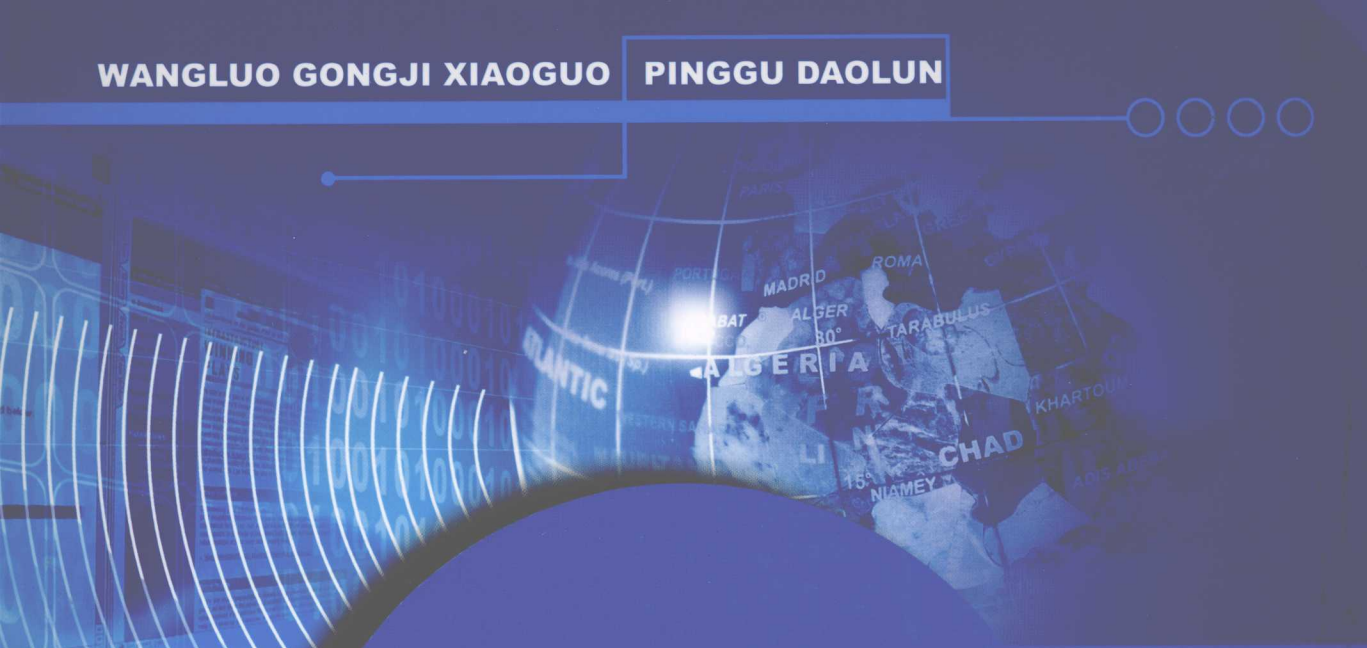
WANGLUO GONGJI XIAOGUO PINGGU DAOLUN



网络攻击效果评估导论

鲜 明 包卫东 等编著

国防科技大学出版社

网络攻击效果评估导论

鲜　明　包卫东　王永杰　肖顺平　编著

国防科技大学出版社
·长沙·

图书在版编目(CIP)数据

网络攻击效果评估导论/鲜明等编著 .—长沙:国防科技大学出版社,2007.3
ISBN 978-7-81099-410-1

Ⅰ.网… Ⅱ.鲜… Ⅲ.计算机网络—安全技术—评估 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2007)第 022304 号

国防科技大学出版社出版发行
电话:(0731)4572640 邮政编码:410073
http://www.gfkdcbs.com
责任编辑:徐 飞 责任校对:耿 筠
新华书店总店北京发行所经销
国防科技大学印刷厂印装
*
开本:787×1092 1/16 印张:16.25 字数:356 千
2007 年 3 月第 1 版第 1 次印刷 印数:1-2500 册
*
ISBN 978-7-81099-410-1
定价:38.00 元

前　言

随着信息技术的发展，网络已成为全球信息基础设施的主要组成部分，给人们的生活、工作和人与人之间的沟通带来了极大的方便，人们可以通过网络购买定制产品，实现企业的资源共享，进行远程教育等等。网络为现代人类生活质量的提高带来了深刻影响，并促进了科学、技术、文化、教育、生产的发展；但由于网络本身具有开放性、互联性和联结形式多样性、终端分布不均匀性等特征，致使网络面临很多潜在的安全威胁，容易受到黑客、恶意软件和其他不轨行为的攻击；因此，网络实际上是一把双刃剑，在推动人类进步的同时，也给保障社会和国家安全带来了极大的挑战。网络的安全不仅关系到战争的胜负、国家的安危、科技的进步、经济的发展，而且也关系到每个人的切身利益。

网络安全是一个复杂的学科，它综合利用了数学、物理、生物、通信技术和计算机技术等诸多学科的基础理论和最新发展成果；网络信息安全又是一门发展迅速的年轻学科，没有长期深入的研究和实践就不可能全面理解和掌握网络信息安全的理论与技术。开发网络安全防护系统需要首先了解网络攻击的手段和系统暴露的问题，其研究是网络安全工作中不可缺少的一个环节，对于透彻理解网络安全问题的本质有指导意义，也为研究信息系统安全的技术手段提供了依据。由于网络攻击紧密围绕着网络协议和信息系统进行，所以网络协议和信息系统的架构和运行机制决定着攻击行为的具体形式。Internet 上的网络协议和信息系统多种多样，各自有着不同的服务目的和架构，它们的多样性决定了网络攻击的多样性。网络攻击的研究实际上是构建网络安全系统的前期工作，它为进行更加深入的研究与开发提供了一个基础平台。本书关于网络攻击效果评估的研究就是对主机系统安全防护技术的试探性研究工作，它也为将来的深入研究提供技术思路和参考。

全书从理论和技术两个方面对网络攻击效果评估进行全面和系统介绍，可以作为高等学校信息安全、信息与计算科学、通信与信息系统、计算机软件与理论、计算机应用技术、军事通信学等专业研究生的教学参考书，也可作为相关领域科技工作者的实用工具书或技术培训教材。其中第1章、第7章、第9童、第12章由鲜明编写，第2章、第4章、第11章由包卫东编写，第5章、第6章、第10章由王永杰编写，第3章、第8章由肖顺平编写，全书由鲜明统稿。

本书是国防科技大学相关课题组全体成员多年来集体智慧的结晶。在写作过程中张义荣博士、胡影博士、博士生解文斌、博士生江亮、博士生王会梅、王晖硕士、邹芳硕士、吕金刚硕士、硕士生袁爽、硕士生汪莉莉等为本书提供了丰富的资料和相关工作支持。本书写作过程中还得到蒋兴才教授、张权副教授、王伟副教授、马双双副教授、周丰副教授、刘忠副教授、黄惠女士等的帮助，在此一并表示感谢。本书也是国家自然科学基金项目（批准号：60372039）和国防科技大学基础研究项目（批准号：JC04-04-13）的成果总结。

由于作者水平有限，书中难免出现各种失误和不当之处，恳请读者和各位专家给予批评指正。

作　者

2007年1月

目　录

第一章　绪　论

第二章　评估的数学基础

第三章　网络信息系统安全与风险评估

第四章　网络攻击及其分类技术

第五章　网络攻击建模与仿真技术

第六章　网络攻防过程的博弈模型

第七章　网络攻击效果评估指标体系

第八章　基于移动 Agent 的评估指标采集方案

第九章　网络攻击效果评估模型

第一章 绪 论

1.1 引 言

随着信息技术的发展和广泛应用，人类进入了信息时代，信息已成为与材料和能源同等重要的战略资源，是重要的财富和资产，是这个时代最活跃的驱动因素。这种时代特征突出地表现在对信息资源的掠夺和垄断上，信息技术的先进与落后，信息资源的多少以及知识产权的拥有量已成为比较各国技术力量和综合国力的重要指标。国家安全的争取和维护历来同人类科学技术的发展与进步密切相关，以信息技术为核心的新技术革命对传统国家安全观念产生了深刻的冲击。在信息时代，国家安全的概念不仅只是维护国家主权与领土完整，也不仅存在于军事领域，还存在于经济、社会、科技等其他领域，信息网络技术的发展和应用对传统的国家安全概念产生了巨大挑战。信息安全已上升为一个事关国家政治稳定、社会安全、经济有序运行的全局性问题。

计算机网络是通过通信线路互连起来的自治的计算机集合，是信息时代最标志性的产物。20 世纪 90 年代以来，计算机网络技术得到了飞速发展，计算机网络已由单个的局域网发展到目前的跨区域的、国际性的计算机网络，成为能够相互通信、资源共享、任务分布式处理的高性能的计算机网络，即国际互联网，又称因特网（Internet）。当前，互联网的开放性、共享性、互连程度不断扩大，互联网已经深入到了社会的各个领域，如政府部门、军事领域、教育研究机构、企事业单位等，使得网络的重要性及其对社会的影响越来越大，日益成为人们进行信息交换的主要手段。网络信息系统已经成为一个国家、一个机构不可缺少的信息基础设施。随着网络的飞速发展和广泛应用，计算机网络的资源共享进一步加强，人们在享受互联网带来的丰富信息、巨大便利的同时，也面临着网络安全的威胁。对于一个国家来说，没有网络安全，信息基础设施的安全就无从谈起，更没有网络空间上的国家主权和国家安全。以平台为中心的计算正在向以网络为中心的计算转移，这一转变不仅为商业发展提出新的竞争动力，而且也为军事变革注入了新的动力。以网络为中心，利用强大的信息基础网络，收集、处理、分发战场信息，实现信息共享，获取信息优势，并最终将信息优势转化为知识优势和决策优势，从而达

到快捷的指挥速度、超强的打击能力和最小的伤亡，提高作战效能，已成为各国军方、工业界和学术界的共识。

现代战争中，计算机与网络已成为武器装备系统和作战指挥系统的核心工具，对军用计算机信息系统进行攻击，往往能发挥其它武器系统难以起到的独特作用。因此以军用计算机网络为基础的信息安全防护和对抗问题，就自然成为军事领域必须关注和解决的问题，计算机网络攻击战成为现代高技术条件下战争的重要作战样式之一。计算机攻击网络技术就是要研究在信息战过程中，如何有效地突防敌方的军事网络，获取重要的军事信息，利用网络达到打击敌方的目的，同时不断研究新的网络防护技术、安全保障模型，使其服务于己方网络信息系统，防止敌方利用网络对己方军事目标实施攻击。网络攻击技术是网络环境下信息战的核心手段，谁能在网络战对抗中占据信息控制的优势地位，谁就能在未来的信息战中处于主动。世界各国都已经意识到了网络对于国家安全所蕴涵的巨大战略潜力，纷纷采取措施，努力加紧本国信息网络的攻防对抗能力建设，以求占得先机[1]。网络战已不再仅仅是一个虚无的概念，正实实在在地向人类社会走来[2]。美国智库兰德公司进一步提出了“战略战”的概念，认为战略战是一种破坏性极大的“顶级”作战形式，它实施的成败关系到国家的安危与存亡。兰德公司指出，工业时代的战略战是核战争，信息时代的战略战主要是网络战。

美国是开展计算机网络攻防技术研究最早的国家。从 20 世纪 90 年代初期开始，美国就把计算机网络攻防技术作为一个国防高技术主题予以发展，在该技术领域，美国已经形成了相对完善的技术体系及相当的研究规模，针对计算机网络攻防技术的未来发展，美国是站在国家安全的高度予以设计与规划的，并授权美国航天司令部专门负责该项技术的发展。美军于 1996 年 7 月颁布《2010 年联合构想》[3] 和于 2000 年 5 月颁布《2020 年联合构想》[4] 两份新世纪宣言，提出了未来美军建设的总目标，以及美军在 21 世纪之初的主要发展趋势；这两份“构想”确定了美军未来 15～20 年发展的战略目标，即以联合作战为中心，发展赢得未来战争胜利联合部队应具备的能力，特别是提高信息作战的能力，而其中获取信息优势将是联合作战的主要因素。因此，美军十分重视计算机网络的攻防研究与建设，以求夺取未来信息战的主动权。在网络攻击方面，美军要求未来网络战应具备：对所需目标网络的侦察能力；灵活准确的计算机网络攻击能力；对网络攻击效果的评估能力；具备先进准确的网络攻击武器以实施对目标 100% 的精确打击，最终达成政治和军事的目的。在网络防御方面，美军要求在不远的将来要达到：完成计算机网络防护评估程序与作战指挥程序的集成；定期向有关人员提供客观、简洁的计算机网络防护情况报告；建立完善各级司令部、各军兵种和各防御部门之间的近实时的信息共享；开发完成动态绘制国防部信息系统和信息基础设施结构图的工具，其中包括关键系统对网络的依赖程度等信息，以辅助确定网络系统对完成作战任务的影响程度等。

2002 年，美总统布什签署了“国家安全第 16 号总统令”，要求美国国防部牵头，组织中央情报局、联邦调查局、国家安全局等政府部门制定一项网络战战略。2005 年 3 月，美国防部公布的《国防战略报告》[5] 明确将网络空间和陆、海、空和太空定义为同等重要的、需要美国维持绝对优势的五大空间。2006 年 2 月，美国防部公布的《四年防务评估报告》[6]，也要求美军强化网络战能力，以应对“潜在竞争对手”使用网络进行“不对称”进攻的可能。2006 年 2 月 6 日至 10 日，美国国土安全部组织了一场美国历史上最大规模的网络战演习——“网络风暴”行动。白宫、国家安全委员会、国防部、国务院、司法部、财政部、国家安全局以及联邦调查局、中央情报局等重要部门都参与其中，著名的电脑和软件公司微软、思科、Citadel 和 VeriSign 等都倾力相助。此次演习的主要目的是检验美国的公、私各部门如何应对网络黑客、竞争对手等发起的破坏性网络攻击。从军事应用的角度，网络攻击是一种十分灵活的攻击方式，它既可在平时或战时实施，又可在本国、他国甚至敌国实施；既可破坏对方的信息系统，又可以采取窃取对方情报、传播计算机病毒、散布虚假信息等形式向对方进行攻击。美国军方每年进行一次被称作是“网络防御”项目的演习，由国家安全局的电脑专家充当“黑客杀手”负责进攻，西点军校、空军学院、海军学院和陆战队学院的专业人士进行防御，以研究美军网络安全可能存在的漏洞。计算机网络攻击设备和高功率微波武器目前被视为美陆军新型“旅级作战部队”（BeT）的主要作战装备，这些作战装备是专门为下一代战争而设计的。

根据目标范围，计算机网络作战模型通常包含 4 个层次，如图 1 - 1 所示。第 1 层次，实体层次的计算机网络对抗，主要以常规物理方式直接破坏、摧毁计算机网络系统的实体，完成目标打击和摧毁任务。在平时，主要指敌对势力利用行政管理方面的漏洞对计算机系统进行的破坏活动；在战时，通过运用高技术明显提高传统武器的威力，直接摧毁敌方的指挥控制中心、网络节点以及通信信道。

第 2 层次，能量层次的计算机网络对抗，主要是敌对双方围绕着制电磁权而展开的物理能量的对抗。敌对双方通过运用强大的物理能量干扰、压制或嵌入对方的信息网络、乃至像热武器（如高功率微波武器、强脉冲武器等）一样直接摧毁敌方的信息系统；另一方面又通过运用探测物理能量的技术手段对计算机辐射信号进行采集与分析，获取秘密信息。

第 3 层次，信息层次（逻辑层次）的计算机网络对抗，主要是运用逻辑手段破坏敌方的网络系统，保护己方的网络系统的对抗。这个概念接近于美国人讲的 Cyberspace Warfare，主要包括计算机病毒对抗、黑客对抗、密码对抗、软件对抗，芯片陷阱等多种形式。他与计算机网络在物理能量领域对抗的主要区别表现在：信息层次的对抗中获得制信息权的决定因素是逻辑的，而不是物理能量的，取决于对信息系统本身的技术掌握水平，是知识和智力的较量，而不是电磁能量强弱的较量。信息层次的计算机网络对抗是网络对抗的关键层次。

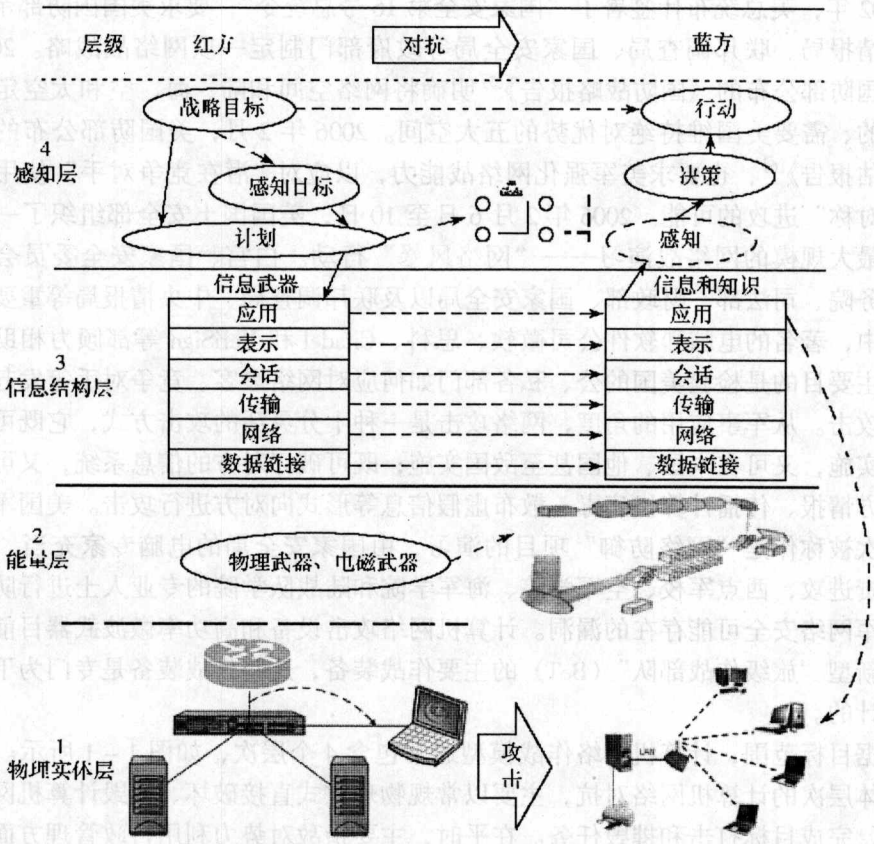


图 1-1 网络作战模型示意图

第 4 层次，感知层次（超技术层次）的计算机网络对抗。感知层次（超技术层次）的计算机网络对抗是网络空间中面向信息的超逻辑形式的对抗。网络对抗并不总是表现为技术的、逻辑的对抗形式，如国内外敌对势力利用计算机网络进行反动宣传，传播谣言，蛊惑人心，进行情报窃取和情报欺骗，针对对方军民进行心理战等，就已经超出了网络的技术设计的范畴，属于对网络的管理、监察和控制的问题。利用黑客技术篡改股市数据以及对股市数据的完整性保护属于逻辑的对抗，而直接发表虚假信息欺骗大众则属于超逻辑的对抗。后一种意义上的网络对抗瞄准了人性的弱点，运用政治的、经济的、人文的、法制的、舆论的、攻心的等各种手段，打击对方的意志、意念和认知系统，往往以伪装、欺诈、谣言、诽谤、恐吓等形式出现。

1.2 基于信息优势作战

网络作战本身并不是目的，而只是达到目的的手段，其真正价值在于实现目标，达成战略、战役或战术效果。因此实质上，基于效果作战，或者更进一步说是基于信息优势作战才是真实的目的。那么信息优势包含什么？如何来进行效果评估？就成为一体化联合作战条件下重要的理论研究课题。

信息作战是对敌人的信息和信息系统施加影响，同时使我方的信息和信息系统免受敌人影响的行动。信息优势就是指我方具有不受干扰地搜集、处理和分发信息流的能力，同时能利用和剥夺敌人的这种能力。信息优势实际上是对信息控制程度的一种描述，即指信息优势的一方，在军事中能对信息进行有效的控制而不会遭受有效的对抗。信息优势必然会创造有利条件以有利于军事力量的应用，信息优势应被看成是采取这些军事行动的前提条件。基于信息的战争，目的就是通过对信息资源的有效运用而最终实现军事上的目标，而信息优势是运用军事力量总体战略的一个组成部分。非对称性、相对性、动态性是信息优势的三大特征。

对于信息优势，美军在其 1998 年 10 月正式颁布的《联合信息作战》中明确了信息优势的定义，即信息优势是指在保持己方连续不间断地收集、处理和分发信息的权力及剥夺或压制敌方相同权力的能力。该定义包含 5 个方面的含义。

(1) 己方指挥自动化系统比敌方系统具有更实时、更准确、更有效的获取、处理、分发信息的能力；

(2) 通过对己方的信息防护，使己方保持获取、传递和使用信息的自由，使己方的整个作战系统保持快速反应的敏捷性和整体作战的协调性；

(3) 通过攻击敌方的信息探测系统，剥夺或压制敌方的信息探测能力加重敌方的“战争迷雾”，使其“耳目失聪”，无法及时、准确地了解战场态势的发展变化，削弱和剥夺其观察和决策的能力；

(4) 通过攻击敌方的通信系统和信息中心，摧毁或使敌方的指挥控制系统瘫痪，割断敌指挥系统与部队和武器系统的联系，削弱和剥夺其对部队和武器系统的指挥、控制能力；

(5) 通过对敌方的指挥自动化系统的综合性打击，瘫痪敌方的整个作战体系，粉碎敌方的抵抗意志、从而能够使我方在较短的时间内，以较小的损失，获得较大的作战效益。

美国“联合构想 2010”(JV 2010) 明确表述的战略可以更加深入来理解信息优势的作用。“JV 2010”要求美军联合运用各种作战力量以整体作战效果来适应美国防御战略的需要。总体作战力的取得来源于四种作战概念（主导机动能力、精确交战能力、集中

后勤能力、全维防护能力），它们为高度分散的部队提供高度的协同，并通过远距离高精度武器精确打击敌人。图 1－2 显示了信息优势的效果，其作用就是将四种作战行动的效果进行集成并产生倍增的效果。

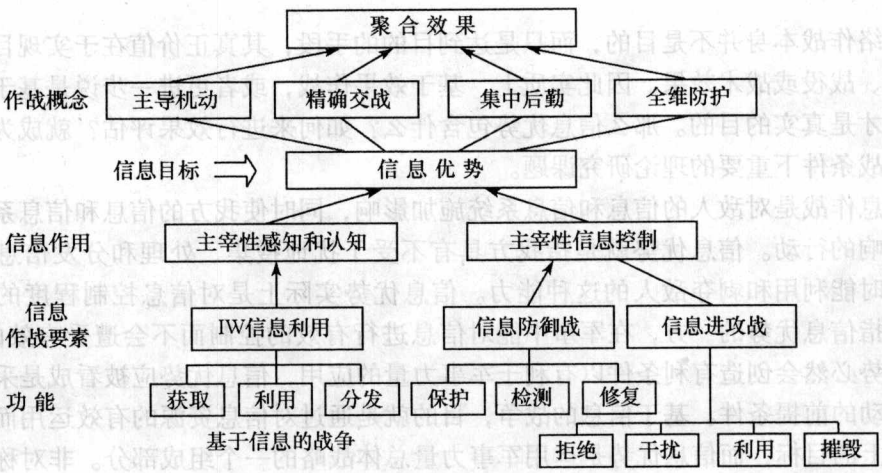


图 1－2 信息优势倍增效果示意图

信息优势的重要作用也可以从图 1－3 中体现：美军精心构建的“全球信息栅格”和“网络中心战”的作战思想，其根本目的就是在全球范围内夺取信息优势，从而取得决策优势从而达到目标最优。

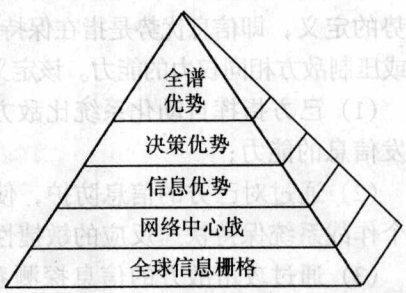


图 1－3 信息优势作用示意图

信息优势是敌对双方在获取和使用信息方面的一种优越性。要夺取和保持战场的信息优势，除了己方具有功能强大的电子信息系统外，还必须对敌方的电子信息系统进行积极而有效的破坏，抑制其信息活动的能力。信息优势可能是责任区域或联合作战区域内全局性的，也可能只局限于某一特定的方面、某一个局部和某一个时期，需要注意的是，指挥自动化系统的信息能力与信息优势能力是两个不同的概念。如前所述，信息优势能力是敌对双方在获取和使用信息方面的一种优越性，它反映的是一种相对的优越性；而信息能力则是一个单方的概念，它主要用于衡量单方指挥自动化系统获取、传输和处理信息的能力；指挥自动化系统的信息能力可以分为静态条件下的信息能力和对抗条件下的信息能力，在对抗条件下仅仅分析单方的信息能力是没有意义的。

由于信息化战争在战争形态、作战力量和作战空间等方面均发生了根本性改变，从