

<<指挥信息系统>>

图书基本信息

书名：<<指挥信息系统>>

13位ISBN编号：9787118079265

10位ISBN编号：711807926X

出版时间：2012-1

出版时间：国防工业出版社

作者：曹雷

页数：289

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<指挥信息系统>>

内容概要

本书是一本全面介绍指挥信息系统概念、结构、技术、应用及对信息化战争影响的教科书。全书共分10章，围绕指挥信息系统这一核心概念，主要阐述了指挥信息系统的基本概念、核心业务模型与系统功能结构，介绍了态势感知、军事通信、指挥控制等关键系统，阐述了指挥信息系统对抗与安全防护、组织运用、分析设计与综合集成的概念与方法，最后介绍子外军的指挥信息系统。

本书涉及指挥信息系统的概念模型、系统结构、基本原理、分析设计、组织运用等各方面的内容，可作为指挥信息系统工程(指挥自动化工程)、作战信息管理、军用网络工程等相关专业的本科生教材，也可作为地方高等院校国防生相关专业的教材和各类军队干部培训(轮训)教材，还可作为国防科技人员和军事爱好者的参考资料。

<<指挥信息系统>>

作者简介

曹雷，1965年1月生于江苏省苏州市。

现为解放军理工大学指挥自动化学院教授。

长期从事指挥信息系统工程、作战仿真等领域教学和科研工作。

先后主持和参与多项全军重大科研项目。

获国家科技进步特等奖1项、军队和省部级科技进步二等奖2项、三等奖8项。

发表各类论文50余篇。

享受军队优秀专业技术一类岗位津贴。

获军队育才银奖。

荣立三等功1次。

鲍广宇，1974年6月生于安徽省嘉山县。

现为解放军理工大学指挥自动化学院教授。

长期从事指挥信息系统工程、指控系统仿真与评估等领域的教学和科研工作。

先后主持和参与多项全军重大科研项目。

获军队科技进步一等奖1项、二等奖1项、三等奖10余项。

发表各类论文40余篇，编写各类教材9部。

荣立三等功1次。

<<指挥信息系统>>

书籍目录

第1章 指挥信息系统概述

1.1 信息化战争

1.1.1 人类战争的历史轨迹

1.1.2 信息与战争

1.1.3 信息化战争的特征

1.1.4 信息化转型

1.2 指挥信息系统

1.2.1 指挥信息系统基本概念

1.2.2 指挥信息系统与信息化战争

1.2.3 指挥信息系统分类

1.3 指挥信息系统发展历史

1.4 几个重要的基本概念

1.4.1 指挥控制与指挥控制系统

1.4.2 指挥控制理论与指挥信息系统

1.4.3 信息化战争与信息战

1.4.4 信息化战争与信息化作战

思考题

参考文献

第2章 指挥信息系统的业务模型

2.1 作战过程模型

2.1.1 经典的作战过程模型

2.1.2 信息化条件下的作战过程模型

2.2 态势感知过程

2.2.1 态势感知模型

2.2.2 态势获取

2.2.3 态势处理

2.2.4 态势共享

2.3 指挥控制过程

2.4 小结

思考题

参考文献

第3章 指挥信息系统的功能结构和信息基础设施

第4章 态势感知系统

第5章 军事通信系统

第6章 指挥控制系统

第7章 指挥信息系统的对抗与安全防护

第8章 指挥信息系统的组织运用

第9章 指挥信息系统分析设计与系统集成

第10章 外军的指挥信息系统

<<指挥信息系统>>

章节摘录

版权页：插图：信息保障特别将保障信息安全所必需的“保护（Protection）、检测（Detection）、响应（Response）和恢复（Restoration）”（PDDR）视为信息安全的四个动态反馈环节，从而安全管理在一个大的框架下，能够针对薄弱环节，有的放矢，有效防范，围绕安全策略的具体需求有序地组织在一起，架构一个动态的安全防范体系。

生存技术就是在系统在攻击、故障和意外事故已发生的情况下，在限定的时间内完成使命的能力，具有“可生存性”，其核心就是要做到入侵容忍。

当故障和意外发生的时候，可以利用容错技术来解决系统的生存问题，如远地备份技术和拜占庭式（Byzantine）容错冗余技术。

除了容错之外，还要解决因攻击者攻击而造成的系统错误。

所以，生存技术中最重要的并不是容忍错误，而是容忍攻击。

容忍攻击是指在攻击者到达系统，甚至控制部分子系统时，系统不能丧失其应该有的保密性、完整性、真实性、可用性和不可否认性。

解决了入侵容忍，也就解决了系统的生存问题。

入侵容忍技术是第三代信息安全技术的代表和核心，也被直接称为第三代信息安全技术。

7.3.2 指挥信息系统面临的威胁与安全防护特点 7.3.2.1 指挥信息系统面临的威胁 信息化条件下的现代战争中，战场侦察监视系统将日趋完善，大量精确制导武器和电子武器、信息武器将广泛投入作战运用，指挥信息系统安全面临严重威胁。

1. 侦察技术空前提高，精确打击威胁极大 现代战场上，发现目标的手段多样，侦察、监视系统与精确制导武器组成了“精确定位打击系统”，从而实现侦察、指挥与控制、打击一体化。

敌对双方可利用巡航导弹、反辐射导弹、精确制导武器对信息结点实施精确打击和破坏。

反辐射导弹以对方指挥系统的电子设备、无线电台、无线网桥通信系统的电磁源为引导，对指挥信息系统构成更为直接的威胁。

“斩首攻击”等作战思想，使指挥信息系统的重要地位凸显出来，指挥信息系统一旦被敌方侦察系统所捕获，则难逃被打击的命运。

在海湾战场上，以美军为首的多国部队从“沙漠风暴”行动一开始，就把伊军的指挥控制中心和通信枢纽作为首要突击目标，使用了从空中到地面的众多高技术武器装备实施“软打击”和“硬摧毁”，开战不到10天，就使伊军指挥信息系统瘫痪，使指挥机构失去了对部队的控制，从而控制了战局。

2. 电磁攻击手段多样，系统稳定性易遭破坏 指挥信息系统的网络数据交互，主要有有线通信组网、无线通信组网以及混合通信组网三种基本链路组织方式。

有线方式通过野战光缆、野战被覆线、双绞线连接，其信息流量大，受自然环境的影响小，通信质量高，抗干扰能力和保密性强。

不利之处是，开设周期比较长，对人力、物力保障依赖大。

因此为保证实现快速互联，必将利用无线传输，以无线或混合通信的组网方式进行互连。

但无线通信方式易遭受敌方的电磁攻击。

如敌对双方可采用有源电子干扰方式，发射或转发与对方信号形式相同的电磁波。

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>