21世纪 高等学校信息安全专业规划教材

上海市教学成果二等奖

上海市重点课程配套用书

信息对抗与网络安全（第2版）

贺雪晨 主编

清华大学出版社

上海市重点课程配套教材.上海市教学成果二等奖组成部分
21世纪高等学校信息安全专业规划教材

信息对抗与网络安全

（第2版）

贺雪晨　主编

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，并结合实例介绍了文件的加密与破解；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。

本书是2006年上海市重点课程“信息对抗与安全”的建设成果之一，也是2009年上海市教学成果二等奖“基于身份认证平台的电子信息人才培养模式的创新与实践”的重要组成部分。

本书可作为高等学校计算机类、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/贺雪晨主编. —2版. —北京：清华大学出版社，2010.5
(21世纪高等学校信息安全专业规划教材)
ISBN 978-7-302-22051-0

Ⅰ. ①信… Ⅱ. ①贺… Ⅲ. ①计算机网络—安全技术—高等学校—教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2010)第026050号

责任编辑：魏江江　顾　冰
责任校对：白　蕾
责任印制：杨　艳
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦A座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：北京市清华园胶印厂
经　　销：全国新华书店
开　　本：185×260　**印　张**：19　**字　数**：455千字
版　　次：2010年5月第2版　　**印　　次**：2010年5月第1次印刷
印　　数：1～3000
定　　价：29.00元

产品编号：032932-01

出版说明

由于网络应用越来越普及，信息化的社会已经呈现出越来越广阔的前景，可以肯定地说，在未来的社会中电子支付、电子银行、电子政务以及多方面的网络信息服务将深入到人类生活的方方面面。同时，随之面临的信息安全问题也日益突出，非法访问、信息窃取、甚至信息犯罪等恶意行为导致信息的严重不安全。信息安全问题已由原来的军事国防领域扩展到了整个社会，因此社会各界对信息安全人才有强烈的需求。

信息安全本科专业是2000年以来结合我国特色开设的新的本科专业，是计算机、通信、数学等领域的交叉学科，主要研究确保信息安全的科学和技术。自专业创办以来，各个高校在课程设置和教材研究上一直处于探索阶段。但各高校由于本身专业设置上来自于不同的学科，如计算机、通信和数学等，在课程设置上也没有统一的指导规范，在课程内容、深浅程度和课程衔接上，存在模糊不清、内容重叠、知识覆盖不全面等现象。因此，根据信息安全类专业知识体系所覆盖的知识点，系统地研究目前信息安全专业教学所涉及的核心技术的原理、实践及其应用，合理规划信息安全专业的核心课程，在此基础上提出适合我国信息安全专业教学和人才培养的核心课程的内容框架和知识体系，并在此基础上设计新的教学模式和教学方法，对进一步提高国内信息安全专业的教学水平和质量具有重要的意义。

为了进一步提高国内信息安全专业课程的教学水平和质量，培养适应社会经济发展需要的、兼具研究能力和工程能力的高质量专业技术人才。在教育部相关教学指导委员会专家的指导和建议下，清华大学出版社与国内多所重点大学共同对我国信息安全人才培养的课程框架和知识体系，以及实践教学内容进行了深入的研究，并在该基础上形成了“信息安全人才需求与专业知识体系、课程体系的研究”等研究报告。

本系列教材是在课程体系的研究基础上总结、完善而成，力求充分体现科学性、先进性、工程性，突出专业核心课程的教材，兼顾具有专业教学特点的相关基础课程教材，探索具有发展潜力的选修课程教材，满足高校多层次教学的需要。

本系列教材在规划过程中体现了如下一些基本组织原则和特点。

(1) 反映信息安全学科的发展和专业教育的改革，适应社会对信息安全人才的培养需求，教材内容坚持基本理论的扎实和清晰，反映基本理论和原理的综合应用，在其基础上强调工程实践环节，并及时反映教学体系的调整和教学内容的更新。

(2) 反映教学需要，促进教学发展。教材要适应多样化的教学需要，正确把握教学内容和课程体系的改革方向，在选择教材内容和编写体系时注意体现素质教育、创新能

力与实践能力的培养,为学生知识、能力、素质协调发展创造条件。

(3) 实施精品战略,突出重点。规划教材建设把重点放在专业核心(基础)课程的教材建设上;特别注意选择并安排一部分原来基础比较好的优秀教材或讲义修订再版,逐步形成精品教材;提倡并鼓励编写体现工程型和应用型的专业教学内容和课程体系改革成果的教材。

(4) 支持一纲多本,合理配套。专业核心课和相关基础课的教材要配套,同一门课程可以有多本具有各自内容特点的教材。处理好教材统一性与多样化,基本教材与辅助教材、教学参考书,文字教材与软件教材的关系,实现教材系列资源的配套。

(5) 依靠专家,择优落实。在制定教材规划时依靠各课程专家在调查研究本课程教材建设现状的基础上提出规划选题。在落实主编人选时,要引入竞争机制,通过申报、评审确定主编。书稿完成后认真实行审稿程序,确保出书质量。

繁荣教材出版事业,提高教材质量的关键是教师。建立一支高水平的、以老带新的教材编写队伍才能保证教材的编写质量,希望有志于教材建设的教师能够加入到我们的编写队伍中来。

21世纪高等学校信息安全专业规划教材
联系人:魏江江 weijj@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世纪的信息全面保障。

本书从信息时代的战争引出电子战、网络战的概念，进而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，使读者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，使学生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。

第1章介绍信息对抗与网络安全的基本概念；第2章介绍密码学的基本概念以及如何使用密码技术实现加密与破解；第3章介绍数据、语音和图像的通信保密技术；第4章介绍如何防范黑客使用病毒、木马、扫描、嗅探、攻击进行入侵，如何使用防火墙、入侵检测技术、数据备份和数据急救进行安全保障；第5章介绍电子邮件、网络浏览、网络聊天和网络购物的安全防范。

根据几十所高校使用第1版教材的反馈情况以及信息安全技术不断发展的需要，在第2版中进行了如下修订：第4章新增了ARP欺骗攻击、数据库攻击、防火墙的发展趋势、Ghost备份等内容；第5章新增了反垃圾邮件、“网络钓鱼”及其防范、浏览器安全、网络购物安全防范等内容；按照信息安全技术的发展对部分文字进行了修改，新增了部分案例，对原有案例中涉及的软件采用中文版或最新版进行了改写。

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学生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.blogcn.com 或 http://blog.sina.com.cn/heinhe 一起探讨。此外，在精品课程网站 http://jpkc.shiep.edu.cn/?courseid=20065305 上提供了教学大纲、电子教案、模拟试卷、习题答案、实践教学、视频课件、交互课件、素材下载等模块供各位教师参考。

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批评指正。

编　者

2010年1月

目　录

第 1 章　信息对抗与网络安全概述 …… 1
1.1　信息时代的战争 …… 1
1.1.1　信息战的主要内容 …… 2
1.1.2　信息战的主要形式 …… 2
1.1.3　信息战的主要武器 …… 3
1.1.4　信息战的种类 …… 4
1.2　电子战 …… 4
1.2.1　电子战的历史 …… 5
1.2.2　电子战的攻防 …… 6
1.2.3　电子战的发展 …… 6
1.3　网络战 …… 7
1.3.1　计算机病毒战 …… 7
1.3.2　黑客战 …… 8
1.4　心理战 …… 8
1.5　情报战 …… 9
1.6　理想战争模式 …… 10
习题 …… 10
第 2 章　密码技术 …… 11
2.1　基本概念 …… 11
2.1.1　明文、密文与密钥 …… 11
2.1.2　解密与密码分析 …… 12
2.1.3　密码体制 …… 12
2.1.4　加密方法 …… 13
2.2　古典密码学与近代密码学 …… 14
2.2.1　古典密码体制 …… 14
2.2.2　近代密码体制 …… 18
2.3　现代密码学 …… 19
2.3.1　秘密密钥密码体制与公开密钥密码体制 …… 20
2.3.2　分组密码与序列密码 …… 21

2.3.3 DES算法 …… 23
2.3.4 认证与数字签名 …… 24
2.3.5 密钥管理 …… 36
2.3.6 密码学新技术 …… 37
2.4 文件加密与破解 …… 43
2.4.1 压缩文件的加密与破解 …… 43
2.4.2 Office文件的加密与破解 …… 46
2.4.3 其他文件的加密与破解 …… 50
2.4.4 文件夹加密 …… 56
2.4.5 Windows XP加密文件系统 …… 61
2.4.6 系统加密 …… 64
2.4.7 密码的保存 …… 67
2.4.8 密码强度的检测 …… 71
2.5 数据库加密 …… 72
2.5.1 数据库加密的方法 …… 72
2.5.2 数据库加密的实现 …… 73
2.5.3 数据库加密系统的结构 …… 73
2.6 光盘加密 …… 74
2.6.1 软加密 …… 74
2.6.2 硬加密 …… 79
2.6.3 物理结构加密技术 …… 79
习题 …… 80
第3章 通信保密技术 …… 81
3.1 保密通信的基本要求 …… 81
3.2 数据保密通信 …… 82
3.2.1 网络通信保密技术 …… 82
3.2.2 信息隐藏技术 …… 83
3.3 语音保密通信 …… 89
3.3.1 窃听与反窃听 …… 89
3.3.2 模拟话音保密技术与数字话音保密技术 …… 96
3.3.3 扩展频谱与无线通信保密技术 …… 98
3.4 图像保密通信 …… 100
3.4.1 数字图像置乱、分存、隐藏技术 …… 100
3.4.2 数字水印技术 …… 101
3.4.3 视频加密技术 …… 105
习题 …… 109
第4章 计算机网络安全技术 …… 110
4.1 计算机安全问题 …… 110
4.1.1 计算机犯罪类型 …… 110

4.1.2　计算机犯罪手段…… 111
4.1.3　计算机安全保护…… 111
4.1.4　一般安全问题…… 113
4.1.5　安全威胁…… 114
4.1.6　黑客入侵攻击…… 116
4.1.7　常用黑客软件及其分类…… 117
4.2　计算机病毒 …… 118
4.2.1　计算机病毒的定义…… 119
4.2.2　病毒的特点…… 119
4.2.3　病毒的分类…… 120
4.2.4　计算机病毒在磁盘中的存储…… 121
4.2.5　计算机病毒的构成…… 122
4.2.6　计算机病毒的传染机制…… 123
4.2.7　计算机病毒的表现和破坏…… 125
4.2.8　计算机病毒的检测与防范…… 128
4.2.9　计算机病毒的发展历史及趋势…… 133
4.3　木马 …… 144
4.3.1　木马原理…… 144
4.3.2　木马实例——冰河…… 149
4.3.3　木马的检测…… 155
4.3.4　木马的清除…… 164
4.3.5　木马的预防…… 164
4.4　扫描器 …… 167
4.4.1　漏洞概述…… 167
4.4.2　扫描器原理…… 173
4.4.3　漏洞扫描器 X-Scan …… 176
4.4.4　扫描技术的发展趋势…… 179
4.4.5　反扫描技术…… 179
4.5　嗅探器 …… 191
4.5.1　网络监听原理…… 191
4.5.2　监听工具“艾菲”网页侦探…… 192
4.5.3　网络监听的检测和防范…… 195
4.6　拒绝服务攻击 …… 196
4.6.1　DoS 攻击类型…… 196
4.6.2　DoS 攻击手段…… 197
4.6.3　DoS 攻击的防范…… 201
4.7　共享攻击 …… 202
4.7.1　共享攻击的实现…… 202
4.7.2　禁用共享…… 203

4.8 ARP欺骗攻击 …… 205
4.8.1 ARP欺骗攻击原理 …… 206
4.8.2 ARP攻击防护 …… 207
4.9 数据库攻击 …… 207
4.9.1 SQL注入攻击 …… 207
4.9.2 暴库攻击 …… 210
4.10 防火墙 …… 212
4.10.1 基本概念 …… 212
4.10.2 防火墙技术 …… 214
4.10.3 包过滤防火墙 …… 217
4.10.4 屏蔽主机防火墙 …… 219
4.10.5 屏蔽子网防火墙 …… 220
4.10.6 防火墙的发展趋势 …… 221
4.10.7 使用天网防火墙保护终端网络安全 …… 222
4.11 入侵检测技术 …… 225
4.11.1 基本概念 …… 225
4.11.2 基于主机的入侵检测系统 …… 228
4.11.3 基于网络的入侵检测系统 …… 229
4.11.4 现有入侵检测技术的局限性 …… 230
4.11.5 Windows 2000/XP简单安全入侵检测 …… 231
4.11.6 单机版入侵检测系统Nuzzler Intrusion Detection …… 233
4.12 数据备份 …… 237
4.12.1 数据备份与恢复 …… 237
4.12.2 Windows XP系统还原功能 …… 243
4.12.3 Ghost备份 …… 246
4.13 数据急救 …… 250
4.13.1 数据急救原理 …… 250
4.13.2 数据恢复工具EasyRecovery …… 250
4.13.3 文件的彻底销毁 …… 254
习题 …… 255
第5章 日常上网的安全防范 …… 257
5.1 电子邮件安全防范 …… 257
5.1.1 入侵E-mail信箱 …… 257
5.1.2 E-mail炸弹 …… 259
5.1.3 反垃圾邮件 …… 261
5.2 网络浏览安全防范 …… 266
5.2.1 IE恶意修改和恢复 …… 266
5.2.2 网页炸弹攻击与预防 …… 269
5.2.3 “网络钓鱼”及其防范 …… 269

5.2.4　浏览器安全…… 272
5.3　网络聊天安全防范 …… 277
5.3.1　网络通信软件密码盗取…… 277
5.3.2　网络通信软件消息炸弹…… 281
5.3.3　偷窃网络通信软件记录…… 283
5.4　网络购物安全防范 …… 284
5.4.1　预防网络购物诈骗…… 284
5.4.2　防止 Cookie 泄露个人信息 …… 286
习题…… 289

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世纪初的信息全面保障。

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。

计算机网络的出现和发展，特别是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络在一起，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，国家安全赖以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。人们开始像重视“制海权”、“制空权”一样重视“制信息权”，有意地将

各种信息技术和武器装备综合、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行动上升为关键性的,甚至是决定性的作战形式,从而形成了信息战理论。

信息战的目的是夺取信息优势,其核心是保护己方的信息资源,攻击敌方的信息系统,是全方位的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以生存和运转的基础——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。

大量的安全事件和研究成果揭示出信息系统中存在许多设计缺陷,存在情报机构有意埋设安全陷阱的可能。例如,在发达国家现有技术条件下,CPU 中可以植入无线发射接收功能;操作系统、数据库管理系统或应用程序中能够预先安置从事情报收集、受控激发破坏功能的程序。通过这些程序,可以接收特殊病毒、接收来自网络或空间的指令,触发 CPU 的自杀功能、搜集和发送敏感信息;通过特殊指令在加密操作中将部分明文隐藏在网络协议层中传输等。而且,通过唯一识别 CPU 个体的序列号,可以主动、准确地识别、跟踪或攻击一个使用该芯片的计算机系统,根据预先设定收集敏感信息或进行定向破坏。

由于信息系统安全的独特性,人们已将其用于军事对抗领域。目前信息对抗理论与技术主要包括:黑客防范体系、信息伪装理论与技术、信息分析与监控、入侵检测原理与技术、反击方法、应急响应系统、计算机病毒、人工免疫系统在反病毒和抗入侵系统中的应用等。

1.1.1 信息战的主要内容

信息战的内容涉及到在信息领域中战胜被攻击对象的所有行动,其对抗的双方彼此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。

(1) 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。

(2) 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。

(3) 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，以攻为主，互相支援配合，才能从根本上夺取信息优势。

海湾战争中，由于伊拉克军队在信息对抗领域的指导思想是一味采取消极防御策略，尽管其隐蔽、伪装取得了一定的成效，但由于没有采取积极有效的信息进攻策略，结果在多国部队强大的信息攻势面前始终摆脱不了十分被动的局面。相反，在科索沃战争中，面对北约强大的信息攻势，处于信息劣势的南联盟采取隐蔽、伪装、规避、控制等信息防御的同时，积极主动地采取多种手段，与北约部队展开信息优势的争夺，结果取得了包括击落 F-117A 隐形飞机和大量巡航导弹的不菲战果。

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。

进攻性信息战武器或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，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，至少名义是，目前还没有哪一个国家敢承认它是这些病毒的制造者。

1990 年海湾战争时期，美军把具有神经网络细胞式的自我变异功能的病毒程序注入伊拉克国家通信网接口，在美军正式进攻前，伊拉克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。

海湾战争爆发前不久，美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伊拉克购买的计算机打印机中的芯片。战争爆发后，美国用指令激活了伊拉克防空系统计算机打印机内的计算机病毒，病毒通过打印机侵入防空系统的计算机中，使整个防空系统的

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,可以被导弹或炸弹等武器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,嗜食硅集成电路,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

另一种摧毁性武器就是能量比高能射频枪大,以光速发射出去的电磁脉冲,它能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。

电磁大轰炸是科索沃战争采用的手段之一,通过电磁干扰,使得南斯拉夫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。不但能使敌人的战场指挥网络失灵,更能使敌国金融混乱、股市崩溃、交通瘫痪,经济全面衰退,直至完全丧失抵抗能力。

心理战部队利用各种现代信息传播手段,以前所未有的速度、无所不在的广度、对敌人进行全方位的心理攻击,使敌人军心涣散、民心动摇、斗志丧失、精神崩溃。

1.2 电 子 战

电子战,也叫电磁战,是利用电磁频谱进行的斗争和对抗。其对抗的基本形式是侦察与反侦察、干扰与反干扰、摧毁与反摧毁。目的在于削弱、破坏敌方电子设备的使用效能和保护己方电子设备正常发挥效能。

电子战是随着电子武器装备的发展而发展的。无线电的发明并应用于军事,出现了窃听与反窃听、破译与反破译的装备与对抗;伴随雷达的发明与发展,出现了雷达探测与反探

测的对抗；光电技术在装备上的应用，出现了光电对抗；计算机技术的飞速发展，出现了计算机网络的对抗。

信息时代的电子战，其频谱范围已从无线电射频扩展到声波、光波频段，电子战的作战领域也已经扩展到深海和太空。原来以通信和雷达对抗为主的电子战，发展到现代战场 C4ISR（Command、Control、Communication、Computer & Intelligence、Surveillance、Reconnaissance，指挥、控制、通信、计算机与情报、监视、侦察）系统之间的整体对抗。电子战手段也由以软杀伤为主，发展到软杀伤和硬摧毁相结合。它以最广泛的渗透性进入军事斗争的各个领域，成为未来信息战场的核心和支柱。

1.2.1　电子战的历史

人类战争史上比较公认的第一次电子战出现在 1904 年 2 月的日俄战争中，日方试图通过无线电通信把正确的射击指令传送给装甲巡洋舰。然而，俄国基地的一个报务员听到了日方舰艇之间正在进行信息交换，意识到了它的重要性，本能地按下了当时无线电通信设备的火花发射机的按键，对日方舰艇之间的通信实施了干扰。结果在那天的海战中，由于日方的正确射击指令受到了干扰，俄国军舰几乎无一损伤。

第二次世界大战之后，雷达技术得到迅速发展，雷达的探测距离、跟踪精度、分辨能力都有了进一步的提高，飞机、导弹、卫星、舰艇、火炮都装备了先进的雷达。人们针对雷达制导系统研制出了各种欺骗干扰装备和器材，还研制出了专门对付雷达的反辐射导弹，以及专门用于电子对抗的电子战飞机。

20 世纪 60 年代，越南战争初期，越军平均发射 2～3 枚地对空导弹就能击落 1 架美军飞机。20 世纪 70 年代，由于美军在飞机上安装了雷达报警接收机，部署了反辐射导弹，还使用了杂波干扰机，越军平均发射 70～80 枚导弹才能打落 1 架美国飞机。

1982 年 6 月的贝卡谷地作战是一次典型的电子战。战斗开始前，以色列派了一些无人机到叙利亚阵地上空飞行。无人机经过了特殊伪装并装有防空设备，这种无人机本身反射面积很小，雷达回波反射信号比较弱，但加装了一些角反射器之类的装置，使得反射面积增大，信号增强。叙利亚误以为大型飞机来攻击，于是开动制导雷达。无人机将导弹系统的一些参数，如频率参数测到了，同时也把叙利亚的导弹阵地的位置侦察到了。以色列第一步先取得信息，第二步就发动攻击。攻击时，最高一层是预警飞机，作为空中指挥；第二层是 F-15 作为护航；最底层是 F-16 攻击地面目标。以军攻击前首先派无人机引诱导弹阵地开机。导弹阵地开机后，以色列发射反辐射导弹。就这样，以色列一举摧毁了叙利亚 19 个导弹阵地和几十架作战飞机。

1982 年 5 月 25 日，阿根廷的斯坦利雷达站发现英军的“竞技神”号航空母舰在马岛东北方约 120 海里处活动。阿根廷 2 架“超级军旗”飞机立即起飞，向英军“竞技神”号航空母舰发射了 2 枚“飞鱼”导弹。几个月前，就是这种“飞鱼”导弹，取得了将英国“谢菲尔德”号驱逐舰艇击沉的辉煌战绩，但这次“飞鱼”导弹却失去了往日的光环。吃过苦头的英国人在“飞鱼”导弹袭来时，立即发射大量的箔条干扰导弹的制导系统，结果 2 枚导弹都偏离了目标。马岛之战，充分显示了电子战的巨大作用。

1991 年海湾战争结束后，人们总结这场战争的特点是陆、海、空、天、电，五维一体。电子战过去一直是战场上的配角，海湾战争中竟然与陆战、海战、空战、天战平起平坐，成为第

五维战场。海湾战争的实践表明,电子战在信息化战争中具有十分重要的地位和作用。海湾战争作为首次信息化战争,电子战既充当了战争的"先行官",又作为战争的主力军,贯穿于战争的始终,成为真正的关键角色,使人们对它刮目相看。

1.2.2 电子战的攻防

目前电子战武器已发展为两大类。一类为电子战软杀伤武器,包括各种信息侦察设备、干扰设备、欺骗设备以及计算机病毒等;另一类为电子战硬摧毁武器,包括各种反辐射导弹、反辐射无人机、电磁脉冲弹等武器。

1. 电子攻击战

利用电子战手段,对敌方的信息网络接收设备实施干扰和压制,是破坏敌方进行电磁信息交换的主要战法,可迫使敌方电磁信息设备无法有效地接收和处理战场信息,变成战场上的"瞎子"和"聋子"。

这种战法在20世纪局部战争中获得了广泛的应用。越南战争期间,美军采用雷达干扰压制,使其作战飞机的损失率由初期的14% 下降到后期的1.4%,约340架飞机免遭击落。在贝卡谷地战斗中,以色列使用干扰压制方法,一举摧毁叙利亚19个防空导弹阵地、击落其80架战斗机,而己方却没损失一架飞机。

在信息对抗的要求下,大规模破坏对方电子系统的武器应运而生,如电磁脉冲弹、电力干扰弹等。

电磁脉冲弹可以在瞬间产生大范围、宽波束、高功率的电磁脉冲,将各种电子设备中的敏感电子器件统统烧毁。电磁脉冲弹的出现,将使所有以电子技术为核心的高技术武器装备面临前所未有的考验。

电力干扰弹在高压线和变电站上空炸开后,大面积的导电纤维丝散布开来,降落在高压线上,造成大面积、长时间的停电事故。美军在海湾战争中通过"战斧"导弹携带这种"碳纤维"弹头,在伊拉克的7座发电厂上空爆炸,使巴格达一片漆黑。

2. 电子防守战

未来的信息作战,敌方必将充分运用其先进的信息网络系统,对我方实施全方位、全天候的信息攻击。为有效地防护敌方的信息攻击,可以采用隐蔽频谱、隐蔽电文、干扰掩护等手段。

(1) 隐蔽频谱:采用随机多址通信、扩频通信、跳频通信等技术手段,减少通信中的泄密。

(2) 隐蔽电文:充分利用电子加密技术,特别是利用计算机技术,在保密通信中的控制、检验、识别、密钥分配及加密、解密等环节,为电磁信息的密化提供有利的条件。

(3) 干扰掩护:利用电子干扰手段,使某一特定环境内或某一方向上,己方电磁能量达到信息接受设备所能允许的电磁兼容限度,以掩护己方电磁信息不被敌方识别。在对越自卫反击作战中,我军为保护通信频率,在通信频率附近发射干扰信号,曾多次成功地掩护了我军的通信。

1.2.3 电子战的发展

电子战已经走过了整整100年的历史,留下了一串串耀眼夺目的光辉。它开始是作为