网络对抗

NETWORK WARFARE

刘锋 李志勇 陶然 王越 编著

国防工业出版社
National Defence Industry Press
http://www.ndip.com.cn

网络对抗

NETWORK WARFARE

刘锋　李志勇　陶然　王越　编著

国防工业出版社

·北京·

图书在版编目(CIP)数据

网络对抗/刘锋等编著 .—北京：国防工业出版社，2003.1

ISBN 7-118-03023-6

Ⅰ.网... Ⅱ.刘... Ⅲ.计算机网络－安全技术 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字(2002)第 086482 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 22¼ 511 千字

2003 年 1 月第 1 版 2003 年 1 月北京第 1 次印刷

印数：1—4000 册 定价：30.00 元

内 容 简 介

网络对抗是信息战的全新领域，受到世界各国的高度重视。国内某些院校已获准开设网络安全对抗工程专业。

本书共分 6 章。第 1 章“绪论”介绍网络对抗的发展、国内外现状和网络对抗的组成及其特征。第 2 章“网络对抗基础知识”介绍计算机、通信、计算机网络三方面的相关知识。第 3 章“网络防御”从网络拓扑结构、操作系统、应用程序、数据、人员五个方面全面分析如何进行网络安全防御。第 4 章“网络进攻”介绍渐进式攻击的各个步骤、方法及相关技术。第 5 章“病毒武器”介绍病毒的实现技术，分析了多种典型病毒。第 6 章“网络对抗发展趋势”从各种新技术的应用和网络技术的发展论述网络对抗的发展趋势。

本书是从事网络安全防护人员和网络安全产品开发人员的必备参考资料，也可供广大计算机网络爱好者参考学习，并可作为高等院校网络对抗专业本科生、研究生的教学用书。

序　言

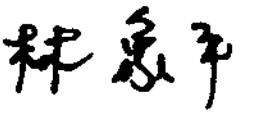
网络对抗是一个全新的研究领域。20世纪90年代，各国对该领域的研究工作十分重视，且投资力度很大，近年来，网络对抗理论与技术得到了迅猛发展，并在军事和民用信息领域得到广泛应用。网络对抗技术成为保障国家信息基础设施和国防信息基础设施安全运行的必要手段，也是军事上C^4ISR（指挥、控制、通信、计算机、情报、监视、侦察）系统的核心技术。

在美军内部，有一种强烈的倾向，认为网络攻击手段属于大规模毁灭性武器，并称“美国核力量的基本任务是遏制大规模毁灭性武器的使用”，俄罗斯则在军事学说中已经将这种手段视为可以利用大规模毁灭性武器或核武器进行反击的先决条件之一，足见美、俄已把网络进攻认定为极具威力的武器。

本书作者在国内较早地开展了网络对抗领域的研究工作，并在网络防御、网络进攻以及网络病毒武器三个方面，开展了一系列研究课题，取得了一些研究成果。在网络对抗体系构成、网络安全组网、网络口令破解、渐进式网络进攻以及典型病毒程序设计方面均有独到见解。

本书内容是作者多年来在网络对抗领域所取得的研究成果的提炼，涵盖了网络对抗各个方面，相信本书将对我国的网络对抗研究工作能起到一定的积极作用，对我国的网络对抗专业建设和学科发展具有一定的指导意义，同时为广大计算机网络爱好者提供了一本有价值的参考书。

著名电子对抗专家



前　言

信息战主要包括“电子战”和“网络战”两个方面。电子战是信息战的核心内容，网络战是信息战的全新领域，网电一体战是信息战的发展方向。

网络战实施的环境主要为作战指控网和民用网（主要为国际互联网），本书仅介绍基于民用网的网络对抗。

国际互联网已成为各国接入“信息高速公路”的纽带，在世界各国迅速发展，从而涌现了大量基于国际互联网的应用和服务，这些服务以网络的形式深入到千家万户，其安全性越来越引起人们的高度重视，如何增强网络安全防御是本书介绍的内容之一。

网络已从最初的军事防御发展成为军事攻击的重要目标。网络进攻是信息战的重要进攻手段，在各国竞相开展网络对抗研究的背景下，从事网络对抗的相关人员掌握网络进攻技术是必要的。本书较全面地介绍了网络进攻技术。

“知己知彼，百战不殆”，网络防御与网络进攻作为矛盾的两个方面必须全面掌握才能相辅相成，相互促进。对网络防御的点、面、体要充分防范可能的入侵，利用网络进攻方法检测自身网络安全性；网络进攻的立足点在于错综复杂的网络不可能天衣无缝，随着新技术、新工具的应用，过去安全的现在不一定安全，网络安全管理工具同样能为进攻提供信息。网络对抗技术的研究，其中网络安全防御技术对军事、民用网络的安全组建和防范具有重要的指导意义。

网络对抗是信息战的全新领域，受到世界各国的高度重视。国内某些院校已获准开设网络对抗工程专业。本书涵盖网络对抗各个方面。

本书共分六章。第 1 章介绍网络对抗的发展、国内外现状和网络对抗的组成及其特征。第 2 章介绍网络对抗基础知识。第 3 章介绍网络防御技术。第 4 章介绍网络进攻技术。第 5 章介绍病毒实现技术。第 6 章论述网络对抗发展趋势。

本书是从事网络安全防护人员和网络安全产品开发人员的必备参考资料，书中进行的网络攻防测试对未来的信息安全产品开发具有重要的指导意义。可作为网络对抗专业本科生、研究生的教学用书。

本书在写作中参阅了许多网络资料，其中有知名网络安全公司网站、网络安全专家的个人网站和一些院校的留言板系统中所公布的网络漏洞材料与技术文档。在此向这些公司和人员的帮助表示感谢。本书的编写得到了我国著名电子对抗专家林象平教授的鼓励和支持，林教授在百忙中对书中内容进行了审阅、修改。北京理工大学齐林博士、王玲博士、赵兴浩博士、党华硕士分别对本书的有关章节进行了认真仔细地校对与修改。另外对本书的编写工作提供帮助和支持的还有西安电子科技大学赵国庆教授，北京理工大学周思泳教授，信息产业部53所王铁红总工程师，海军司令部孟涛、李伟以及海军航空工程学院秦兰悦、徐一天、孔民安、王宝林、陈铁柱、许柯文、刘强等领导和同事，在此一并表示感谢。

本书所提供的网络进攻方法和计算机病毒的实现方法具有一定的破坏性，读者在使用时必须遵照国家有关法律规定，否则责任由使用者自负。网络安全工作人员了解这些方法则有助于改进自身系统，加强安全防范。

由于笔者水平有限，加之时间仓促，书中难免有不当之处，敬请广大读者提出宝贵意见。

编　者

2002年10月

目　录

第1章 绪 论

1.1 引 言

20世纪90年代，以Internet为代表的计算机网络技术突飞猛进，并在军事和民用信息领域得到广泛应用。计算机网络已成为国家信息基础设施和国防信息基础设施，也是军事上C^4ISR（指挥、控制、通信、计算机、情报、监视、侦察）系统的基础。由于计算机网络在国防和民用的各个方面发挥着举足轻重的作用，因此各国在竞相发展计算机网络的同时，也十分注重来自网络的“入侵”与破坏，而在军事领域，对这一阵地的角逐越来越剧烈，并且已从理论走向实战。

1997年，美国海军提出了“IT21”（21世纪信息技术计划），即将指挥、控制、通信、计算机、情报、监视和侦察设备纳入一个统一的、可扩展的网络，为所有的海军和联合部队提供实时、高速、宽带的信息服务，其核心就是网络中心战，即利用强大的计算机网络将分布的各种探测装置、指挥中心和武器融合成统一、高效的大系统，实施战场信息和武器的共享、联合、协同作战，对目标进行更快、更强、更有效的连续打击。美国海军称“从平台中心战转向网络中心战是一个根本性的转变”，并称其为两千年来军事领域最重要的变革。在1998年12月的“沙漠之狐”行动中，装备有“IT21”的“企业”号航空母舰战斗群借助卫星和Internet进行通信联络和传达作战指令，使每个作战平台都能参加作战方案的实时决策。

网络中心战是通过强大的网络把具有信息优势的、地理位置分散的部队连接在一起形成战斗力的战争。美国国防部正在制定网络中心战的基本框架。其作战模式已写入1996年美参联会主席颁发的《2010年联合构想》（JV2010）中，并且JV2010的作战概念将以网络中心战为特征。网络中心战是利用网络将C^4I系统和各个作战平台火力融合，然而要将不同时期研制的C^4I系统实现互联通信、控制决非易事。网络越庞大越复杂其所存在的漏洞也就越多，且在后期的使用中人们不断发现一些网络技术的缺陷。网络技术日新月异，不断推陈出新，而对于复杂的大系统来说要对其硬件、软件进行升级换代却是十分缓慢的，许多人皆知的漏洞和后门至今还存在于网络系统中。另外，由于网络互联，也就使得来自世界的任意角落、任意时刻的网上入侵都成为可能。网络越发达，对网络的依赖程度性越强，网络的安全和防御也就越重要，同时对其进行的网络攻击所造成的干扰和破坏也将越大。

近年来，“电脑黑客”、计算机病毒受到了各国军方高度重视，它在军事领域的应用也已从理论走向实战。现代科学技术日新月异，武器系统和作战指挥系统自动化、数字化使计算机技术在军事上得到了广泛应用，而战场的复杂性、变化性使作战中急需实时

快捷地了解战场势态，掌握敌方举动，从而计算机网络作为快速、高效的传输手段在军事、民用信息领域中得以广泛应用。并且由网络终端、计算机控制的传感设备武器系统能在空间完成采集目标参数、解算目标轨迹、判断武器攻击的最佳时刻和地点并控制武器射击，而经过联网之后多兵种可相互协调、配合，多种不同武器系统可完成集中攻击和火力分配。计算机网络在军事领域的广泛应用将实现总体力量的集成，可使各种武器平台的作战效能成倍的提高。20 世纪 90 年代，通信网络技术与计算机技术的相互融合、广泛应用，使以单个平台为中心进行的处理转向利用整个网络环境进行处理，“网络中心战”的概念被提出，并在美国开始实施、应用。

随着对通信网传输、交换和终端设备的深入研究和高速开发应用，以及网络结构、信令、编码、加密和网络管理控制等有关网络运行软件的不断完善和发展，网络的性能取决于网络中各个软、硬件因素的组合，网络中心战的概念将使通信电子战的性质和概念发生深刻的变化，通信网必须采用各种先进的技术来抗干扰，防泄密。在严密防范的同时，主动进攻技术也受到各国高度重视，并且成立了专门的研究机构对网络进攻技术进行研究。美国是最早开始研究计算机网络的国家，并且在计算机技术、计算机网络技术方面远远领先于其他国家，在网络进攻技术的研究方面，美国已开展用无线电、卫星辐射的注入方式、网络连接注入方式把计算机病毒植入敌方计算机主机、各类传感器及网桥中的研究，以伺机破坏敌方的武器系统、指挥控制系统、通信系统等高敏感的网络系统。随着高科技在军事领域的应用，未来的计算机技术将应用于每一个单兵系统中，许多的战术决策、武器控制将通过计算机输入指令完成，因此计算机网络上的对抗将会成为战争的重要组成部分。

到目前为止，尚未有真正意义的军事网络进攻的战例，大多网络入侵事件都是民间自由网络“黑客”所为。据美国信息局估计，1995 年 DOD 的网络系统就遭到二十多万次的攻击。美国联邦调查局估计计算机网络攻击造成的损失每年高达 100 亿美元。1999 年 4 月，一个黑客组织称已通过 Internet 控制了英国的一颗军事卫星，并提出金钱讹诈，尽管英国军方否认，但当时，这颗卫星确实不能正常工作。科索沃战争爆发后，南联盟与美国的黑客在 Internet 上进行了“混战”，美国白宫、北约总部的网站均被攻击。美国国防部称其网站仅四月份就遭到全球 15 个地方的黑客攻击。在网络攻击中以计算机病毒的危害性最大，自 CIH 病毒出笼以来，首次制造计算机病毒对计算机硬件的破坏，1999 年 4 月 26 日 CIH 病毒在世界各国大规模发作，许多计算机的硬盘、BIOS、主板遭到严重毁坏，造成的损失是前所未有的，使得许多的计算机用户谈 CIH 色变，每逢 26 日都不敢开机。除了计算机病毒，世界各国还活跃着一批计算机编程高手，他们对计算机的软件、硬件十分精通。为了炫耀或为了达到某种目的，他们利用软件、硬件的漏洞和网络管理人员的疏忽，编制了各种网络程序，并通过 Internet 广泛传播。今天在 Internet 上，即使是初中生都能轻易获得一些高效的、操作简单的入侵程序。关心每天的报道，人们就会发现计算机网络攻击事件越来越多。在 Internet 上还有一大批计算机网络高手，他们相互交流入侵技术和“战果”，并且诸如美国联邦调查局、中央情报局、军方等在网络安全方面进行层层防范的机构都频繁受到来自 Internet 的攻击。在 20 世纪与 21 世纪交替之际，美国军方等机构为防范黑客利用系统千年计时的缺陷而入侵，相继关闭了一些站点，就在 21 世纪刚开始不久，2000 年 2 月 16 日雅虎的网站遭到攻击，并被迫关闭 3 小时。

第二天，电子零售商 Buy.com 公司在宣布公开上市数小时后也遭到了攻击。当天晚上，eBay 公司、亚马逊公司和有线新闻电视公司（CNN）的网站全部瘫痪，像这类的网络攻击事件再一次向世人敲响了警钟，计算机网络安全不容忽视。

目前，任何一个国家的军事力量都无法与美国抗衡，美国拥有大批的先进战斗机、舰船和精确制导武器，直接在战场上与美国这样的强敌进行抗击是十分艰难的。然而尽管美军在常规高技术武器方面占有绝对优势，但在网络技术方面的情况却有所不同，网络战将是极少数能对美国构成重大威胁的作战手段之一。通过计算机网络或其他途径进行极具隐蔽且不留痕迹的攻击将是一种十分有效的进攻手段，在技术研究方面尽管美国有运行速度最快的计算机，但军方使用的计算机多是 1995 年以前的产品，并且在今后很长的一段时间内将继续使用，而这些计算机的性能已远落后于民用的最新体制的计算机。尽管美国开发了许多加密技术、防火墙，但依然能被一些精明的黑客攻破，并且以 Internet 为渠道，许多美国的领先技术同样可被其他国家分享，例如在加密方面，非常著名的加密程序 PGP，其版本是在美国保密机构中专用且被禁止出口的，但在一些黑客站点依然可以获得。作为单个或某一小组的网络入侵群体，可紧跟时代技术的发展，采用最先进的计算机、高速的连接设备和先进的技术武装自己，而庞大的军事网络更新的速度却十分缓慢。

计算机网络对抗包括防御和进攻两个方面，这二者是矛盾的两方面，相辅相成、互相促进。正因为计算机网络中存在安全漏洞才会遭到网络攻击，因而有必要采取有效的防范措施。而网络进攻以其潜在的巨大破坏性将与网络防御进行长期的、针锋相对的对抗。

1.2 信息时代的网络战

信息是对客观物体动能相互关系紧密变化的描述，信息可以用文字、语言和图像、数字、符号等来表示，利用光盘、磁盘、纸张来记录，利用声波、光波、电波和其他交通工具来传送，信息以及根据信息而提出的情报是指挥决策的基础，也是武器控制的前提。“知己知彼，百战不殆”是古人对信息在战争中所起的巨大作用的总结。现代战争不仅有军事武器的对抗，同时也包括对信息、战场局势掌握情况的对抗。在现代战争中，对信息的利用和依赖更加突出，信息在战争中所起的作用更加显著。网络战进攻的直接目标就是敌方的信息和通信系统，包括干扰、截获和破坏，其目的是通过网络尽可能地了解敌方的一举一动，通过攻击敌方重要的数据库，而使之出现紊乱或者伺机获取口令，进而加入假信息或获得设备控制权限进行毁坏性操作。

为迎接信息化战争的到来，各国开发研制了各种信息化作战武器，如预警机、电子战飞机、对敌防空压制飞机、电子侦察卫星、反辐射导弹、机载自卫电子战系统以及电磁炸弹和石墨软炸弹等。这些信息武器各自只能完成单一的信息收集处理或信息干扰、作战指挥等，而计算机网络战却是攻防一体、作战方式灵活、隐蔽多样。

随着信息时代网络化的发展，网络对抗将作为全新的战场展现于世人面前。目前世界各国正在加紧对网络方面的研究，准备迎接网络战争。

1.3 网络对抗体系

1.3.1 网络对抗的组成

网络对抗主要包括网络防御、网络攻击两个部分。网络对抗研究的网络模型基于以下三种：

1. 完全独立的局域网

许多的网络攻防技术可以在这一环境下进行测试，如系统漏洞，口令破解等，所以这一模型是研究网络攻防技术的主要平台。在下面的实验网络构建中将具体给出这一平台上要进行的实验。

2. 通过防火墙接入 Internet 网络

这一模型是目前各大单位、公司和院校接入 Internet 的主要方法，其攻防重点在于内部网络与 Internet 连接的接口部分的安全防范和突破，如图 1.1 所示。

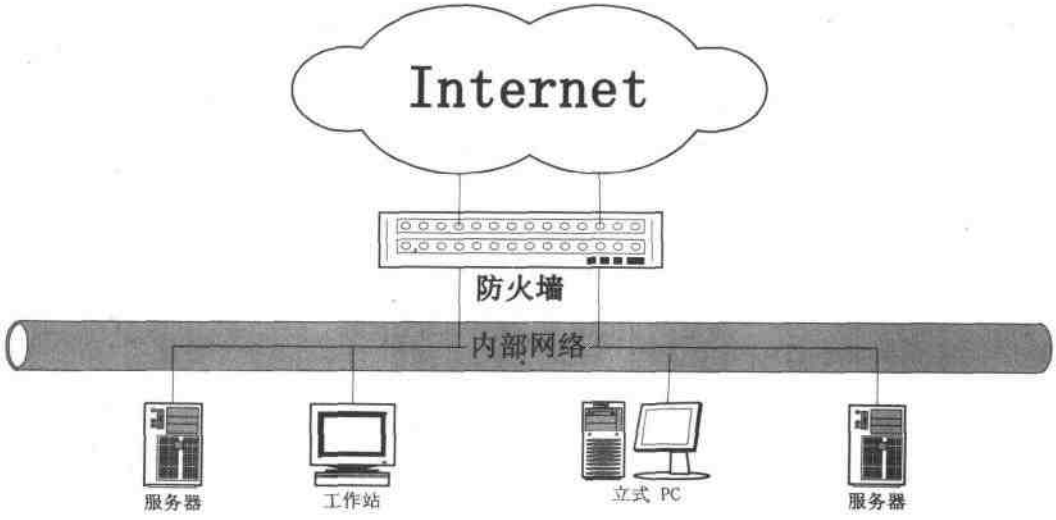


图 1.1 通过防火墙接入 Internet 的网络

3. 与 Internet 存在离散连接的独立的网络

在这一模型中内部网络每一时刻都没有与 Internet 直接连接的物理链路，但是内部网络与 Internet 网络之间存在若干台游离的主机，这些主机有时接在 Internet 上，有时接入内部网络，则可认为在一段时间内内部网络与外部的 Internet 存在微弱的连接。这一模型的提出主要目的在于为攻击独立的内部网络寻找突破口和可攻击物理链路。在这一模型中要对内部网络进行探测，则需借助这些游离的主机，当游离主机接在 Internet 网络时，对其攻击并注入后门和病毒，当游离主机接入内部网时，病毒对内部网络进行探测并传播、扩散，当游离主机接回 Internet 时，它将搜集、窃取的信息传到指定地点。其攻击的难点在于搜索并确定游离的主机，注入游离主机的病毒应具有相互协调功能，且应尽快将信息反馈，如图 1.2 所示。

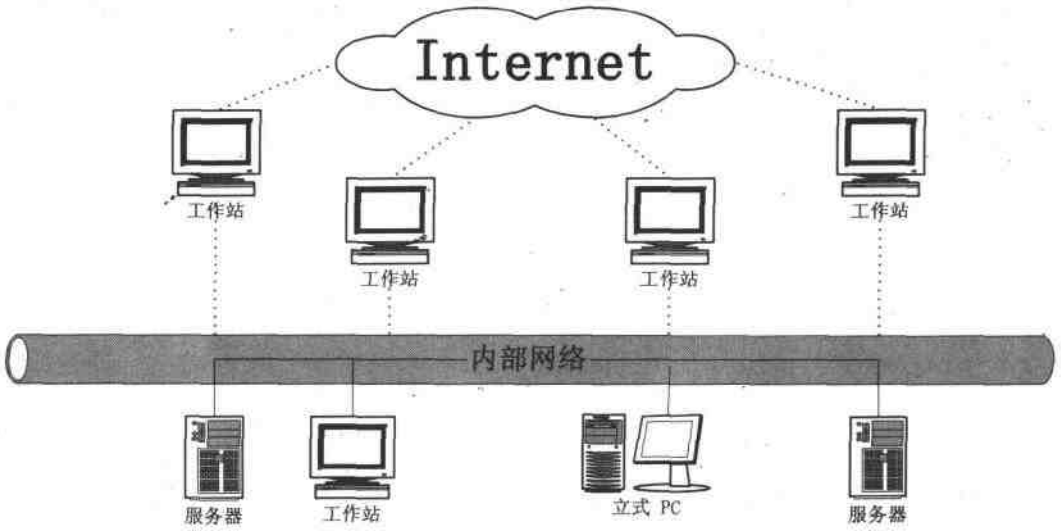


图 1.2　与 Internet 存在离散连接的独立的网络

1.3.2　网络对抗内容体系

网络对抗应从三个方面开展研究：网络防御、网络进攻和计算机病毒武器。详细的体系结构如图 1.3 所示。

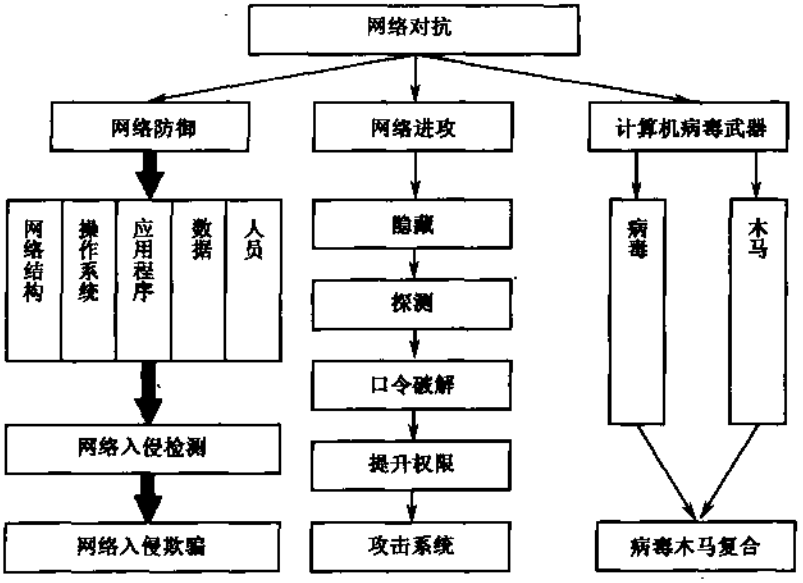


图 1.3　网络对抗内容体系

1.3.3　网络防御

网络防御要做到面面俱到，国际著名的网络安全公司 Hurwitz Group 在经过系统科学的研究分析后，得出以下结论。在考虑网络系统安全问题时，应全面考虑以下五个方面：