

<<全球视野下的中国信息安全战略>>

图书基本信息

书名：<<全球视野下的中国信息安全战略>>

13位ISBN编号：9787302314493

10位ISBN编号：7302314497

出版时间：2013-2

出版时间：清华大学出版社

作者：张显龙

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>

## <<全球视野下的中国信息安全战略>>

### 内容概要

《全球视野下的中国信息安全战略》在探讨国外信息化战略的基础上对上述三大核心进行了详细论述，对如何构建中国信息安全战略给出了自己的见解。

对中国而言，国家信息安全战略的理想模式是三位一体的“积极防御型”战略模式，即全面提升网络信息空间的信息保障、信息治理和信息对抗的能力和水平，积极应对信息安全的威胁与挑战，全面保障国家综合安全和核心利益的实现。

信息基础设施保障、网络信息治理和信息战是中国信息安全战略的三大核心。

## 书籍目录

第1章 研究背景与全书的总体结构 1.1研究背景和问题的提出 1.1.1信息革命从预言到现实 1.1.2 高信息依赖导致高安全风险 1.2信息安全的研究现状 1.3本书的基本思路及总体结构 1.4本书的研究方法 第2章 国家信息安全战略的概念体系 2.1信息安全的内涵与特征 2.1.1从“信息”的本源看信息安全 2.1.2从发展历程看信息安全的内涵 2.1.3 网络安全是信息安全的核心 2.2 国家安全的内涵与特征 2.2.1 国家安全的发展 2.2.2 国家安全的内涵 2.2.3 国家安全战略的内涵 2.3 国家信息安全的范畴与地位 2.3.1 国家信息安全的范畴 2.3.2 国家信息安全的地位 2.3.3 国家信息安全的特征 2.3.4 时代呼唤国家信息安全战略的诞生 第3章 国家信息安全战略的构成要素 3.1 国家信息安全战略的总体框架 3.1.1 国家信息安全战略的内容框架 3.1.2 国家信息安全战略的制定步骤 3.2 国家信息安全战略的目标 3.3 国家信息安全战略的方针与原则 3.3.1 国家信息安全战略方针 3.3.2 国家信息安全战略原则 3.4 国家信息安全战略模式 3.4.1 国家信息安全战略模式的含义 3.4.2 国家信息安全战略模式的基本类型 3.5 国家信息安全战略能力 3.5.1 国家安全战略能力 3.5.2 国家信息安全战略能力 3.6 国家信息安全重点战略措施 3.6.1 国家信息安全的组织体系 3.6.2 国家信息安全法制体系 3.6.3 国家信息安全运作机制 3.6.4 国家信息安全人才建设机制 3.6.5 信息安全技术、标准与产业 3.6.6 国际信息安全合作体制 第4章 西方发达国家信息安全战略概述 4.1 美国信息安全战略 4.1.1 美国信息安全面临的环境与威胁 4.1.2 美国国家信息安全发展历程 4.1.3 美国信息安全战略要素 4.1.4 当前美国信息安全战略解读 4.1.5 美国国家信息安全战略措施 4.2 俄罗斯信息安全战略 4.2.1 俄罗斯国家安全战略面临的挑战 4.2.2 俄罗斯国家安全战略的演变 4.2.3 俄罗斯国家信息安全分析 4.3 西方其他国家信息安全战略综述 4.3.1 英国的信息安全战略 4.3.2 法国的信息安全战略 4.3.3 德国的信息安全战略 4.3.4 日本的信息安全战略 4.4 西方发达国家信息安全战略对我们的启示 第5章 中国国家信息安全战略框架 5.1 中国信息安全现状及形势分析 5.1.1 中国信息安全战略的发展历程 5.1.2 中国信息安全面临的外部风险 5.1.3 中国信息安全面临的内部风险 5.2 中国未来信息安全战略目标 5.3 中国信息安全战略方针与原则 5.3.1 中国信息安全战略方针 5.3.2 中国信息安全战略原则 5.4 中国信息安全战略模式选择 5.5 中国信息安全战略能力分析 5.6 中国信息安全战略的三大核心 第6章 信息基础设施安全保障 6.1 信息基础设施安全保障现状 6.1.1 国家信息基础设施保障的重点 6.1.2 信息基础设施安全保障存在的问题 6.1.3 信息基础设施安全保障措施 6.2 新技术环境下的信息基础安全保障 6.2.1 云计算环境下的信息安全保障 6.2.2 物联网环境下的信息安全保障 6.2.3 三网融合环境下的信息安全保障 第7章 互联网治理与国家政治安全 7.1 中国政治安全面临的威胁与挑战 7.1.1 国家政治安全的内涵 7.1.2 中国政治安全的内外部威胁 7.2 互联网对国家政治安全的双面效应 7.2.1 互联网对民主政治的促进作用 7.2.2 互联网给政治安全带来难题 7.3 加强互联网治理, 保障国家政治安全 7.3.1 互联网时代国家政治安全控制的难点 7.3.2 西方网络治理的现状与问题 7.3.3 我国互联网治理应坚持的几大原则 7.3.4 我国互联网治理的措施 第8章 信息战与国家信息安全 8.1 信息战的内涵与特点 8.1.1 信息战的基本内涵 8.1.2 信息战的几种重点样式 ..... 第9章 中国信息安全重点战略措施 第10章 信息安全的国际合作 后记 参考文献

章节摘录

版权页：插图：自评估和检查评估可依托自身技术力量进行，也可委托具有相应资质的第三方机构提供技术支持。

但由于信息安全风险评估工作敏感性强，涉及系统的关键资产和核心信息，参与风险评估工作的单位及其有关人员均应遵守国家有关保密法规，对风险评估工作中涉及的保密事项，应采取相应保密措施，签订具有法律约束力的保密协议，并承担相应责任。

国内已经出现过由于委托第三方机构进行信息安全风险评估而带来新的风险的情况。

（4）信息安全风险评估的工具 风险评估的进行离不开风险评估工具，自动化的风险评估工具不仅可以将分析人员从繁重的手工劳动中解脱出来，最主要的是它能够将专家知识进行集中，使专家的经验知识被广泛的应用。

目前对风险评估工具的分类还没有一个业界普遍认可的标准，有些技术人员把漏洞扫描工具称为风险评估工具，在信息安全风险评估过程中，漏洞扫描工具确实是基础性工具，通过漏洞扫描工具可以发现系统存在的漏洞，根据漏洞扫描结果提供的线索，可以利用渗透性测试来确认系统存在的高风险漏洞，但信息安全风险评估是技术和管理相结合的综合评估，因此，风险评估工具至少应包括安全管理评估工具、脆弱性分析和渗透性测试工具、风险评估辅助工具。

（5）信息安全评估分析方法 在风险评估过程中，可以采用多种操作方法，包括基于知识（Knowledge—based）的分析方法、基于模型（Model—based）的分析方法、定性（Qualitative）分析和定量（Quantitative）分析，无论何种方法，共同的目标都是找出组织信息资产面临的风险及其影响，以及目前安全水平与组织安全需求之间的差距。

基于知识的分析方法 基线风险评估时，组织可以采用基于知识的分析方法来找出目前的安全状况和基线安全标准之间的差距。

基于知识的分析方法又称作经验方法，它牵涉到对来自类似组织（包括规模、商务目标和市场等）的“最佳惯例”的重用，适合一般性的信息安全组织。

采用基于知识的分析方法，组织不需要付出很多精力、时间和资源，只要通过多种途径采集相关信息，识别组织的风险所在和当前的安全措施，与特定的标准或最佳惯例进行比较，从中找出不符合的地方，并按照标准或最佳惯例的推荐选择安全措施，最终达到削减和控制风险的目的。

基于知识的分析方法，最重要的还在于评估信息的采集，信息源包括：会议讨论；对当前的信息安全策略和相关文档进行复查；制作问卷，进行调查；对相关人员进行访谈；进行实地考察。

## <<全球视野下的中国信息安全战略>>

### 编辑推荐

《全球视野下的中国信息安全战略》既是中国信息安全战略、国家安全战略研究者和实践者的精华读本，又是广大关心互联网发展、关心信息化建设人员的必读参考书。

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>