信息隐藏技术及其军事应用

XINXI YINCANG JISHU JIQI JUNSHI YINGYONG

王也隽　主编

国防工业出版社
National Defense Industry Press

总装部队军事训练“十一五”统编教材

信息隐藏技术及其军事应用

王也隽　主编
彭德云　刘胜利　周　立　副主编

国防工业出版社
·北京·

图书在版编目（CIP）数据

信息隐藏技术及其军事应用/王也隽主编. —北京：国防工业出版社，2011.5
总装部队军事训练“十一五”统编教材
ISBN 978-7-118-07245-7

Ⅰ.①信… Ⅱ.①王… Ⅲ.①电子计算机-安全技术-应用-军事-教材 Ⅳ.①E919

中国版本图书馆 CIP 数据核字(2011)第 030736 号

※

国防工业出版社出版发行
（北京市海淀区紫竹院南路 23 号　邮政编码 100048）
国防工业出版社印刷厂印刷
新华书店经售
*
开本 880×1230　1/32　**印张** 14⅜　**字数** 398 千字
2011 年 5 月第 1 版第 1 次印刷　**印数** 1—4000 册　**定价** 38.00 元

国防书店：(010)68428422　　发行邮购：(010)68414474
发行传真：(010)68411535　　发行业务：(010)68472764

前　言

军队信息化建设和国防安全建设系及国家和民族的兴衰存亡。当前，我军正经历由机械化向信息化的历史转变。在信息化飞速发展的过程中，如何确保军事信息的安全，如何进行安全有效的信息传输，成为摆在全军各级指挥员和技术人员面前的一项重大课题。而目前的保密通信系统基本上都是以密码理论为基础，安全等级很大程度上取决于密钥的长度。但随着计算机处理能力的迅速提高，这种通过增加密钥长度来提高系统安全等级的方法变得越来越不可靠。信息隐藏技术作为一种新颖的信息对抗方式，为隐蔽通信提供了高等级的安全传输途径，它将对未来信息化战争产生深远的影响。

信息隐藏技术的研究始于20世纪90年代，是一项崭新且有着古老思想渊源的信息保护技术。自提出以来，国内外学术界、工业界、政府和军方研究机构投以极大的热情，掀起了信息隐藏的研究热潮。各种信息隐藏理论和算法如雨后春笋般提出，各种应用技术产品也不断涌现。信息隐藏的理论和技术以惊人的速度向前发展。经历了十几年的发展，信息隐藏的研究逐步走向成熟。信息隐藏技术和密码技术、数字签名、软件保护、电子印章、信号处理等多种技术相互交融，不断走向实用化。

信息隐藏最初就起源于军事上的秘密通信，目前的发展也和军事应用有很深的渊源。信息隐藏的军事应用，一方面可用于情报传递、信息安全基础设施、隐蔽通信和应急通信领域，另一方面可用于情报侦察领域。这些军事领域的应用，在目前的相关研究文献中曾有报道，但缺乏翔实、系统、前沿的论述。

针对军队研究人员和部队院校通信、电子信息、情报等专业的学员在此领域的学习需要，为使我军在隐蔽通信和信息对抗的新领域中占得先

机，我们编写了这部教材。本书共分为8章：第1章着眼于网络时代的信息安全问题，主要介绍信息隐藏技术的研究背景、应用和进展等基本情况；第2章是信息隐藏系统的总体描述，包括信息隐藏系统的定义、一般构成和术语、评价指标等，以使读者对信息隐藏系统有总体、全局的理解和把握；第3章着重介绍信息论、加密技术、扩频编码、混沌、分形等信息隐藏相关的理论和技术；第4章结合源代码介绍信息隐藏的各种具体算法的原理和实现；第5章介绍数字水印的概念、技术原理和典型算法，以及数字印章技术、可见水印、数字水印标准化等水印技术的最新进展；第6章介绍隐写分析的技术原理、模型、性能评价和主要算法实现；第7章介绍信息隐藏在应急隐蔽通信、情报侦察正反两个领域的应用；第8章介绍国外信息隐藏技术的研究和应用进展情况，并重点分析美、欧、日等国家（地区）的信息隐藏项目案例，作为我军开展该领域研究的借鉴。

本书内容覆盖了目前信息隐藏研究领域的主要理论和技术，跟踪前沿动态，重点论述了该技术在军事领域的应用。主要读者对象为从事通信、情报和信息对抗领域的研究人员、工程技术与管理人员，计算机、通信专业的本科生或硕士研究生。

本书第1章、第3章由王也隽编写，第2章、第4章、第5章和第8章由彭德云编写，第6章、第7章由刘胜利编写，王也隽、彭德云负责书稿的审定工作。另外，周立在整理和校对方面做了许多工作。

本书汇集了编者最新的研究成果，并参阅了大量的文献资料，引证标注如有遗漏，请与我们联系。由于篇幅限制，书中实现代码未能在附录中全部体现，如需要参考请给我们发邮件（peng_d_y@ sohu. com）。特别感谢王嘉祯教授和汤光明教授的指导帮助，并向所有为本书出版付出劳动、做出努力的同志以及文献资料的作者表示衷心的感谢！

由于编者水平有限，写作时间仓促，错误之处在所难免，恳请读者不吝赐教，以资修正。

编著者

目　录

第1章 绪 论

信息隐藏(Information Hiding)技术是指利用人类感官的不敏感性和信号本身存在的冗余,采用软件或硬件的方法将某种信息嵌入到宿主信号(如图像、声音、视频或文本文档)中,并在必要时可检测或提取隐藏信号的技术。作为一项新兴的前沿技术,其研究内容主要涉及计算机软硬件技术、图像处理技术、信号处理技术,并与最新的国际标准和技术紧密相关,例如,小波变换、分形学、混沌学、现代加密技术、快速算法等。

本章重点为网络时代的信息安全问题,主要介绍信息隐藏技术的研究背景、应用和进展等基本情况。从信息安全及其目前存在的问题入手,引出信息隐藏的概念;给出信息隐藏与信息安全的主要支撑理论——密码学之间的关系,给信息隐藏一个基本定位;介绍信息隐藏的应用情况和研究进展。

1.1 信息安全问题

1.1.1 网络时代和信息安全问题

21世纪是网络的时代。随着科技的快速进步和社会需求的日益增长,全球最大的网络——因特网(Internet)正以惊人的速度发展。据Internet World Stats[①]统计,2000年底,全球网民数量为3.6亿人;而截至2009年3月,全球网民数量已达15.8亿人,增长了3.38倍,其中中国以

① http://www.internetworldstats.com/stats.htm。

2.98 亿高居首位。我国网民的增长速度惊人。1998 年底为 210 万人，而截至 2008 年 6 月底，我国网民数量达到了 2.53 亿人，增长了 120 倍。并首次大幅度超过美国，跃居世界第 1 位，如图 1 - 1 所示。

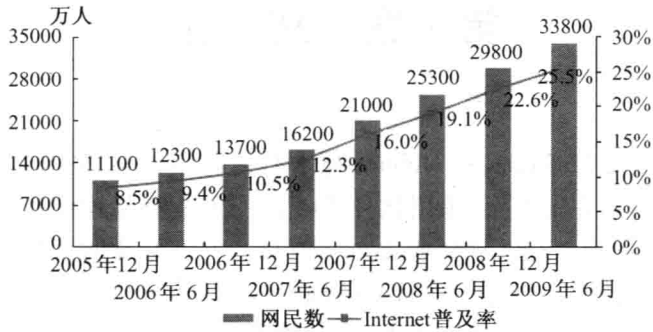

图 1 - 1 中国网民人数增长情况①

Internet 的触角遍布全球，将地球连接成为一个紧密相连的网络村。计算机网络已经将地球紧密地连接为一体！图 1 - 2 是计算机生成的 Internet 的拓扑结构图。

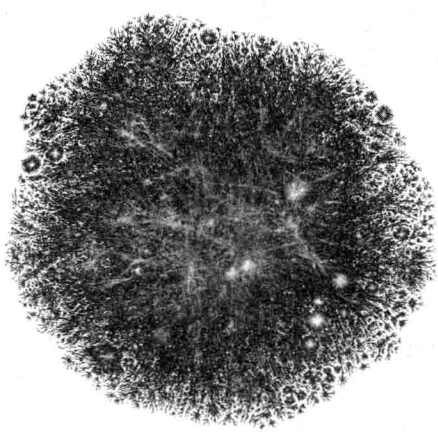

图 1 - 2 Internet 的全球主要路由器分布可视图

① 摘自 http://www.cnnic.cn。

越来越多的公司、团体、机关、个人通过信息网络互相连接，其应用范围从单纯的电子邮件通信扩大到按需点播、远程会议、电子商务、电子政务、电子银行、网上图书馆、网上购物等，从而发展成为陆、海、空、天、电磁之外人类社会生存与发展的另一维空间，即信息空间（Cyberspace）。信息成为一种重要的战略资源，信息技术的发展水平和信息安全保障能力已成为综合国力的重要组成部分。

与此同时，网络与信息安全可能会影响个人的工作、生活。因此，网络与信息安全产业在整个产业布局乃至国家战略格局中具有举足轻重的地位和作用。

信息技术的发展和网络社会的到来，在给人类社会带来巨大进步的同时，也在深刻改变着人类的安全观念，并使国家安全面临诸多新的挑战，甚至会影响国家政治稳定、经济发展、社会和谐和国防军事安全。一方面，信息领域的争夺日益激烈，控制信息权成为新的战略制高点；另一方面，计算机病毒和黑客攻击等大量信息时代的威胁应时而生，对信息化程度较高的银行、交通、商业、医疗、通信、电力等重要国家基础设施造成严重破坏，成为影响国家安全的新威胁。

作为全球信息化程度最高的国家，美国拥有世界上最先进和最庞大的信息系统，对信息网络的依赖性也最大。一旦受到攻击，其后果非常严重。据统计，美国由于网络安全问题造成的损失粗略估计每年高达几百亿美元。例如，2000 年 2 月初，美国多家著名网站遭到黑客攻击，造成的直接和间接损失超过 10 亿美元；2005 年 6 月，美国最大信用卡公司之一的万事达公司的众多用户的银行资料被黑客窃取，酿成美国最大规模信用卡用户信息泄密案；2006 年 5 月，美国退伍军人事务部发生失窃事件，窃贼将存有 2000 多万名退伍军人个人资料的电脑硬盘偷走，造成美国前所未有的军人资料数据大规模失窃，对美国的军事安全构成了潜在威胁。

因此，美国一直高度重视信息安全问题，把确保信息系统安全列为国家安全战略最重要的组成部分之一，采取了一系列旨在加强网络基础设施保密安全的政策措施。例如，美国是最早引入网络战概念的国家，也是最先将其应用于战争的国家。美国还组建了网络攻防部队，严防网络恐

怖袭击。2009 年 2 月 9 日,美国总统奥巴马要求对美国的网络安全状况展开为期 60 天的全面评估,以检查联邦政府部门采取保护机密信息和数据的措施。

不仅美国,俄罗斯近年来对国家信息安全的重视程度也日益提高,已将信息网络安全纳入国家安全战略,并采取不断完善网络信息安全立法、建立网络信息安全保障体系等措施维护国家的信息安全。2000 年,总统普京批准了《俄罗斯联邦信息安全构想》,并强调“信息资源和信息基础设施已经成为争夺世界领先地位的舞台,未来的政治和经济将取决于信息资源”。

日本政府也强调“信息安全保障是日本综合安全保障体系的核心”,于 2001 年发布《电子日本战略》,宣布要确保信息通信网络的安全性及可靠性。另外,为了应对这一新形势,英国、法国、德国等发达国家已将信息安全提高到前所未有的高度,大力加强军事信息安全建设,谋求在信息化战争的有利地位。

“他山之石,可以攻玉”。发达国家的做法表明,信息安全已成为国家和军事安全的重要组成部分。当前,我国的信息化建设正飞速发展,信息安全的需求十分迫切。利用计算机网络进行犯罪、窃取机密信息的案例屡见不鲜,信息安全风险威胁到了国家信息基础设施的安全。然而,网络与信息安全问题必须依靠我国自己的力量来解决,引进国外产品或照搬国外先进技术无异于引狼入室,将生存决定权置于他人之手。为此,国家明确规定:信息安全产品一定要立足于国内自主开发。

1.1.2 信息化战争与信息时代的军事信息安全

进入信息时代,无形的信息已在现代信息化战争中起到决定性作用。信息已成为除了“陆、海、空、天、电磁”以外的又一维空间。为了夺取“制信息权”,信息对抗将是未来信息化战争的重要作战样式。信息安全也必然成为关系未来信息化战争胜负的战略课题,成为夺取作战胜利的重要保证,甚至是决定性因素。确保军事信息安全是信息化作战的关键任务之一,是掌握战场主动权乃至战争制胜权的前提和基础。

信息时代的军事威胁不是大军压境，而发生在敌对双方在信息领域的干扰与反干扰、破坏与反破坏、摧毁与反摧毁的斗争中。军事信息安全内涵具有特殊性，如严格的保密性、地位的战略性和超强的技术性，主要表现为军事泄密、黑客攻击和信息战三个方面。

海湾战争和伊拉克战争中，美国通过监听、跟踪所有伊拉克的通信，为美军的作战行动获取了大量有价值的情报信息；并通过多种途径，散布大量虚假消息，使伊军的信息系统陷入瘫痪，使其指挥混乱，武器火力无法发挥作用。

科索沃战争中，北约对南联盟狂轰滥炸，唯独对其手机基站网开一面，原因何在？就是利用手机网络的开发和广播特性，从中截获所需情报。于此同时，北约的信息系统也连续遭到俄罗斯和南联盟计算机“黑客”的网上攻击，致使其计算机系统的软、硬件受到计算机病毒的重创，白宫网站曾经一整天无法工作，某航空母舰的指挥控制系统也曾被迫停止运行 3 小时。

美国最早将信息安全提升到国家战略安全的高度，认为网络攻击是与核、生、化等武器并列的大规模破坏性武器。特别是“9 · 11”事件以后，美国接连颁发了多个重要信息安全法规和总统令，专门组建了信息安全机构，加强了统一领导，建成了专门的信息作战力量。

要打赢信息化条件下的局部战争，就必须拥有信息优势，必须适应信息化日新月异的更新步伐。原中央军委副主席、国务委员兼国防部长曹刚川表示：信息安全是国家安全体系中的关键要素。因此，我们必须从战略高度重视军事信息安全技术的推广与应用。

1.1.3　新兴的信息隐藏技术

目前的信息安全技术基本都是基于密码学理论的，无论是采用传统的密钥系统（如 DES）还是公钥系统（如 RSA），其保护方式都是控制文件的存取，即将文件加密成密文，使没有密钥的非法用户无法获知明文。其致命的缺点是它明确地提示攻击者或监听者哪些是重要信息，容易引起攻击者的好奇和注意，增加其攻击破解的欲望。

而随着计算机计算能力的不断提高和分布式计算技术的迅猛发展，