现代电子信息技术丛书

信息安全与保密

—— 现代战争的信息卫士

主编 黄月江　副主编 龚奇敏

国防工业出版社

信息安全与保密

电子科学研究院组织编著

现代电子信息技术丛书

信息安全与保密

——现代战争的信息卫士

主　编　黄月江
副主编　龚奇敏

国防工业出版社
·北京·

图书在版编目（CIP）数据

信息安全与保密：现代战争的信息卫士/黄月江主编．
－北京：国防工业出版社，1999（2001．3重印）
（现代电子信息技术丛书）
ISBN 7-118-02092-3

Ⅰ．信… Ⅱ．①黄… Ⅲ．①信息-安全-技术②保密通信③电子计算机-安全技术 Ⅳ．TN918

中国版本图书馆 CIP 数据核字（1999）第 02763 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 100044）
涿中印刷厂印刷
新华书店经售
*
开本 787×1092 1/16 印张 13 288 千字
1999 年 9 月第 1 版 2001 年 3 月北京第 2 次印刷
印数：3001—5000 册 定价：19.00 元

《现代电子信息技术丛书》编审委员会

《现代电子信息技术丛书》总编委

《信息安全与保密》分册编著人员

主　　编　黄月江

副 主 编　龚奇敏

编著人员（按姓氏笔划排序）

王晓鸣　方关宝　朱甫臣　陈　倩　罗昭武

段丽斌　唐　勇　蒋继洪

序

信息技术是一个复杂的多层次多专业的技术体系，粗略地可以分为系统和基础两个层次。属于系统层的一般按功能分，如信息获取、通信、处理、控制、对抗（简称为5C技术，即Collection，Communication，Computing，Control，Countermeasure五个词的第一个字母）等；基础层技术一般按专业分，如微电子、光电子、微波真空电子等。

信息技术革命的火炬是由微电子技术革命点燃的，它促进了计算机技术、通信技术及其他电子信息技术的更新换代，迄今，尚未有尽期。信息技术革命推动产业革命，使人类社会经历了农业、工业社会后进入了信息社会。

大规模集成电路的集成度是微电子技术革命的重要标志，它遵循摩尔（Moore）定律，每18个月翻一番，预计可延伸到2010年。届时，每个芯片可包含100亿（10^{10}）个元件，面积可达到10cm^2，作为动态存储器的存储量可达64Gb（吉比特），接近理论极限10^{11}个元件和256Gb存储量。微处理器芯片的运算速度每5年提高一个数量级，到本世纪末，每个芯片运算速度可达10～100亿次每秒，有人认为，实现2000亿次的单片微处理器在技术上是可能的。与此相适应，每芯片比特存储量与每MIPS（兆指令每秒）运算量的成本将呈指数式下降，现在一个100兆指令/s专用数字信号处理芯片只售5美元。如果飞机的价格也像微电子那样呈指数式下降的话，70年代初买1块比萨饼的费用在90年代就可以买1架波音747客机。3年内1部电话机将只用1块芯片，5年内1台PC机的全部功能可在1个芯片上实现，6年内1部ATM交换机的核心功能也可用1个单片完成。由于微处理器芯片价格持续不断地下降，构成了它广泛应用的基础。现在，在一般家庭、汽车和办公室中，就有100多个微处理器在工作，不仅是PC机，而且在电话机、移动电话机、电视机、洗衣机、烘干机、立体声音响、家庭影院中也有。1辆高档汽车中包含20多种可编程微处理器，1架波音777客机含有100多万行的计算机程序代码。

通信技术的进步还得力于光子技术的进步。光通信速率（比特每秒）每两年翻一番，现在实验室中已可做到10^{12}b/s，即可将全世界可能传输的全部通信量于同一时刻内在1根光纤中传送，或相当于1s内传输1000份30卷的百科全书。通信速率的提高和通信容量的增大，使光通信成本也不断降低，与80年代相比，降低了两个数量级。

因特网是全球信息基础设施的雏形，其发展速度惊人。现在每0.4s增加

一个用户，每4min增加一个网络。1996年联网数大于10万，联网主机数大于1000万，用户数大于7000万(预计到本世纪末，将大于2亿)，PC机总量将达5亿，联网主机达3000万，信息量每5年翻一番。越来越多的公司、团体、机关、个人通过信息网络相互联接，其应用范围从单纯的电子函件通信扩大到远程合作(包括教育、诊断、办公、会议、协作等)、按需点播、多媒体文娱、电子商务、银行、支付等，人类社会生存与发展的另一维空间，即信息空间或称为赛博空间(Cyberspace)正在形成。如果说工业社会是建筑在汽车与高速公路上的话，信息社会则是建筑在信息与信息高速公路上的。政府、军队、经济、金融、电力、交通、电信等关键部门都要依赖于信息基础设施的正常运行。信息技术和信息产业的水平已成为综合国力的重要标志，也是国际竞争力的焦点与热点。

信息技术的飞跃发展及其渗透到各行各业的广泛应用，不仅推动了产业革命，而且也深刻地改变了人们的工作、学习和生活的方式。信息技术不仅扩展了人的视觉、听觉等感知能力，而且还渗透到思维领域，减轻或部分地替代人的脑力劳动，提高思维的效率和质量，实现人的思维能力的延伸，增强人的认知能力。信息作为事物的属性与相互关系的状态的表达是客观存在的，但不是显在的，很多是潜在的，有的是深埋的，有待挖掘与提炼。信息技术大大地丰富了信息采集的内容，提高了信息处理的能力，为人们对客观事物及其规律的认识提供了创新的工具，也为人们正确认识与有效改造主观世界和客观世界提供了源泉，将使社会的物质文明与精神文明建设得到极大的发展。

信息、能源与物质是人类社会赖以生存与发展的三大支柱。在信息社会中，信息是最重要的支柱和最重要的产业，它影响着其他两个支柱的健康发展，包括生产、传输、分配、运行、减少损耗、改善管理、提高效率、降低成本等等；同时，它还能不断地培育与发展新物质和新能源的发明与生产，不断地改善生态环境，从而使人类社会进入可持续发展的健康轨道。

信息革命在带动产业革命的同时也带动军事革命，使得军事技术、武器装备、作战思想、作战方式、战争形态、军事原则、军事条令与部队编成等都将发生深刻的变化。如果农业社会是冷兵器时代，工业社会是热兵器时代，那么信息社会则是信息兵器时代。信息、信息系统与信息化平台、武器与弹药成为战场上的主战兵器。信息优势成为传统的陆地、海洋、空中、空间优势以外的新的争夺领域，并深刻地制约着传统领域的战斗胜负，从而构成信息化战争的新形态。在这种战争中，战争胜负决定于敌对双方掌握信息与信息技术的广度与深度。信息不仅是兵力倍增器，它本身就是武器和目标，是双方必争的制高点。1991年初的海湾战争，被称为硅片战胜钢铁的战争，即源于这样的认识。它开启了赛博空间战、网络战、信息战等簇新的作战方式。

以信息优势为核心的军事革命是建筑在先进的指挥、控制、通信、计算机、情报、监视、侦察及其一体化的信息战能力的基础上的，这个众系之系（系统的系统）我国称为综合电子信息系统，与美军后来提出的 C^4ISR/IW 相当，它由以下 6 部分组成。

1. 鲁棒的多探测器信息栅格网络。为作战部队提供作战空间感知优势。

2. 先进的指挥控制与作战管理栅格网络。为部队提供作战的先期规划、胜敌一筹的作战部署，执行作战指挥控制与一体化兵力管理能力。

3. 从探测器到射击器的栅格网络。为部队提供精确制导武器的动态目标管理、分配与引导，协同作战，一体化防空，快速战损评估和再打击能力。

4. 联合的通信、导航与定位栅格网络。提供可靠、安全、大容量与高精度的信息，以支持部队的机动行动，确保全面优势。

5. 信息进攻能力。采取侵入、操纵与扰乱等手段，阻碍敌人作战空间感知、认知与有效用兵能力。

6. 信息防护能力。保证我方信息系统的安全，防护敌方对我信息网络的利用、干扰和破坏。

这个系统的系统涉及众多先进的信息技术的横向与纵向的有机集成，它包括雷达和光电的有源与无源探测技术、有线和无线及固定和移动通信技术、计算机硬件和软件技术、精确导航定位技术、航天航空测控技术、信息安全保密技术、电子战技术等横向专业技术的集成；也涉及微电子技术、光子与光电子技术、真空电子技术、压电与传感器技术等先进元器件技术，电子材料技术、电源技术、测试技术、先进制造技术等纵向基础技术的集成。当代军事革命要求在创新的军事思想指引下，发展有层次多专业的纵横集成的信息技术；同时，又要求在先进的信息技术驱动下，培育与发展新的军事思想，并在此基础上推动作战原则、军事条令与部队编成的变革，形成军事革命与信息革命的有机结合。

我们正处于世纪之交，党的第十五次代表大会的胜利召开，启动了有中国特色的社会主义事业在邓小平理论的指引下全面进入 21 世纪。我国的国防与军队现代化建设的跨世纪历史进程已经开始。为了适应军事革命环境下的高新技术军事斗争的需要，我军必须拥有信息优势，必须拥有以先进的综合电子信息系统为基础结构的性能优良的武器装备，必须提高部队素质，把人才培养推上新的台阶。

江泽民总书记非常重视人才的培养，他多次指示，要用高新技术知识武装全军头脑。在未来的信息化战场上，知识将成为战斗力的主导因素，敌对双方的较量将更突出地表现为高素质人才的较量。本丛书的编写出版就是为贯彻这个伟大号召提供系统基础知识。全书以先进的综合电子信息系统为龙头，

多层次、全方位地介绍相关的各项先进信息技术，既包括系统技术，也包括基础技术，共17个方面，荟萃成17个分册。丛书的编写以普及先进信息技术知识为目标，以中专以上文化程度，从事军、民用电子信息技术有关业务的技术人员和管理干部为主要对象，努力做到深入浅出，雅俗共赏，图文并茂，引人入胜，文字简练，语言流畅，学术严谨，论述准确，使其具有可读性、可用性、先进性、系统性与权威性。参加丛书各分册撰写的作者都是长期从事现代信息技术研究与发展的专家，他们在繁重的业务工作的同时，废寝忘食，长期放弃节假日的休息，辛勤耕耘，鞠躬尽瘁，为本丛书做出了卓越的贡献。他们以自己的模范行动，“努力成为先进思想的传播者、科学技术的开拓者、‘四有’公民的培育者和优秀精神产品的生产者”。我谨代表总编委向他们致以衷心的敬意！

本丛书的编写出版得到原国防科工委与原电子工业部领导的大力支持，得到国防工业出版社领导及责任编辑们的积极推动与努力，借此之机，向他们表示由衷的感谢！

中国工程院院士
原电子工业部科技委常务副主任 童志鹏

前　言

本书是《现代电子信息技术丛书》的一个分册，向读者介绍有关信息安全的基础知识。

20世纪90年代初，海湾战争给人们带来深刻启示：未来战争是海、陆、空、天、电一体化的高科技战争，也是敌对双方政治、军事、经济、科技综合能力的较量。因此各国相继调整国防乃至整个国家的科技发展计划，把发展信息技术放在突出地位。

今天，信息已成为国家的重要战略资源，人类社会活动的各个领域都越来越依赖于信息网络的正常运转，因此，信息与网络的安全直接关系到国家政治稳定、战争胜败、经济繁荣和社会进步，而且，社会信息化程度越高，信息与网络越将成为敌对国家、反政府分子、犯罪分子及各种竞争对手的攻击目标。据美国政府1996年公布的一项报告，近几年各种“黑客”通过因特网非法入侵美国军方、政府机构以及民航、铁路、金融等重要部门的计算机系统，有的窃走包括弹道导弹研究报告、飞机设计档案、有关朝鲜核检查等机密情报，也有的使系统出现混乱甚至瘫痪。仅1995年，美国国防部的网络系统就遭到来自国内外计算机“黑客”多达25万次的攻击，国防信息系统局从1992年到1995年，曾进行过3.8万次攻击试验，攻击的成功率为65%，其中系统管理员只发现4%。美军为检验其国防信息系统的安全性，在1995年9月进行了代号为“联合武士”的演习，一个年轻的空军上尉，在马萨诸塞州汉斯科姆空军基地的电子系统中心控制室，面对五角大楼的高级军事专家，用一台从商店买来的普通微机和调制解调器，在没有任何情报和其他辅助设备的情况下，轻而易举地侵入了美国海军计算机指挥和控制系统，很快获得了美国海军大西洋舰队的指挥权，并向该舰队发布命令，而大西洋舰队的舰长们却一直蒙在鼓里，根本不知道该命令竟来自那位无权的上尉。

在此期间，美国军政首脑部门深入开展了有关信息战的讨论，并从制定规划、改组或新建机构到建立数字化部队各个方面，为打赢未来的信息战而作实质性的准备。1996年7月15日，克林顿总统签发“保护关键基础设施”令，决定成立保护电信、电力分配、石油天然气储运、金融、交通、供水及紧急服务等系统的国家基础设施总统委员会。

据权威部门统计，截止到1998年2月，我国直接接入因特网的计算机已达6.4万台，拨号接入的计算机达34万台，接入网络总数已超过1000个，使用因特网的用户人数超过80万，他们分布在政府各部门及企事业单位。联网后给我国社会信息化带来的好处是非常明显的，但也应十分重视在信息安全方面的负面影响，为此要从法规上、组织管理上及技术上采取综合手段，减小随之而来的安全风险。本书便试图向读者介绍信息安全保密技术的有关知识，以唤起更多人的关心和兴趣。

全书共分六章，第一章：信息安全保密技术概述，用古今中外的若干生动实例说明

信息安全保密对赢得战争、保卫国家是何等的重要，本章还简要介绍信息化社会中信息安全保密的新概念以及实现信息安全保密的基本手段。第二章：撩开密码学的神秘面纱，介绍了作为信息安全保密技术核心——密码学的基本概念，用破译古典密码的实例说明密码的发展史便是密码的编制与破译这对矛盾的斗争史；本章还介绍了当代流行的分组密码体制、序列密码体制和公开密钥密码体制；最后对密码体制的关键性参数——密钥及其管理作了简要介绍。第三章：永远年轻的通信保密技术，介绍保密通信的基本要求，话音、数据、图像等保密通信的特点以及通信网络保密技术和密钥分配技术。第四章：日新月异的计算机安全技术，介绍了造成日益严重的计算机安全问题的主要威胁——计算机病毒等恶意程序以及计算机黑客，并针对这些攻击手段，介绍了基本的保护方法，如隔离、访问控制及采用密码技术的各种安全机制；本章接着还介绍了安全系统的实现以及可信计算机和可信网络的安全性评价方法。第五章：充满挑战的信息系统安全保密技术，较完整地介绍了信息系统安全的策略；信息系统安全保密的体系结构（包括开放系统互连安全体系结构及美军的国防信息系统安全计划）；有关安全协议和安全保密标准体系；信息系统安全管理以及信息技术安全性评价的通用准则。第六章：信息安全保密技术发展趋势，从密码理论、信息基础结构下的安全保密技术及信息战防御体系方面，概略地介绍了可能的发展趋势。

参加本书写作的有黄月江、龚奇敏、蒋继洪、方关宝、朱甫臣、唐勇、罗昭武、王晓鸣、陈倩、段丽斌等。

本书编写过程中，得到童志鹏工程院士以及吴世忠、邱荣钦、李德珍等同志的大力帮助，我们表示衷心感谢。

作　者

内容简介

本书以通俗的语言向读者介绍有关信息安全与保密的基础知识。全书共分六章，分别介绍信息化社会中信息安全保密的新概念以及实现信息安全保密的基本手段；信息安全保密技术核心——密码学的基本概念；通信保密技术；计算机安全技术；信息系统的各种保密措施及信息安全保密技术的发展趋势。

读者对象：具有中专以上学历并从事信息技术研制或管理工作的人员及大中专学校有关专业的师生。

目　录