国家信息安全问题研究

李孟刚 著

国家信息安全问题研究

THE STUDY OF NATIONAL INFORMATION SECURITY

社会科学文献出版社
SOCIAL SCIENCES ACADEMIC PRESS (CHINA)

国家信息安全问题研究

The Study of
National Information Security

李孟刚◎著

社会科学文献出版社
SOCIAL SCIENCES ACADEMIC PRESS (CHINA)

图书在版编目(CIP)数据

国家信息安全问题研究/李孟刚著. —北京：社会科学文献出版社，2012.11
ISBN 978-7-5097-3806-1

Ⅰ.①国… Ⅱ.①李… Ⅲ.①信息安全-国家安全-研究-中国
Ⅳ.①D631

中国版本图书馆CIP数据核字（2012）第223516号

国家信息安全问题研究

著　　者／李孟刚

出 版 人／谢寿光
出 版 者／社会科学文献出版社
地　　址／北京市西城区北三环中路甲29号院3号楼华龙大厦
邮政编码／100029

责任部门／财经与管理图书事业部（010）59367226　　责任编辑／陶　璇
电子信箱／caijingbu@ssap.cn　　责任校对／李瑞芬
项目统筹／恽　薇　蔡莎莎　　责任印制／岳　阳
经　　销／社会科学文献出版社市场营销中心（010）59367081　59367089
读者服务／读者服务中心（010）59367028

印　　装／北京鹏润伟业印刷有限公司
开　　本／787mm×1092mm　1/16　　印　　张／19
版　　次／2012年11月第1版　　彩插印张／0.375
印　　次／2012年11月第1次印刷　　字　　数／308千字
书　　号／ISBN 978-7-5097-3806-1
定　　价／59.00元

本书如有破损、缺页、装订错误，请与本社读者服务中心联系更换
版权所有　翻印必究

序

对于一个国家来说，信息资源是重要的战略资源。特别是在当今信息化深入发展的时代，信息资源的争夺已成为各国资源争夺的焦点。随着信息化的不断发展，信息安全在国家安全中的地位越来越高，信息安全问题也伴随着网络信息技术的发展与成熟成为关系到国家安全的突出问题。系统地研究国家信息安全的基本理论和保障方法，分析国家信息安全存在的问题和改进措施，正确把握国家信息安全的发展战略和趋势，对于维护国家安全和社会稳定、构建社会主义和谐社会具有十分重要的意义。

目前，信息安全方面的研究成果不少，成效也很大，但主要集中在信息安全技术领域，强调信息系统的技术安全防护方法；其次是信息化风险评估领域，强调信息化过程的风险控制；还有的是集中在信息安全立法的比较研究、制度和保障体系建设等方面，强调国外经验的介绍与借鉴。然而，从国家宏观层面和体系建设角度，进行信息安全调查和分析的研究则相对匮乏。

应该说，信息安全不单单是一个技术问题、局部问题，它已上升为事关国家安全和社会稳定的全局性战略问题。由于互联网发展在地域上的不平衡性，信息强国对于信息弱国已形成了“信息势差”，众多发展中国家尚不能主动、有效地传播自己的信息和及时、充分地分享所需要的信息，信息流通呈现明显不对等、不公平、不公正的态势。因此，站在更高的层次上、从全局的视角，全面系统地研究国家信息安全问题并提出应对策略，是非常有必要的。

信息时代的国家信息安全问题研究是一个复杂的系统工程，涉及政治、经济、文化、法律、军事等各个方面。为了完成这一艰巨的课题，中国产业安全研究中心成立了由多名教授和博士生组成的研究小组，查阅了大量信息

安全理论方面的文献，搜集了众多国外信息安全建设方面的资料，调查走访了一些信息安全相关部门和企业，对我国信息安全存在的问题进行了重点的分析、归纳和讨论，在理论和问题研究的基础上，通过与国外信息安全战略、体系的比较，提出了我国的国家信息安全战略与体系。

本书主要解决了两个问题：一是从全球信息化和经济全球化的背景出发，构建了国家信息安全的理论体系；二是从产业安全的视角，明确了国家信息安全问题的研究范式，从而为各种专题研究提供了理论与方法，这也是本书最大的价值所在。相信本书的出版对于今后进一步研究国家信息安全问题会大有裨益，也希望中国产业安全研究中心能够有更多成果问世。

以上，是为序。

国家发展和改革委员会秘书长

2012 年 7 月 16 日

此为试读，需要完整PDF请访问：www.ertongbook.com

摘　要

国家信息安全问题作为国家安全体系中的关键要素，关系到国家未来的生存和发展。本书致力于在明晰国家信息安全的基本理论和保障方法的基础上，分析国家信息安全存在的问题和改进措施，正确把握国家信息安全发展战略和趋势，为我国的国家安全、社会稳定和构建社会主义和谐社会作出贡献。

本书致力于全面系统地研究国家信息安全问题，并提出应对策略，重点解决两个问题：一是从全球信息化和经济全球化大背景出发，构建国家信息安全的理论体系构架；二是从产业安全的视角，构建国家信息安全问题的研究范式。从而为今后的各种专题研究提供理论与方法。以此为出发点，本书主要包括国家信息安全理论研究、国家信息安全问题分析和国内外信息安全战略与体系比较研究三部分内容。

一　国家信息安全理论研究

本书首先对国家信息安全相关理论进行了详细阐述，为研究工作构建了坚实的理论基础。理论研究部分主要从四个方面进行了系统分析。

1. 信息化与信息安全

首先对信息化与信息安全进行了概述，分别介绍了信息基本属性与生命周期、信息化的内涵与发展趋势、全球信息化与经济全球化以及全球信息化下的信息安全问题。信息安全问题是一个系统工程问题，涉及的内容十分广泛，既有技术问题，又有管理问题，还有立法问题。因此，站在全球信息化大背景下，对信息化及信息安全的相关问题进行系列的研究，是非常必要的。

2. 信息安全的概念解析

信息安全的概念解析主要是界定了信息安全的基本内涵，解释了国家信息安全的内涵、特点以及主要内容，最后对国家信息安全保障体系进行了概括，并在上述研究的基础上，总结了国家信息安全保障体系的建设策略，包括建立和完善国家信息安全基础设施、推动信息安全技术的创新和发展、建立有自主产权的信息安全产业以及创造良好的国家信息安全支撑环境。

3. 信息安全管理与技术

世界各国都在加强各自的信息安全保障体系建设，以免遭受更大的威胁和外来入侵。在整个信息安全保障体系建设中，信息安全管理发挥着重要作用，它是信息安全体系建设的重要基础。信息安全管理与技术的相关理论研究，明确了信息安全管理的方法、内容、体系标准以及平台等，介绍了当前主要的信息安全技术，包括防火墙技术、虚拟专用网络技术、入侵检测系统技术、身份认证技术、数字签名技术以及加密技术，最后引入信息安全工程的概念，对信息安全工程建设流程和生命周期、系统安全工程能力成熟度模型、信息安全工程实施以及等级保护等内容进行了阐述。

4. 信息安全评估

保障信息系统产品和技术的安全性，是保证国家、行业、企业信息安全的基础。因此，针对信息系统产品和技术，制定相关的评估和评价标准是非常必要的。信息安全评估是国家信息安全理论的重要组成部分，本书首先介绍了几种流行的信息化评估体系，并对其要素构成和算法原理进行了解释，在此基础上，系统分析了信息安全评估体系，包括信息安全标准化概述、信息安全评估的目的与过程、信息安全指标体系、信息安全综合评价方法，除此之外，还分析了信息化项目风险评价，包括信息化项目及其风险管理、风险产生的原因及表现分析、风险的识别与估计方法、风险评估原理与模型方法。

二 国家信息安全问题分析

在理论研究的基础上，对国家信息安全问题进行了深入研究，重点分析了中国国家信息安全基本问题和中国信息安全产业。

对于中国国家信息安全基本问题，主要从电子政务、电子商务、一般企

业及国家基础设施四个角度进行了剖析。

1. 电子政务信息安全

在界定电子政务信息安全基本内涵和分析我国电子政务发展现状的基础上，总结了我国电子政务信息安全存在的问题，具体包括硬件和软件的对外依赖性、各级政府网站中存在的系统漏洞和管理漏洞及安全立法和标准体系的欠缺三个方面。

在此基础上，选取有代表性的税务系统、金融系统、财政系统、海关系统以及政法系统等五个电子政务系统进行了更加深入的分析，结合电子政务系统的应用现状，分别归纳了各电子政务系统存在的信息安全问题。

税务系统信息安全存在的问题有：计算机病毒和网络攻击，计算机病毒的传播和黑客的攻击可以导致税务信息系统的瘫痪、被窃取和篡改重要数据，给系统中的各方带来巨大的、不可估量的损失；安全意识薄弱，我国的税务信息化几乎已经覆盖到了全国税务系统的每个工作角落，目前我国税务对信息系统的依赖程度非常高，如果各级领导干部不能跟上时代的步伐，要搞好信息化、保障信息安全是不可能的；基础设施建设不够，基础设施建设不够主要表现在基层部门，这与安全意识的缺乏，以及各地信息化发展水平不一致有关。但是由于木桶原理，基层部门安全设备的配置薄弱会导致整个网络的效率下降。

金融系统信息安全，存在的问题有计算机病毒和网络攻击，计算机病毒的传播和黑客的攻击可以导致金融系统的瘫痪、被窃取和篡改重要数据，给金融系统中的银行和用户等各方带来巨大的、不可估量的损失；身份认证风险，由于网络的虚拟性，金融交易方的身份认证变得十分重要，例如，曾经发生过很多假冒银行网站骗取持卡人卡号密码的案件（网络钓鱼）。同时，还存在金融系统内部人员监守自盗的行为。

财政系统信息安全，存在的问题有黑客攻击和计算机病毒，计算机病毒的传播和黑客的攻击可以导致财政系统的瘫痪、被窃取和篡改重要数据，给财政工作带来巨大的、不可估量的损失；安全管理制度存在问题，政府财政部门从最高领导层到全体工作人员都要提高安全意识，建立完整的安全管理组织，明确安全目标、安全策略和安全职责；基础设施建设不够，主要表现在基层部门，这与安全意识的缺乏，以及各地信息化发展水平不一致有关。

海关系统信息安全，存在的问题主要有大范围的网络环境的安全问题，即整个信息网络的安全环境，包括因特网和通信网络，具体有黑客攻击、病毒传播、网络犯罪、垃圾信息和网络突发故障等；管理信息安全的组织架构存在问题，海关的信息系统维护集中于总关的科技部门，采取集中式维护的方式，各部门各司其职，条块分割，这样的组织架构导致了协同管理效率较低，人员专业素质专而不广，无法建立起完整、广泛的信息安全管理控制体系。

政法系统信息安全，存在的问题有网络及应用系统的安全问题，包括硬件和软件安全；来自内部或外部的黑客攻击，黑客攻击手段可分为非破坏性攻击和破坏性攻击两类；来自内部人员（合法用户）的滥用权力、有意犯罪、越权访问机密信息，或者恶意篡改数据等，内部安全威胁包括内部员工的恶意攻击和内部人员的误操作；病毒或有害信息的传播、自然灾害或人为造成的物理破坏等，病毒往往会利用计算机操作系统的弱点进行传播，提高系统的安全性是防病毒的一个重要方面。

2. 电子商务信息安全

首先界定了电子商务信息安全的基本内涵，电子商务的信息安全是指商务数据信息在产生、接收、分发、处理、存档等信息生命周期全过程中有可能被破坏完整性、正确性、精确性和被窃取，它涵盖了整个信息环境的各个方面，包括信息网络、信息内容、信息应用、媒体、通信基础设施等。本书明确了我国电子商务发展的现状及电子商务信息安全存在的问题，存在的问题具体包括四点。

一是计算机系统和通信网络本身存在的安全问题。电子商务依赖于计算机系统和通信网络，它们本身存在的安全问题也影响到电子商务的信息安全。例如，黑客、病毒、网络和系统故障等。

二是商务软件中存在的安全漏洞。随着软件和程序的复杂性和编程多样性越来越高，漏洞出现的可能性就越大。这样的漏洞加上操作系统本身存在的漏洞，使得电子商务安全遭受巨大的威胁。

三是交易中的身份认证问题。随着我国电子商务的普及，网民的理财习惯正逐步向网上交易转移，针对网上银行、证券机构和第三方支付的攻击将急剧增加。针对金融机构的恶意程序将更加专业化、复杂化，可能集网络钓

鱼、网银恶意程序和信息窃取等多种攻击方式为一体，实施更具威胁的攻击。

四是电子商务立法和安全标准滞后。目前我国电子商务交易中产生的问题存在着原有法律条文没有涉及或者有涉及但不完全适用的情况。电子商务要有一个安全的交易环境，就必须要有一个统一的市场规则来支撑。

3. 一般企业信息安全

在界定企业信息安全基本内涵的基础上，归纳了企业信息安全的两个特征：信息安全具有级别性，企业内部工作人员根据其职位职级对信息情报有着不同程度的访问权和修改权；信息安全的对立双方是不对称的，信息安全符合“短板效益”。在此基础上，分析了我国企业信息化的发展现状，明确了我国企业信息安全面临的问题主要是来自企业外部的攻击和来自企业内部的威胁。

第一，来自企业外部的攻击。我国企业，尤其是中小型企业，普遍缺乏对于外部攻击的防护能力和意识。这些攻击包括通信线路的切断，在网络上搭线窃听以获取数据，改变数据文件的值，改变网络中消息的内容，伪造身份等。企业从外国引进和购买了大量的信息技术和设备，但是对这些设备的隐形安全问题却无从根本解决。

第二，来自企业内部的威胁。来自企业内部的威胁，一方面是由于企业自身的管理漏洞、体制问题和人员素质问题，另一方面存在着内外勾结的可能。人为的失误可能造成错误信息的产生、误删误改信息、泄露信息等。企业的内部人员对本单位局域网的熟悉程度加剧了其作案和被外部人员勾结引诱的可能性。

4. 国家基础设施信息安全

重点阐述了电信信息安全、广电信息安全、证券信息安全、电力信息安全、铁路信息安全、交通信息安全、民航信息安全以及国防信息安全等不同基础设施的信息安全现状。

电信信息安全，存在的问题有传输线路信息泄漏、非授权访问和拒绝服务攻击、伪造身份、破坏数据的完整性、破坏系统的可用性、网络病毒问题以及来自内部人员的威胁。

广电信息安全，存在的问题有技术干扰，包括无意的干扰和有意的干

扰，以及相关的安全人才匮乏。

证券信息安全，存在的问题有系统众多，缺乏统一的安全体系（例如网上业务系统、交易系统、登记清算系统等方面），以及人才队伍培养有待加强。

电力信息安全，存在的问题有物理设施安全问题、网络安全问题、标准体系的建设问题以及智能电网的发展带来的新问题。

铁路信息安全，存在的问题有，信息安全管理现状仍比较混乱、信息安全意识缺乏，普遍存在“重产品、轻服务，重技术、轻管理”的思想以及网络信息系统存在的固有的不安全性和脆弱性。

交通信息安全，存在的问题有，病毒的泛滥对计算机信息网络系统的正常运行造成很大的影响，发展水平参差不齐，各地分别发展，容易形成信息孤岛。

民航信息安全，存在的问题主要是信息泄露，在民航领域，一旦信息系统被攻击、无线电通信系统受到干扰、重要专机信息被泄密、出现各种系统故障等，飞行安全都会受到严重威胁，轻者会造成航班正常运作中断，重者会危及飞行安全甚至国家安全。

国防信息安全，存在的问题有缺乏统一规划、物理方面的威胁、辐射信息泄漏、硬件和软件的对外依赖性、通信通道的安全风险、信息安全人才匮乏。

对于中国信息安全产业，主要分析了信息安全产业概况、信息安全产业环境及信息安全产业发展趋势和保障措施：

（1）信息安全产业概况

“十一五”期间，我国信息安全产业持续快速发展，年均增速超过30%，产业规模不断扩大，产品体系逐渐完善，企业实力逐步提升，标准化体系不断完善，人才队伍不断壮大，对国民经济和社会发展的支撑作用进一步增强。在总结当前我国信息安全产业规模、产品体系及企业实力的发展现状的基础上，本书指出我国信息安全产业快速发展的同时，仍面临诸多挑战：产业整体相对弱小，关键产品和高端服务依赖进口，对国家信息安全保障的支撑能力需要进一步提升；产业核心技术积累不足，创新能力急需提升，缺乏引领产业发展的大企业，行业内的收购整合不可避免，缺乏技术创

此为试读，需要完整PDF请访问：www.ertongbook.com

新、服务能力和独特商业应用模式的企业将逐步被淘汰；高端信息安全人才不能满足产业快速发展的需要；国家信息安全标准仍不完善，市场竞争急需进一步规范，管理体制迫切需要调整优化，产业发展环境有待完善。

（2）信息安全产业环境

重点分析了信息安全产业的政策法律环境、技术环境和标准化体系与测评认证等，中国信息安全产业发展环境如政策法律环境、技术环境、标准化体系和测评环境等各方面正在全面改善，关键技术取得一定突破，民族企业研发实力和服务水平逐步提高，自主可控能力持续提升，信息安全保障能力得到很大提升。

在政策法律环境方面，政府在政策、规划和标准等方面的支持、引导和规范，有利于营造良好的产业发展环境，充分发挥市场机制作用，促进产业持续、健康、快速发展。

在技术环境方面，与国际先进水平相比，我国信息安全行业的产业核心技术积累不足，并且技术成果转化能力亟待提高，但是在安全服务方面，安全服务水平处于领先地位。

在标准化体系和测评环境方面，我国信息安全标准化工作有序推进，初步建立了信息安全标准体系框架，形成了覆盖信息安全基础、技术、管理、测评等领域的支撑国家信息安全保障体系建设的国家标准，信息安全产品认证认可体系逐步完善。围绕国家信息安全保障体系建设，我国信息安全标准化体系已经取得一定的成果，为国家重大信息化工程和信息安全保障体系建设提供了重要的标准支撑。

（3）信息安全产业发展趋势和保障措施

工业和信息化部制定的《信息安全产业“十二五”发展规划》指出信息安全产业的发展呈现出以下趋势：

第一，向系统化、主动防御方向发展。信息安全保障逐步由传统的被动防护转向“监测—响应式”的主动防御，信息安全技术正朝着构建完整、联动、可信、快速响应的综合防护防御系统方向发展。产品功能集成化、系统化趋势明显，功能越来越丰富，性能不断提高；产品间自适应联动防护、综合防御水平不断提高。

第二，向网络化、智能化方向发展。计算技术的重心从计算机转向互联

网，互联网正在逐步成为软件开发、部署、运行和服务的平台，对高效防范和综合治理的要求日益提高，信息安全产品向网络化、智能化方向发展。网络身份认证、安全智能技术、新型密码算法等信息安全技术日益受到重视。

第三，向服务化方向发展。信息安全产业结构正从技术、产品主导向技术、产品、服务并重调整，安全服务逐步成为产业发展重点。信息技术网络化、服务化等都在积极推动信息安全服务化，信息安全服务在产业中的比重将不断提高，将逐渐主导产业的发展。

同时，为保障我国信息安全产业健康可持续的发展，《信息安全产业“十二五”发展规划》还指出我国信息安全产业的保障措施：一是完善政策和法律制度，优化产业发展环境；二是加强创新能力建设，增强产业竞争实力；三是完善标准化体系，支撑产业发展；四是完善信息安全产品认证，规范产业发展；五是加强人才队伍建设，夯实产业发展基础。

三 国内外信息安全战略与体系比较研究

在国家信息安全理论基础和国家信息安全问题研究的基础上，对国内外信息安全战略与体系进行了比较研究，重点分析了国外信息安全战略与体系，并且提出了我国国家信息安全战略与体系。

1. 国外信息安全战略与体系

对美国、俄罗斯、欧盟等国家的信息安全战略与体系进行了深入分析，具体内容包括国家信息安全战略的背景与目标、国家信息安全保障管理体系、技术体系、评估体系等，并通过以上的分析归纳，从中得出一些可供我国信息安全战略参考与借鉴的经验、教训以及启发。例如美国作为世界首屈一指的信息强国，国家信息安全体系相较于其他国家来说是比较先进与完善的。管理体系、技术体系和评估体系之间的相互结合补充使得整个体系能够始终保持稳定性、安全性和高效性。美国国家信息安全体系带给我们的启发主要有：

第一，管理体系作为国家信息安全体系的基础支撑，应当为技术体系提供更多的法律支持、政策支持，提供更多制度标准保证；

第二，管理体系不能过于庞杂，甚至出现权力冲突，应当有统一的权力机构，将管理权力集中起来，下设其他组织，协调好权力划分问题，从而形

成金字塔式的健康架构；

第三，制定管理战略和政策法规的同时，要注意公众隐私和群众知情权，找到“管”和“放”的平衡点，在不影响公众情绪的同时，保障国家信息安全；

第四，从奥巴马政府新发布的《国家安全战略报告》可以看出，美国开始通过谋求国际合作解决信息安全问题，事实上互联网的跨国特性和世界经济相互依存性共同决定单一国家不可能单纯凭借自身力量控制全球信息流动，国家必须通过合作维护境内信息安全；

第五，要确保国际信息安全体系的高效性，必须建立和完善信息安全评估体系，也就是要构建一个能够发现隐患、制定对策、提升强度，具备认证效果的闭环式反馈型的评估机制；

第六，国家信息安全要进一步提升和发展，除了管理体系的制度支撑和评估机制需信息反馈，还对技术体系要进一步完善，这就需要扩大“信息安全队伍”、增加信息安全技术研发成本，重视人才培养工作；

第七，提高网络攻防能力，积极防御，力求“先发制人”；

第八，提高全民信息安全意识，加强网络安全教育培训工作。

2. 中国国家信息安全战略与体系

首先归纳了中国国家信息安全面临的主要问题，包括信息化领域对外依存度较高、信息安全管理模式有待完善以及网络信息安全威胁尤为突出三个方面。

在明确问题的前提下，深入剖析了中国国家信息安全战略的构成要素：

（1）战略目标

逐步建立和完善适应信息化发展的信息安全保障体系，全面提高国家信息安全保障能力，提高对信息安全的管理、防范、控制能力，确保基础网络、重要信息系统和信息内容的安全，促进国家信息化建设健康、稳步地发展，维护国家安全、社会稳定和公众合法权益。

（2）指导方针

我国的国家信息安全战略应当紧紧围绕“积极防御、综合防范”的基本方针，全面提高信息安全发现预警、防范控制、保护评估、应急恢复、查处打击、对抗反制、监督检查等能力，构建立体防御体系，提高我国信息安

全保障的整体水平，促进信息化健康发展。面向信息安全市场需求，以提升对国家信息安全保障的支撑能力为目标，以保障基础信息网络安全和重要信息系统安全为中心，按照“安全可控、创新发展、环境营造”的原则，推进技术产品创新、应用和服务模式创新，不断推动国家信息安全向体系化、规模化、特色化、高端化方向发展。

（3）基本原则

一是坚持安全可控。通过建立完整的信息安全技术、产品、服务和标准体系，保障基础信息网络、重要信息系统、新技术和新应用的安全可控，为国家、企业和个人的信息安全保障提供技术支撑。在两化融合上升到国家战略高度时，要确保信息安全必须多管齐下，其中很关键的一点就是要研发具有自主知识产权的软件产品，并在市场上予以大范围的推广应用，充分发挥国产软件的“安全、可靠、可控”特点，使其在信息安全的源头上发挥顶梁柱作用。此外，政府应当引导国产软硬件协同作战，互相扶持，互相促进，确保信息化建设道路上自主可控的信息安全。

二是坚持创新发展。通过聚集各方资源，加大信息安全技术创新投入力度，突破信息安全核心技术和关键产品，创新服务模式，占领价值链高端，提升核心竞争力。面向国家信息化建设和两化深度融合带来的信息安全保障需求，加快安全可控信息安全技术、产品和服务的应用推广，鼓励和支持采用安全可控的产品和服务，通过重大应用提升竞争能力，加速信息安全发展。

三是坚持环境营造。信息网络和信息系统主管部门负责领导本系统的信息安全工作，承担和落实信息安全责任，组织运营、使用单位落实安全措施；信息网络和信息系统运营、使用单位应当落实安全组织、人员和安全管理制度、安全技术措施；提供信息安全产品和安全服务的单位，应当保证其提供的服务和产品的安全，维护国家安全、公共利益，保守国家秘密，保护公民、法人和其他组织的合法权益；公民、法人和其他组织在信息网络和信息系统应用中，应当遵守国家法律、法规的规定，承担法律法规规定的安全责任。

在明确中国国家信息安全战略目标、指导方针、基本原则的前提下，提出中国国家信息安全保障体系应当是多层面、多方位的，它的建设工作应当

有总体规划，应当有全局意识，国家信息安全的保障体系需要围绕以下细节全面建设，具体为：要健全信息安全法律体系、构建信息安全标准体系、提升信息安全技术能力、落实信息安全监管责任、重视信息安全应急体系、加强信息安全学科建设。

综上所述，本书构建了国家信息安全的理论体系构架和国家信息安全问题的研究范式，期望能为今后的各种专题研究包括信息安全工程学等提供理论与方法。我们相信，在国家与各级政府的大力支持下，在全体信息安全工作者的共同努力下，我国国家信息安全一定会取得更加辉煌的成绩。

Abstract

As a key factor in the State security system, state information security is closely related to the existence and future development of a nation. Based on the full knowledge of the basic theory and safeguards approaches of state information security, this paper is committed to analyzing the existing problems concerning state information security and the corrective actions, as well as grasping its development strategies and trends in the right direction, so as to make contributions to our country's safety, social stability and the construction of a harmonious socialist society.

This paper aims to study the issue of state information security soundly and systematically, put forward countermeasures, and solve two problems: first, against the background of global informationization and economic globalization, it will form a theoretical framework for state information security; second, from the perspective of industrial safety, it will establish an authoritative form of study on state information security, so as to provide theory and methods for various future monographic studies. With this starting point, the paper mainly consists of three parts, namely, research on the theory of state information security, analysis on the issue of state information security, and China's information security strategies and systems by comparison with those of other countries.

Ⅰ. Research on Theories of State Information Security

Firstly, this paper elaborates on the related theories concerning state information security, which lays down a solid theoretical foundation for the

此为试读,需要完整PDF请访问: www.ertongbook.com