信息安全与信息战

（美）晓宗　编著

“第一次世界大战是化学家的战争；第二次世界大战是物理学家的战争；第三次世界大战，如果不幸发生的话，将是数学家和信息学家的战争。”生活在信息时代的每一个热爱和平的人，都不能不严肃地自问：对这个已经出现在我们身边的信息战，我们了解了多少？我们准备好了吗？

清华大学出版社

信息安全与信息战

（美）晓宗　编著

“兵者，国之大事，死生之地，存亡之道，不可不察也。”

——孙子

清华大学出版社
北京

内容简介

本书以“9·11”事件和伊拉克战争为背景，从国家安全的高度，首次从历史、理论、技术、教育、法律、管理、实战方面全方位、多视角、深入地探讨了信息安全与信息战。

全书以信息战的侦察、进攻和防御为主干，介绍了网络战场、电磁战场、心理战场上的信息战。重点介绍了美国信息安全界对信息安全的调整、运作、成果、动向和新认识；分析了其中的特点，难点与不足；提出了信息战不应局限在对指挥控制系统(C4ISR)的攻防的物理层面，而应推进到有意识地诱导敌方统帅作出错误决策的战略层面和心理层面。全书按国际信息安全界流行的趋势，将信息安全放入国家安全的大格局中讨论，介绍了值得读者借鉴和深思的有关信息安全的课题。

全书涵盖内容广，信息容量大，引用资料新，是一本有关信息安全与信息战的简明综合性知识读本。本书适合每日离不开信息又关心信息安全的广大读者，尤其是商业战场和军事战场上的指挥人员和信息管理人员阅读。也适合高等院校相关专业的学生作为参考读物。

图书在版编目(CIP)数据

信息安全与信息战 /（美）晓宗编著. —北京：清华大学出版社，2003
ISBN 7-302-07381-3

Ⅰ. 信… Ⅱ. 晓… Ⅲ. 信息战－研究 Ⅳ. E869

中国版本图书馆 CIP 数据核字(2003)第 091048 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：张　民
封面设计：孟繁聪
版式设计：刘祎淼
印 刷 者：世界知识印刷厂
装 订 者：北京国马印刷厂
发 行 者：新华书店总店北京发行所
开　　本：148×210　**印张**：8.875　**字数**：238 千字
版　　次：2003 年 12 月第 1 版　2003 年 12 月第 1 次印刷
书　　号：ISBN 7-302-07381-3/TP·5356
印　　数：1～3000
定　　价：18.00 元

FOREWORD 前言

在本书交排付印之际，谨向各位读者报告本书的写作动机和成书过程。

1. 本书的对象与特点

在人类进入信息社会的今天，人们每天都要直面各种信息，在尽情享受信息社会带来的种种便利时，也同时可能面对自己的计算机感染病毒、信用卡密码被盗等种种信息风险。本书是写给每天离不开信息而又关心和担心信息安全的读者，尤其是商务战场上的信息管理者，军事战场上的信息指挥官，在校学习的学生，以及广大因特网使用者的关于信息、信息安全和信息战的一本简明知识读本。

所谓知识读本，包含了三层含义。

第一是可阅读性。信息安全涉及面既深且广，阅读已发表的文章，特别是一些大师的作品，或文笔艰深，或算法深奥，或穿插大段的计算机程序，常让读者不得不时时中断阅读，四处查找解释，身心俱疲。因此在写作本书时，笔者对涉及信息安全的知识尽可能地做了“平民化”处理。希冀这本书能写成让读者“读”，而不是像教科书那样需要老师“教”，也不似词典那样割裂成词条，仅供读者“查”的读物。

第二是阅读的方便性。为了成书，笔者查阅了千万字的中外素材，投入了数千学时将知识加以分类和比对，深感

如果每位读者获取信息安全知识都要经此炼狱，则这种重复性的社会学习成本实在高昂。有鉴于此，笔者将所采集到的知识重新加以梳理，力求做一个科技园中的向导，引领读者能方便地从一个信息高地鸟瞰整个信息安全的全貌。

第三是阅读的思考性。仔细学习已经出版的有关信息战的中外书籍，可以发现其中一些书籍从古今中外的信息战史中汲取了一些生动的战例。读完后掩卷长思，笔者和许多读者一样常感意犹未尽，总希望作者在为我们描绘出现代信息战的绚丽画卷时，也能从以往案例中归纳、提炼出共性的内在联系。因此本书在引入信息战案例的同时，尽力融入了一些分析和对比，以期和读者一起对信息安全和信息战作更深层次的思考。

所谓简明，就是希冀这本书能写得简明扼要，提纲挈领，概念清晰。哈佛大学商学院的 Anthony Robert 教授于 1965 年提出了著名的三段管理模式：高层管理者所要回答的是“做什么”(what to do)及“何时做”(when to do) 的战略决策问题，而“如何做”(how to do)则是中层管理者制定战术计划的任务，基层则是在战略的目标指引下，如何按照既定的战术计划来组织“具体实施”(do it) 的战斗行为。显然，如何做和具体去做都不是也不应该是一般读者的职责。在对现代信息安全、信息战的论述中，不可避免地会涉及信息技术。但是，本书的主要任务是向读者呈现战争这一人类存在以来就伴随而生的社会行为在现代信息社会的反映，以及它是如何以前所未有的深度、广度和力度深刻地影响着每一个人、每一个机构和国家。

自 1995 年美国国防大学在全球首次培养出 16 名“第一代网络战士”以来，世界大国无不争相加大对信息安全和信息战的研究力度，力求抢占信息社会中的制高点。为了适应信息安全的挑战和需求，美国国家安全局和被评为全美 2003 年大学计算机系第一名的卡内基·梅隆大学合作，在 2003 年秋季招收了 20 名优秀学生，首次推出信息安全技术和管理科学研究班。在学科的培养目标上，明确地提出了要通过信息技术、商业管理和战略政策的复合研究，培养信

息安全学科的综合型领导者。信息大国对信息安全的投入并不因为经济的不景气而稍缓，浪潮汹涌的信息战后是对信息人才更激烈的争夺。信息安全也在朝着将技术和管理、战略和决策的结合中演进。在信息安全领域里，观念的革新，把握时代进程的方向，法律、制度的建立和完善，道德与操守的调适等远比具体技术的开发更为重要。当今，时代的标杆跃升到了信息社会的新高度，在这一个相对持平的又一条起跑线上，新一轮竞争的发令枪声已响。是落后还是迎头赶上，历史在等待着我们的回答。如果能使读者在读完本书后对我们正在进入的信息时代的竞争有新的思考，将是笔者最大的心愿。

2. 本书的组织

本书的构思始于 1997 年，其间通过阅读大量的书刊、杂志和论文集，向诸多先行学者学习了很多知识。2000 年中，笔者开始按信息的生命周期，即数据产生、数据收集、信息生成、信息处理、信息传输、信息存储、信息应用、信息显示、信息消亡的架构组织文章，中间因工作繁杂而几次停笔。

2001 年发生的“9·11”事件震惊了美国人民和国际社会，很多学者将“9·11”事件和“珍珠港”事件相比，美国的大众传媒纷纷对联邦调查局事前未能掌握恐怖袭击的信息大加抨击。身处硅谷，笔者更亲身体验了信息时代的战争离我们是这样近，它可以在没有任何预警的情况下，随时发生。对信息安全和信息战的认识问题确实已经刻不容缓地摆到了每个人面前。面对着一波又一波快节奏、高密度的信息战争，笔者原稿学术型的以信息生命周期为纵轴的安排已经无法反映现实生活中的信息战况的急剧变化。笔者于是将全书的结构推倒重来，改取战争的横截面，以信息的攻防为突现，向读者呈递一份信息战争的简报和战法的归纳。因此，本书最先完稿的是第 4 章信息战进攻和第 5 章信息战防御。

本书开始将信息侦察也归入进攻章，但深入研究信息战和传统的战争观可以发现：传统的战争有明显的战前兵力集结期，战争是

由在时域和地域上不连续的战役组成；然而在信息战中，攻击方可以说是全天 24 小时无时无刻不在搜寻攻击目标和攻击时机。同样，防卫方也在全天 24 小时地对潜在的进攻威胁执行全天候的侦察和防范。对信息战而言，侦察和反侦察已不再是时域和地域上的离散行为，而是攻、防双方每时每地都在进行的连续拼搏。传统的侦察是攻击方在发起攻击前对敌情、地形、攻击点的选择以及对敌方兵力部署等实时信息的获取，而审计则是侦察在信息战中的对抗和延伸。和攻击方侦察实时信息不同，防卫方是在历史事件中通过审计的手段试图挖掘、侦察出攻击方的攻击企图和攻击目标。攻防双方在电磁战场上无孔不入的电子侦察，在网络战场上的网络映射和端口扫描，构成了信息战侦察篇的相互交织、互为反制的战争奇观。这里没有硝烟和炮声，然而侦察的帷幕一经拉开，攻防双方就以传统战争所不可能具有的广度、深度和力度，快节奏、长距离、全方位、大纵深地进行着反复的试探、仔细的评估和激烈的较量。侦察的性质和地位在信息战中发生了很大的变化，它已不再隶属于进攻。因此，笔者将侦察从进攻章中抽出，单列成全书的第 3 章。

西方的经典军事学家克劳塞维茨(德国)在其传世的军事学巨著《战争论》中，对战争及战争的攻防作了深刻的描述。直到今天，《战争论》和中国的杰出军事家孙武的《孙子兵法》一起，仍是世界各国关心和学习军事对抗的学者们的必读书籍。克劳塞维茨将战争定义为“无非是扩大了的搏斗”，并提出了“战争要素与生俱有的暴烈性”。然而，在信息战中我们看到的是进行信息对抗的双方通过网络和电磁空间进行远距离、无接触、兵不血刃的较量，肢体的搏斗被脑力的搏斗所替代。透视人类古今中外数千年来在战场上的信息对抗，无论是三国时代张飞的“鞭马扬尘迷曹兵”，还是近代的英(国)/阿(根廷)马尔维纳斯岛海战中的英军“炮播箔条弹”，他们所进行的都是释放虚假信息，掩护自己，迷盲敌人。只不过由于时代技术所限，张飞依靠战马拖拉树干扬尘以迷盲曹军的视力；英军却是以军舰的大炮撒播金属箔条用以迷盲阿军“超级军旗”军机释放的制导鱼雷。因

此，从信息对抗的角度，对战争中的防守，我们总可以归纳出诸如屏蔽、隐身、规避、欺骗、扰乱、阻击这样的关键词。同样地，对战争中的进攻，我们也可以归纳出诸如监视、截获、跟踪、识别、定位、压制、肢解、聚歼这样的关键词。有鉴于此，笔者在构建本书的框架时，就希求不以罗列各个时期的信息战例为满足，而是希望和读者在一起跨越时空，试图挖掘、比较、总结出信息安全、信息对抗以及信息战的攻防实质。

综上所述，侦察、进攻和防御这三大战争内容构成了信息战的主体。与之相应地，信息战侦察、信息战进攻和信息战防御这 3 章也就构成了全书的骨架。

除了信息的侦察、进攻、防御外，信息安全还涉及政策、标准、人才教育、资格认证等一系列重要的知识，笔者将所有这方面的知识写入第 2 章“信息安全”。它既是后续主干篇章的基础篇，也是必须事先掌握的引导篇。

在笔者授课时，曾在各章中穿插介绍了一些实例。成书时，感到与其零星分解，不如精选网络战、电子战的大案，单独成篇，既为历史上信息战的精彩片断留下定格，也使读者在结束阅读时能将学习到的知识在信息战的实践中得以回放和思考。

全书以“9·11”事件后美国政府对事件的预后和思考，以及随之打响的伊拉克战争切入正题，以在信息安全领域有影响的重要文件和信息安全英语缩略语结束，由此建构了全书的框架：第 1 章 引论，第 2 章 信息安全，第 3 章 信息战侦察，第 4 章 信息战进攻，第 5 章 信息战防御，第 6 章 信息战案例，第 7 章 附篇。

3. 本书的剪裁与行文

按照信息安全行业权威的信息系统安全专家认证考试大纲（certified information systems security professional，CISSP），信息安全涵盖十大领域，包含方针政策、道德法律、行政管理、技术操作、物理设施等方方面面的知识。据此，笔者在成书时，将这十大领域的

知识尽力择要阐述，力求为读者勾勒出一幅信息安全和信息战的剪影。然而，信息战本身的界定也在不断的发展、变化中。目前许多的信息安全考试，仍然只是偏重于网络，甚至将信息战等同于网络战。实际上，远在公元前2000多年前，古埃及人就在墓碑上用象形文字刻写代码，成为人类使用密码术的首次记录。2500年前，中国古代的杰出军事家孙武在他的《孙子兵法》中，已经对信息和信息的重要性、信息的获取、信息在战争中的有效利用做了精彩的描述。显然，信息战要远比网络战有着深厚得多的历史，宽广得多的内涵。古代的信息战自然不可能有现代因特网上的战法。但是，深入研究即可发现，电子和网络只是现代信息战的两个载体，现代信息战的战法和古代的信息战法有时是一脉相承的。本书力求在信息战的发展史中讲清信息战与情报战、电子战、网络战、心理战的关联，也不局限在CISSP所设定的考试范围内，而是将信息安全放到国家安全、全球竞争的大环境中去考察和定位。我们希望，本书作为读本能尽量携载有关信息安全的信息，在读者初读时能作为一个入门的向导，在复读时也还能让读者感到常读常新。同时也希望本书能起到一个入口网站的作用，即使读者有了较深入的信息安全知识，也还能引领读者到信息安全和信息战的更广阔的天地中遨翔。

还要说明的是，本书的内容绝大部分取自于美国信息社会，只有一两处提到了欧洲的信息安全内容。这一方面因为美国在信息安全和信息战的理论和实践上都处于世界领先的地位，另一方面也因为笔者居于硅谷，对美国信息社会的材料较易收集。这些知识对信息安全研究起步较晚，一些相关法律仍属空白或尚在起草的国家和机构或仍不失借鉴、参考的意义。

本书所涉及的信息安全知识，许多地方，完全可以展开而自成一部书。例如防火墙、密码学、数据库、操作系统等，中外已经有很多这些领域的非常优秀的专著。对于这些知识，本书因任务和篇幅所限，只选择了一些概括性的结论。此外，信息安全还涉及生命科学、法学、管理学、军事学、数学、经济学等领域的知识，受本身学识所限，笔

者只能从信息安全角度提出必须理解的纲领性要点。本书既然作为简明读本，只是希望为读者提供一个有关信息安全全景的“泼墨写意”，而不是每一个细节都着墨的“工笔画”，本书不应该也不可能替代信息安全和各科领域内的那些专著。在笔者有限的阅读范围内，感到中文书籍介绍较少的知识，例如计算机犯罪的调查与法庭审讯，美国的信息安全立法推进过程，美国有关信息的法律，美国典型大学对信息安全的教育，以及即使在美国也非常新的知识（如生物攻击预警系统）等，本书则尽可能地做了介绍。

信息安全是一个如此重大和沉重的课题。书中的内容虽经笔者再三斟酌，也一定存有错误，特别是对那些超出笔者本身修学范围的部分，笔者更是期待着各位读者朋友的指教。一本书的出版凝聚着许多人的共同劳动。清华大学出版社的责任编辑和封面设计、版式设计的各位老师，从书的选题、章节的编排、内容的取舍、读者群的定位，以及版面的安排一直给了笔者宝贵的指导。书中的不少技术内容和观点也来自许多学者的辛勤科研成果。笔者在本书的参考文献中，虽尽可能详细地开列了原文出处，但参考的资料实在太多，未能一一详列。海峡两岸笔者曾一起共同工作的许多同事，都在百忙中对笔者的求助有求必应。在此，笔者很恳切地向各位师友致以衷心的谢忱。

结束本序之际，谨允许笔者转录常置于笔者案头的警语：“第一次世界大战是化学家的战争；第二次世界大战是物理学家的战争；第三次世界大战，如果不幸发生的话，将是数学家和信息学家的战争。”生活在信息时代的每一个热爱和平的人，都不能不严肃地自问：对于已经出现在我们身边的信息战，我们了解了多少？我们准备好了吗？

作　者

2003 年 9 月于美国加州硅谷

CONTENTS 目录