主编　刘由芳　韩 强

JUNSHI XINXI ANQUAN YUANLI

军事信息安全原理

—信息防御作战基础理论

国防大学出版社
GUOFANG DAXUE CHUBANSHE

军事信息安全原理

——信息防御作战基础理论

主编　刘由芳　韩　强

国防大学出版社

图书在版编目（CIP）数据

军事信息安全原理/刘由芳　韩强主编．—北京：国防大学出版社，2005.6
ISBN7-5626-1434-2

Ⅰ.军… Ⅱ.①刘…②韩… Ⅲ.军事-信息系统-安全技术
Ⅳ.E0-059

中国版本图书馆 CIP 数据核字（2005）第 062129 号

国防大学出版社出版发行
（北京海淀区红山口甲 3 号）
邮编：100091　电话：（010）66772856

北京国防印刷厂印刷　新华书店经销
2005 年 6 月第 1 版　2005 年 6 月第 1 次印刷
开本：850×1168 毫米　1/32　印张：9 25
字数：222 千字　印数：3000 册
定价：16.00 元
ISBN 7—5626—1434—2/E・814

《军事信息安全原理》
编 委 会

前　言

21世纪是交互网络社会、信息社会、知识经济社会。随着计算机互联网络的迅速发展和广泛应用，其信息的国际化、社会化、开放化的特性为人们提供信息共享、资源共享和技术共享，但同时也对国家和军队安全提出了严峻的挑战。掌握“制信息权”，建立信息“边防线”、保卫本国的“信息边疆”、捍卫国家主权和安全，已是时不我待的神圣职责。

信息安全学是近十年来迅猛发展的综合性很强的新兴学科。它涉及通信、计算机、数学、运算学、信息学、数理逻辑、人工智能和管理等诸学科，内容相当广泛。本书共分6篇13章。其中，除简要介绍军事信息安全的基础知识外，重点阐述军事信息安全的风险分析、保障策略、主动防护、深透检测、安防认证、动态响应和灾难恢复等7大原理，并创建军事信息安全过程的循环体模型。

军事信息安全原理，是系统研究军事信息安全规律和方法的科学。为顺应新军事变革的时代潮流，该书以面向现代化、面向世界、面向未来为准绳，以培养造就高素质军事人才为重任，以打赢信息化条件下的局部战争需要为目的，系统阐述了军事信息安全原理的基本思想和方式方法。本书力求集普遍性、专业性、技术性和通用性为一体，是新世纪探索军事信息安全思想与规律的理论，也是信息防御作战理论的基础论著。

该书可作为军队院校信息安全的教材，也可作为官兵学习军

事信息安全知识的参考书。

本书在总参郑州科技创新工作站的具体指导下，历时近三个春秋，几易其稿，终于使这部融理论性、学术性、知识性和技术性的军事信息安全原理论著得以面世。除了编著者努力之外，许多人在该书的构思、撰写、输入和校对中做出了积极贡献；此外，本书直接或间接参阅和引用了国内外专家、学者的有关文献，我们深表感谢。同时，感谢国防大学出版社为本书提供出版的机会，感谢责任编辑彭呈仓同志及其编排人员为本书规划、编辑、出版、发行所做出的卓有成效工作。

《军事信息安全原理》涉及的学科领域和理论知识比较广泛、新颖，众多内容相互渗透，加之信息技术和理论发展变化急剧。尽管作者编撰过程中力求做到系统、全面、通俗与严谨，但限于水平和时间，疏漏与不妥之处在所难免，敬请专家、学者和读者批评、指正。

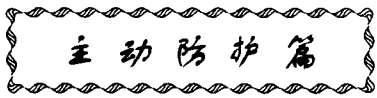
作　者

2005 年 2 月

目　录

基础理论篇

风险分析/保障策略篇



深透检测/安防认证篇

动态响应/灾难恢复篇

基础理论篇

该篇通过对军事信息安全概念、精神、属性、范畴、模型及其展望的论述，主要回答军事信息安全“是什么”、“做什么”的问题。

基础理论篇

第一章　军事信息安全概述

军事信息安全，是巩固国防、促进经济发展、确保国家繁荣、推动社会进步，以及提高人们的工作水平和生活质量的重要保证。解析军事信息安全的原理，必先诠释其概念内涵。

一、军事信息安全概念

（一）安全

“安全”并没有一个统一的定义，但对该词有四种代表性的解释。如：

一是远离危险的状态或特性；

二是客观上不存在威胁，主观上不存在恐惧；

三是没有危险，平安的，不必害怕或焦虑；

四是为防范间谍活动或蓄意破坏、犯罪、攻击等而采取的措施。

这四种解释基本上涵盖了安全的本义。

（二）信息安全

信息安全同样没有公认和统一的定义，也有众多之说，有代表性的解释是：

一是为了防止未经授权就对知识、事实、数据或能力进行使

用、滥用、修改或拒绝使用而采取的措施；

二是信息安全是对信息、系统以及使用、存储和传输信息的硬件的保护。

三是信息安全的含义是通过各种计算机、网络和密钥技术，保证在各种系统和网络中传输、交换和存储的信息的机密性、完整性和真实性。

（三）军事信息安全

“军事信息安全”的定义更是五花八门，不一而足。如：

军事信息安全，主要是指“秘密与关键信息产生、传输、存储过程中不被对方获悉或破坏，确保信息的可用性、保密性和完整性”。

军事信息安全，主要是指军事“信息不受威胁，即保证信息的完整性、可用性、机密性、可靠性和真实性，保证采集信息、传输信息、处理信息、存取信息和使用信息的安全”。

军事信息安全，主要是指军事“信息系统的软、硬件资源受到破坏、信息失泄（窃）或遭受攻击而采取物理的、逻辑的，以及行为管理的方法与措施，以保证信息系统可靠运行与数据存储、处理的安全”。

以上，罗列了“安全”、“信息安全”、“军事信息安全”的有关定义，从这些含义中可以看出，不管是宏观的还是微观的信息安全定义，都是从各自业务系统的角度，从不同的层面上来论述信息安全的。但共性的含义有两点：一是强调信息系统的整体保护。即确保信息处理系统安全、可靠与不间断地运行，为信息系统的所有用户提供有效的服务；二是强调信息系统的信息保护，即确保信息系统中的信息免遭泄露、破坏或篡改，为系统中的各信息提供应有的保护。

为此，军事信息安全就是保障军事信息、系统与机构免遭威胁与侵害，而在分析风险的基础上，制定安全策略，进行主动防

护、深透检测、安防认证、动态响应与灾难恢复等行为过程。

该定义反映出：为抵抗军事信息系统因人为失误、恶意破坏以及各种自然灾害所造成军事系统和机构正常业务中断的能力。

二、军事信息安全属性

（一）军事信息安全是一个相对抽象的概念

军事信息安全，就是关注军事信息本身的安全，而不管应用计算机或什么处理手段，也不是要求达到的绝对量。军事信息安全的任务是保护军事信息资源，以防止偶然的或未授权者恶意泄露、修改或破坏军事信息，从而导致军事信息可靠性差或无法处理。因为这种偶然性或恶意行为的不确定性，使军事组织利用军事信息无法保障不招致损失，而只求损失最小。再则，因为各军事信息系统处在不同层次、担负不同工作、执行不同任务（战斗）的信息系统，其安全要求、标准与指数也不尽相同，所以说军事信息安全只是一个相对而抽象概念。

（二）军事信息安全是个相当广泛的领域

军事信息安全所涉及的领域相当广泛。从技术角度上看，军事信息安全研究的内容主要包括通信安全、计算机安全、操作安全、资源保护和实体安全等；从通信专业来看，包括移动通信安全、数据通信安全、卫星通信安全、网络（计算机网络、多媒体网络和智能化网络）安全等；从信息系统的设备上看，包括质量可靠、性能先进和物理安全等；从管理层次上看，包括人员可信、协议完善，规章制度健全等。

（三）军事信息安全是一个不断更新完善的过程

军事信息安全的静态含义，是创建计算机系统、数据处理系统等军事信息系统时所采取的技术以及管理的保护措施，防止造成军事信息系统的硬件、软件和数据有意无意泄露、破坏、丢失

等问题的发生。

军事信息安全的动态含义，是军事信息系统能连续正常工作。军事信息系统在规划、设计和运行的过程中，安全只是相对的，不安全因素则是绝对的。另外，对原有不安全因素的排除，并不等于遏制了新的不安全因素的出现，也可能刺激了新的不安全因素的产生。所以，在新军事变革的今天，信息对抗愈演愈烈，军事信息安全的周期越来越短，更新——完善——再更新——再完善，由此周而复始才是军事信息安全的真正要义。

三、军事信息安全特征

研究军事信息安全的目的就是保护军事信息资源免受威胁与侵害。根据国际标准化组织（ISO）的定义，以及部分国家政府有关信息安全的规定和专家学者的观点，军事信息安全的内在属性就是实现保密性、完整性、可用性、可控性、占用性和可信性等“六性”安全。

（一）保密性

信息保密性是指静态军事信息防止未授权访问和动态军事信息防止非法截取、解密与利用。

军事信息的保密性是确保拥有权限和特权的人才允许其访问，而那些未获授权的人则被禁止访问的特性。为此，应根据不同的数据类型和应用需求，对具体数据和用户进行分类，并配置不同的访问模式，以此保护静态军事信息的安全。

由于军事系统无法以确认是有未授权用户窃听网上数据，若随保障动态（传输中）信息的安全，应采取数据加密技术来实现这一目标。因加密后的军事信息能保证在传输、转换和使用过程中不被未授权者非法获取与使用。同时，也限制了非法用户对军事信息的访问，从而维护了军事信息的保密性。