协同式网络对抗

卢 昱等著

国防工业出版社

本书得到总装备部“1153”人才工程专项经费资助

协同式网络对抗

卢昱　林琪　李津军　王宇
张建伟　张伶　罗小明　著

国防工业出版社
·北京·

图书在版编目(CIP)数据

协同式网络对抗/卢昱等著. —北京:国防工业出版社,2003.8
ISBN 7-118-03234-4

Ⅰ.协… Ⅱ.卢… 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(2003)第 067680 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)
国防工业出版社印刷厂印刷
新华书店经售
*
开本 787×1092 1/32 印张 11 281 千字
2003 年 8 月第 1 版 2003 年 8 月北京第 1 次印刷
印数:1—4000 册 定价:25.00 元

前　言

在人类战争史上，科学技术的进步和战争工具的发展始终是战争演变和发展的重要动力。正是在科学技术进步的推动下，人类的战争空间才不断地扩展，逐步从陆地扩展到海洋，由陆地延伸到空中，再到太空；由有形战场变化到无形战场。而战争空间的每一次拓展，都带来了战争形态和方式的崭新变化。随着计算机和通信技术的发展，计算机网络的触角已伸向了地球的各个角落，对人们的生活方式和工作方式产生着前所未有的影响，它在改变人类社会生产和生活方式的同时，也在改变着人类战争的形态和方式。事实上，网络空间从开始形成之日就不太平，网络对抗一直伴随网络发展的整个过程。计算机网络是连接未来信息化战场的枢纽，是实现 C^4I 系统和陆、海、空、天一体化的数字化战场的基本保证。研究与发展计算机网络对抗能力，是各国争夺制信息权的竞争焦点，也是获取信息优势的必要手段和途径。在未来高技术战争中，交战双方在信息领域的斗争将空前激烈，争夺信息优势、取得制信息权已经成为作战的重心。

所谓计算机网络对抗，就是采取各种手段侦察、渗透、摧毁和破坏敌计算机网络系统，使其瘫痪，阻止敌战场信息的获取、传递与处理流程，使敌丧失指挥控制能力，同时对我计算机网络实施整体防护，保证我战场信息流畅通的一种作战样式。网络是一个巨大、分散而复杂的人机系统，在这种分布的环境下，单独的网络攻击、网络防护和网络控制行为都难以满足现代战争的要求。网络攻击需要协同，网络防护需要协同，网络控制需要协同，攻击和防护之间需要协同，天地一体化的数字化战场也需要协同，协同是未来网络对抗的发展趋势。应该看到网络对抗离我们并不遥远，对

协同式网络对抗和控制技术以及网络战装备的研究迫在眉睫。这就是我们编著此书的目的。

我们认为:网络对抗包括进攻性行为、防御性行为和支持性行为,并有一套与之相对应的模型体系、技术体系、能力体系和装备体系。本书以协同式网络对抗为主线,融入了近年来作者在网络对抗领域大量的研究成果。本书对协同式网络对抗进行了全面的描述,不仅从理论角度介绍了网络对抗的相关概念和技术基础,提出了攻防协同的网络对抗和天地一体化的协同式网络对抗概念,而且从实践角度提出并设计了协同式网络攻击模型和协同式网络防护模型,并对模型实现进行了研究。

本书论述了空间信息网络的组成及对抗途径,讨论了空间信息网络的安全体系结构、自主安全模型和安全通信等相关内容,并首次提出了基于空间信息网络支持的协同式网络对抗模型。另外,本书首次提出了网络控制论概念,并对其系统分析方法和控制方式、网络控制论系统和模型建立以及协同式网络控制等相关技术进行了介绍和论述。本书还首次提出了网络战装备的概念及体系结构,并提出了网络战装备作战手段体系、网络战装备能力体系和网络战装备技术体系的概念,构建了一个比较系统的、多层面的网络战装备体系。

全书由卢昱确定结构大纲和主要内容,并撰写了第 2 章、第 8 章、第 9 章、第 10 章和第 11 章。绪论和第 1 章由张建伟撰写,第 5 章和第 7 章由王宇撰写,第 4 章和第 6 章由林琪撰写,第 3 章由李津军撰写,张伶参与了第 3 章、第 5 章和第 7 章部分内容的编写,罗小明参与了第 2 章部分内容的编写。全书由卢昱统稿并最后定稿。朱代祥、张晖、王晓云、李勇奇、卢鋆、吴忠望、朱涛江、杨健康、顾丽娜、张莹等也为本书的完成做出了贡献。

全书充分考虑了内容的系统性和完整性,特别突出了协同式对抗技术和攻防模型的实用性,能用作从事网络信息技术的科研人员和相关行业技术人员、管理人员的参考书,同时还可作为计算机网络信息安全专业或相近专业本科生和研究生的教科书。

本书是总装备部“1153”人才培养工程首批资助出版的我国第一部系统论述协同式网络对抗的学术专著。初稿完成后，组织了国内相关领域的专家对书稿进行了评审，专家对本书的评价很高，认为该专著总结了协同式网络对抗所涉及的关键技术和装备，构建了协同式网络对抗理论体系框架，填补了协同式网络对抗研究领域的一项空白，富有开拓性和创新性。根据专家的建议，压缩了初稿的技术基础部分，突出了协同式网络对抗这条主线和相关内容。由于网络对抗涉及的内容范围较广、技术较新，网络控制论的研究还处在起步阶段，对网络战装备的概念和体系结构的分析尚处于探讨阶段，本书不足之处在所难免，恳请广大作者和专家批评指正。

内 容 简 介

计算机网络是连接未来信息化战场的枢纽，是实现C^4I系统和陆、海、空、天一体化的数字化战场的基本保证。研究与发展计算机网络对抗能力，是各国争夺制信息权的竞争焦点，也是获取信息优势的必要手段和途径。

本书以协同式网络对抗为主线，融入了近年来作者在网络对抗领域大量的研究成果。从理论角度介绍了网络对抗的相关概念和技术基础，提出了攻防协同的网络对抗和天地一体的协同式网络对抗概念。从实践角度提出并设计了协同式网络攻击模型和协同式网络防护模型，并对模型实现进行了研究。论述了空间信息网络的组成及对抗途径，讨论了空间信息网络的安全体系结构、自主安全模型和安全通信等相关内容。

本书首次提出了基于空间信息网络支持的协同式网络对抗模型。首次提出了网络控制论的概念、系统分析方法和控制方式，以及网络控制论系统和模型的建立。首次提出了网络战装备的概念及其体系结构，构建了一个比较系统的、多层面的网络战装备体系。

本书内容翔实、例证丰富，涵盖了网络对抗需要的“攻、防、测、管、控、评”等多方面的实施技术，对相关人员研究网络对抗技术有重要的参考作用。本书也是总装备部“1153”人才培养工程首批资助出版的我国第一部系统论述协同式网络对抗的学术专著。

目　录

第 2 篇 协同式网络攻击

第3篇　协同式网络防御

绪　论

1993年美国国际战略研究中心组织近百名专家经过半年的研究后，提出一份名为《军事技术革命：一种结构框架》的研究报告，明确提出了“信息革命是军事技术革命的核心，军事学说和军队编制是军事技术革命的重要组成部分”的观点。1993年托夫勒的《战争与反战争》军事未来学新著以及他的“第三次浪潮”理论使美国军队领导人相信：由于利用各种信息，战争正在以一种与过去完全不同的方式进行，正在到来的信息时代将引发一场真正的军事革命，各国军队必须追赶第三次浪潮，用新思维谋划21世纪的战争。于是，“信息战”一词开始广泛用于表达一种作战样式，同时信息战成了军事理论创新的核心与焦点。可以断言，21世纪的战争将是一场别开生面的信息对抗。

1. 信息对抗的概念

有关战争的概念体系大致划分为战争形态、作战样式、作战行动3个层次，在介绍信息对抗的有关概念之前，先简单介绍一下分属3个概念层次的术语：战争、战和作战。

战争(War)——作为解决争端的非政治、外交途径，是人类冲突的最高表现形式。战争标志着政治、外交努力的失败，通常是竞争和有限冲突逐步升级的结果。

战(Warfare)——战争有多种形式或样式，叫做战争样式，有时亦称作战样式。各种具体的战争样式或作战样式称为“战”。例如，以作战空间来划分有空战、陆战、海战、空地一体战等；以战争样式或作战样式的某种特点(手段、方法、对象)来划分有消耗战、阵地战、运动战、闪电战、持久战、游击战、信息战等。

作战(Operations)——也称作战行动，指战争中为遂行战争任

务、达到战争目的而采取的连续性军事行动。

与信息对抗相对应的3个层次的概念可以用信息化战争、信息战、信息作战来描述。

信息化战争(Information War)——亦称信息战争或信息时代战争,是信息时代的一种战争形态或战争类型。信息化战争就是将作战中各个环节都予以信息化,再用一个完善的信息指挥控制系统对各种信息化了的资源予以优化,以取得最优的效能。信息化战争是在信息技术高度发展并广泛应用于军事斗争之后而诞生的一种新型的、充分利用信息资源的、越来越依赖于信息的战争形态。

信息战(Information Warfare)——美国国防部将信息战定义为:为保护己方信息系统的完整性,免遭敌人利用、扰乱和毁坏,同时又要利用、扰乱和摧毁敌方的信息系统和信息处理过程,以便获得兵力运用上的信息优势而采取的一系列行动。这里的信息系统是指包括人员、计算机、程序及收集、处理、存储、分发和显示信息的系统。信息处理过程包括决策过程、指挥过程、控制过程和武器运行过程等。

信息作战(Information Operations)——美国国防部将信息作战定义为:在军事信息环境中为发挥、增强和保护己方军队收集、处理信息并按照信息行动的能力,以获得在各种军事行动中的优势而采取的连续性军事行动。信息作战包括与全球信息环境的相互作用以及对敌人信息和决策能力的利用和拒止。这里所说的拒止有两方面的含义:一方面是使敌方的信息系统拒绝为其提供服务;另一方面又要阻止敌方利用己方的信息和信息服务能力。

关于信息对抗的概念众说纷纭,至今尚无定论。我们认为信息对抗可以理解为敌对双方为争夺信息空间的制信息权,综合利用以信息技术及装备为主的各种作战手段所展开的全时空信息较量的斗争。它是围绕着信息、信息处理过程、信息系统和计算机网络而进行的信息对抗,通过利用、封锁及施加影响等手段,攻击对方的国家和国防信息基础设施以及指挥控制系统,以夺取和保持