　**邮　　编**：100084

社 总 机：010-62770175　　**客户服务**：010-62776969

责任编辑：魏江江

印 刷 者：北京季蜂印刷有限公司

装 订 者：三河市李旗庄少明装订厂

发 行 者：新华书店总店北京发行所

开　　本：185×260　**印张**：16.5　**字数**：408 千字

版　　次：2006 年 7 月第 1 版　2006 年 7 月第1 次印刷

书　　号：ISBN 7-302-12879-0/TP·8187

印　　数：1～4000

定　　价：21.00 元

编审委员会成员

（按地区排序）

高等学校教材·计算机科学与技术

清华大学	周立柱　教授
	覃　征　教授
	王建民　教授
	刘　强　副教授
	冯建华　副教授
北京大学	杨冬青　教授
	陈　钟　教授
	陈立军　副教授
北京航空航天大学	马殿富　教授
	吴超英　副教授
	姚淑珍　教授
中国人民大学	王　珊　教授
	孟小峰　教授
	陈　红　教授
北京师范大学	周明全　教授
北京交通大学	阮秋琦　教授
北京信息工程学院	孟庆昌　教授
北京科技大学	杨炳儒　教授
石油大学	陈　明　教授
天津大学	艾德才　教授
复旦大学	吴立德　教授
	吴百锋　教授
	杨卫东　副教授
华东理工大学	邵志清　教授
华东师范大学	杨宗源　教授
	应吉康　教授
东华大学	乐嘉锦　教授
上海第二工业大学	蒋川群　教授
浙江大学	吴朝晖　教授
	李善平　教授
南京大学	骆　斌　教授
南京航空航天大学	秦小麟　教授
南京理工大学	张功萱　教授

南京邮电学院	朱秀昌	教授
苏州大学	龚声蓉	教授
江苏大学	宋余庆	教授
武汉大学	何炎祥	教授
华中科技大学	刘乐善	教授
中南财经政法大学	刘腾红	教授
华中师范大学	王林平	副教授
	魏开平	教授
武汉理工大学	李中年	教授
国防科技大学	赵克佳	教授
	肖　侬	副教授
中南大学	陈松乔	教授
湖南大学	林亚平	教授
	邹北骥	教授
西安交通大学	沈钧毅	教授
	齐　勇	教授
长安大学	巨永峰	教授
西安石油学院	方　明	教授
西安邮电学院	陈莉君	副教授
哈尔滨工业大学	郭茂祖	教授
吉林大学	徐一平	教授
	毕　强	教授
长春工程学院	沙胜贤	教授
山东大学	孟祥旭	教授
	郝兴伟	教授
山东科技大学	郑永果	教授
中山大学	潘小轰	教授
厦门大学	冯少荣	教授
福州大学	林世平	副教授
云南大学	刘惟一	教授
重庆邮电学院	王国胤	教授
西南交通大学	杨　燕	副教授

出版说明

改革开放以来，特别是党的十五大以来，我国教育事业取得了举世瞩目的辉煌成就，高等教育实现了历史性的跨越，已由精英教育阶段进入国际公认的大众化教育阶段。在质量不断提高的基础上，高等教育规模取得如此快速的发展，创造了世界教育发展史上的奇迹。当前，教育工作既面临着千载难逢的良好机遇，同时也面临着前所未有的严峻挑战。社会不断增长的高等教育需求同教育供给特别是优质教育供给不足的矛盾，是现阶段教育发展面临的基本矛盾。

教育部一直十分重视高等教育质量工作。2001 年 8 月，教育部下发了《关于加强高等学校本科教学工作，提高教学质量的若干意见》，提出了十二条加强本科教学工作提高教学质量的措施和意见。2003 年 6 月和 2004 年 2 月，教育部分别下发了《关于启动高等学校教学质量与教学改革工程精品课程建设工作的通知》和《教育部实施精品课程建设提高高校教学质量和人才培养质量》文件，指出“高等学校教学质量和教学改革工程”是教育部正在制定的《2003—2007 年教育振兴行动计划》的重要组成部分，精品课程建设是“质量工程”的重要内容之一。教育部计划用五年时间（2003—2007 年）建设 1500 门国家级精品课程，利用现代化的教育信息技术手段将精品课程的相关内容上网并免费开放，以实现优质教学资源共享，提高高等学校教学质量和人才培养质量。

为了深入贯彻落实教育部《关于加强高等学校本科教学工作，提高教学质量的若干意见》精神，紧密配合教育部已经启动的“高等学校教学质量与教学改革工程精品课程建设工作”，在有关专家、教授的倡议和有关部门的大力支持下，我们组织并成立了“清华大学出版社教材编审委员会”（以下简称“编委会”），旨在配合教育部制定精品课程教材的出版规划，讨论并实施精品课程教材的编写与出版工作。“编委会”成员皆来自全国各类高等学校教学与科研第一线的骨干教师，其中许多教师为各校相关院、系主管教学的院长或系主任。

按照教育部的要求，“编委会”一致认为，精品课程的建设工作从开始就要坚持高标准、严要求，处于一个比较高的起点上；精品课程教材应该能够反映各高校教学改革与课程建设的需要，要有特色风格、有创新性（新体系、新内容、新手段、新思路，教材的内容体系有较高的科学创新、技术创新和理念创新的含量）、先进性（对原有的学科体系有实质性的改革和发展，顺应并符合新世纪教学发展的规律，代表并引领课程发展的趋势和方向）、示范性（教材所体现的课程体系具有较广泛的辐射性和示范性）和一定的前瞻

性。教材由个人申报或各校推荐(通过所在高校的“编委会”成员推荐),经“编委会”认真评审,最后由清华大学出版社审定出版。

目前,针对计算机类和电子信息类相关专业成立了两个“编委会”,即“清华大学出版社计算机教材编审委员会”和“清华大学出版社电子信息教材编审委员会”。首批推出的特色精品教材包括:

(1) 高等学校教材·计算机应用——高等学校各类专业,特别是非计算机专业的计算机应用类教材。

(2) 高等学校教材·计算机科学与技术——高等学校计算机相关专业的教材。

(3) 高等学校教材·电子信息——高等学校电子信息相关专业的教材。

(4) 高等学校教材·软件工程——高等学校软件工程相关专业的教材。

(5) 高等学校教材·信息管理与信息系统。

清华大学出版社经过近 20 年的努力,在教材尤其是计算机和电子信息类专业教材出版方面树立了权威品牌,为我国的高等教育事业做出了重要贡献。清华版教材经过 20 多年的精雕细刻,形成了技术准确、内容严谨的独特风格,这种风格将延续并反映在特色精品教材的建设中。

清华大学出版社教材编审委员会

E-mail: dingl@tup.tsinghua.edu.cn

前言

从信息技术发展的历程来看，信息安全已由20世纪80年代的被动保密发展到20世纪90年代的主动保护，继而发展到21世纪初的信息安全全面保障。

信息战的出现是信息社会中信息技术高度进步的必然产物，是信息技术发展和它在军事领域中广泛应用的结果。信息对抗的手段越来越多，范围越来越大，信息优势在战争中的主导作用越来越明显。信息战的最终目标是信息系统赖于生存和运转的基础——计算机网络。

本书从信息时代的战争引出电子战、网络战的概念，并通过它们介绍相关的通信保密技术与网络安全技术。在讲述密码技术、通信保密技术时，结合一些新知识，如量子密码、信息隐藏、无线安全等内容，使学生对相关的前沿知识有所了解。在讲述计算机网络安全技术、日常上网的安全防范时，注意理论联系实际，结合一些常用计算机攻防软件的使用，使读者能够将所学的知识应用到日常生活中。本书试图使读者从宏观上对信息对抗和网络安全有一个比较全面的了解，从微观上掌握如何保护信息安全、防范攻击的具体方法。

全书共5章，介绍了信息对抗与网络安全的基本概念；古典密码学与现代密码学、文件加密与破解、数据库加密和光盘加密；通信保密技术和信息隐藏技术；计算机安全问题、病毒和木马、漏洞与扫描、网络监听的检测和防范、拒绝服务攻击和共享攻击、防火墙与入侵检测技术、数据备份与急救；电子邮件、IE、网络通信软件的攻击与防护。

信息安全技术是一门实践性很强、发展很快的学科，在教学过程中可以通过各种方法提高同学的实际动手能力和自学能力，编者在这方面做了一些尝试，有兴趣的读者可以通过编者的Blog网站 http://hein.blogone.net 一起探讨。此外，在Blog网站中还提供了上课使用的PPT讲稿供各位教师参考。

本书第1～4章由贺雪晨编写、第5章由陈林玲、赵琰编写，全书由贺雪晨统稿。

在清华大学网站上提供的CAI课件由张科挺等同学制作，在此一并表示感谢。

由于编者的水平和经验有限，书中的缺点和疏漏之处在所难免，恳请有关专家和读者予以批评指正。

编　者

2006年4月

目录

第1章

信息对抗与网络安全概述

信息已成为支撑国家政治、经济、军事、科技的重要战略资源，信息安全是保护信息资源的基础，没有信息安全，就没有政治、军事和经济安全，就没有完整意义上的国家安全。

信息安全起源于文字和话音的保密，是一门涉及计算机科学、网络技术、物理学、管理科学、通信技术、密码技术、信息安全技术、应用数学、数论、信息论乃至生物学等多种学科的边缘性综合学科。

从信息技术发展的历程来看，信息安全已由20世纪80年代的被动保密发展到20世纪90年代的主动保护，继而发展到21世纪初的信息安全全面保障。

在20世纪80年代前，信息安全的唯一属性就是信息的保密性；20世纪80年代期间，扩大到了信息的完整性、可用性、可审计性和可认证性；到了20世纪90年代，其内涵已扩展到了信息的可控性。

信息战的出现是信息社会中信息技术高度进步的必然产物，是信息技术发展及其在军事领域中广泛应用的结果。信息对抗的手段越来越多，范围越来越大，信息优势在战争中的主导作用越来越明显。人们开始像重视“制海权”、“制空权”一样重视“制信息权”，有意识地将各种信息技术和武器装备综合地、系统地加以运用，展开全面的信息对抗，使得信息对抗由一种辅助性的作战形式上升为关键性的、甚至是决定性的作战形式，从而形成了现在的信息战理论。

计算机网络的出现和发展，特别是随着Internet日新月异的迅猛发展，使人类对于信息的开发和应用达到了一个空前的高度。先进的计算机系统已把军队乃至整个社会联系在一起，在未来网络世界里，每个芯片都是一种潜在的武器，每台计算机都有可能成为一个有效的作战单元，一位平民百姓可能编制出实施信息战的计划，并付诸实施。任何社会团体或个人，只要掌握了计算机通信技术，只要拥有一台计算机和入网线路，就可以攻击装有芯片的系统和接入网络的装备，利用网络来发动一场特殊战争。

从目前的技术看，计算机网络具有很大的脆弱性，极易被黑客入侵。如果敌对国运用网络犯罪手段进行经济干扰和破坏，足以使当事国经济崩溃。一些国家正在开发研制的“超级病毒”和电磁脉冲装置，就可以对敌国的银行、证券交易、空中交通管制、电话、电视网、发电站、电力网系统进行打击，造成国家经济瘫痪。

随着科学技术的发展和社会生产结构的变化，国家安全赖于存在的基础也发生了变化，从原来的国土、资源、军队等有形的东西为主，转变为以信息和知识等无形的东西为主，使信

息安全成为国家安全的基础。信息安全不能得到保障，国家就会经济紊乱、政治失稳、军事失效、文化迷失、技术落后，进而影响到国家在国际上的地位和形象。

1.1 信息时代的战争

信息战是以计算机为主要武器，以覆盖全球的计算机网络为主战场，以攻击敌方的信息系统为主要手段，以数字化战场为依托，以信息化部队为基本作战力量，运用各种信息武器和信息系统，围绕着信息的获取、控制和使用而展开的一种新型独特的作战形式。

信息战的目的是夺取信息优势，其核心是保护己方的信息系统，攻击敌方的信息系统，是全方位、攻防兼有的信息对抗行动。信息战的最终目标是信息系统赖于生存和运转的基础——计算机网络。

信息战的本质是围绕争夺信息控制权的信息对抗，计算机病毒可以作为一种“以毒攻毒”的信息对抗手段。

美国的权威“智囊团”——兰德公司，对未来信息战曾作过这样一段假想：

2010 年的一天，因遭到信息攻击，美国部分军用和民用电话系统中断；因为信息误导，马里兰州一列时速 320 公里的客车与一列载货列车相撞；一家原油提炼厂遭到计算机破坏并引起爆炸和火灾；由于病毒感染，五角大楼与世界各地军事基地大部分失去联系，命令无法下达；装备、食品、油料配给的计划表数据错误，部队调遣无法正常执行；战场预警指挥机的屏幕出现无名斑点，无法实施指挥；银行计算机出现混乱，账目被任意修改，人们纷纷从银行提出全部存款，金融业务被迫停止；纽约和伦敦的股票市场指数狂跌；政府电视台新闻播音员的面孔突然被替换成了敌方领导人的面孔，并且号召军队发动推翻现政府的政变；美国有线电视网的电视信号中断，美国出现全国性的大恐慌。

这只是一个虚拟的故事，但从中对信息战的看法可见一斑。区区几条计算机程序，就可能造成整个国家的混乱和恐慌，信息杀伤已成为新世纪人类社会所面临的巨大威胁。

1.1.1 信息战的主要内容

信息战的内容涉及在信息领域中战胜被攻击对象的所有行动，其对抗的双方利用信息技术和信息武器，在整个信息战的各个层面、各个环节针对对方的信息目标实施有效的攻击或反攻击。

信息战的主要内容包括信息保障、信息防护和信息对抗。

- 信息保障：掌握敌我双方准确、可靠和完整的信息，及时捕获信息优势，为信息战提供切实可行的依据。
- 信息防护：在敌方开始对我方实施信息攻击时，为确保我方的信息系统免遭破坏而采取的一系列防御性措施，保护我方的信息优势不会受到损害。
- 信息对抗：打击并摧毁敌方的信息保障和信息保护的一整套措施。

其中信息保障是关键，它用于确保信息防护措施和信息对抗措施的有效运作。

1.1.2　信息战的主要形式

信息战有多种分类方法，按作战性质可以分为信息进攻战和信息防御战。

1. 信息进攻战

信息进攻战由信息侦察、信息干扰和破坏、“硬”武器的打击三部分组成。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。

2. 信息防御战

信息防御战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。

信息防御战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。

3. 信息进攻战与信息防御战的关系

在信息化战争中，信息进攻手段将异彩纷呈，信息防御虽然会水涨船高，但只防不攻，很难从根本上取得信息优势。因此，严密的信息防御也必须是积极主动的攻势防御，只有将信息进攻与信息防御有机结合起来，互相支援配合，才能从根本上夺取信息优势。

要打赢一场信息战，关键在于如何有效地保障自身信息系统的安全性。因此，在信息战中，防御占 9，进攻占 1。

1.1.3　信息战的主要武器

按照作战性质划分，信息战的主要武器分为进攻性信息战武器和防御性信息战武器两大类。

进攻性信息战武器和技术主要有：计算机病毒、蠕虫、特洛伊木马、逻辑炸弹、芯片陷阱、纳米机器人、芯片微生物、电子干扰、高能定向武器、电磁脉冲炸弹、信息欺骗和密码破译等。

防御性信息战武器和技术主要有：密码技术、计算机病毒检测与清除技术、网络防火墙、信息设施防护、电磁屏蔽技术、防窃听技术、大型数据库安全技术、访问控制、审计跟踪、信息隐蔽技术、入侵检测系统和计算机取证技术等。

1. 软件武器

软件武器主要包括计算机病毒、逻辑炸弹和特洛伊木马。

1999 年以来，全球爆发的梅莉莎、CIH 病毒等，使世界各地不少计算机系统遭到破坏，经济损失巨大，这实际上就是信息战的一种形式——计算机病毒战，而这些武器的生产都是在民间进行的，至少名义上是，目前还没有哪一个国家敢承认自己是这些病毒的制造者。

例如，A 国把具有神经网络细胞式的自我变异功能的病毒程序注入 B 国通信网接口，在 A 国正式进攻前，B 国的情报系统有一半的计算机遭到破坏，甚至连战斗机上的计算机也感染了该病毒。

2. 芯片陷阱

对计算机芯片进行修改，使芯片有优先接受特定指令的能力，只要卫星系统发出命令，使用这些芯片的信息系统就会发生逻辑错误甚至崩溃。

例如，A 国派特工人员偷偷用一套带有计算机病毒的同类芯片换下了 B 国购买的计算机中的芯片。战争爆发后，A 国用指令激活了 B 国防空系统计算机内的计算机病毒，计算机病毒通过打印机侵入防空系统的计算机中，使部分防空系统的计算机陷于瘫痪。

3. 纳米机器人和芯片微生物

纳米机器人是一些外形类似黄蜂和苍蝇，会飞、会爬的纳米系统，可以被投放到敌人信息系统或武器系统附近，通过缝隙或插口钻进计算机，破坏电子线路。

芯片微生物是经过特殊培育的，能毁坏计算机硬件的一种细菌，它通过某种途径进入计算机，能像吞噬垃圾和石油废料的微生物一样，噬食硅集成电路，对计算机造成破坏。

4. 高能定向武器

高能定向武器对电子目标发射高能无线电信号，使其功能失灵，如高能射频枪。

高能射频枪是一种无线电发射机，可以对一个电子目标发射大功率无线电信号，使其对外部磁场敏感的电子线路出现电路超载，发生故障，从而使遭到攻击的信息系统无法工作，甚至使整个网络系统失灵。

5. 电磁脉冲炸弹

电磁脉冲炸弹是另一种摧毁性武器，能量比高能射频枪大，以光速发射出去的电磁脉冲，使受攻击的计算机内部元件熔化。

电磁脉冲炸弹可以有效地破坏和干扰敌方的计算机及网络等电子通信设备，它产生的超强电磁场，足以破坏任何计算机设备。

电磁轰炸是战争采用的手段之一，通过电磁干扰，使得对方的防空系统陷于瘫痪状态，无法积极有效应战，处于被动挨炸的地步。

1.1.4 信息战的种类

信息战包括指挥与控制战、情报战、电子战、网络战、心理战、空间控制战、黑客战、虚拟战、经济战等。

电子战部队利用通信对抗、雷达对抗、光电对抗、空间对抗等各种电子战手段，对敌人的战场指挥系统和武器控制系统进行强烈的干扰。使敌人变成聋子、瞎子和傻子，全面丧失战斗力。

网络战部队利用有线注入、无线注入等各种手段，将病毒植入敌方的网络之中。不但能