全球视野下的中国信息安全战略

QUANQIU SHIYE XIA DE
ZHONGGUO XINXI ANQUAN ZHANLUE

张显龙　编著

清华大学出版社

全球视野下的中国信息安全战略

QUANQIU SHIYE XIA DE
ZHONGGUO XINXI ANQUAN ZHANLUE

张显龙　编著

清华大学出版社
北京

内 容 简 介

信息时代的到来、信息网络技术的广泛应用，使人们对于国家安全的认识得到了深化和扩展。信息安全逐步成为信息时代国家安全中最突出、最核心的问题，成为国家总体安全的重要基石。作为一个正在逐步崛起的发展中大国，中国的信息安全形势异常复杂，这就更需要制定前瞻、完整、科学的信息安全战略，以应对目前多变、动态、多层次的复杂局面。

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。本书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。

本书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。

图书在版编目（CIP）数据

全球视野下的中国信息安全战略/张显龙编著. --北京：清华大学出版社，2013.2
ISBN 978-7-302-31449-3

Ⅰ. ①全… Ⅱ. ①张… Ⅲ. ①信息安全－国家安全－国家战略－研究－中国
Ⅳ. ①D631

中国版本图书馆 CIP 数据核字(2013)第 020171 号

责任编辑：朱敏悦
封面设计：漫酷文化
责任校对：王凤芝
责任印制：何　芊

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座
邮　　编：100084
社 总 机：010-62770175　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：北京密云胶印厂
经　　销：全国新华书店
开　　本：165mm×240mm　**印　张**：31　**字　数**：361 千字
版　　次：2013 年 2 月第 1 版　**印　次**：2013 年 2 月第1次印刷
印　　数：1～5000
定　　价：66.00 元

产品编号：049670-01

前言

国家信息安全需要顶层设计

信息化是整个世界发展的必然趋势，任何国家都无法置身于这个潮流之外。信息时代的到来、信息网络技术的广泛应用，使人们对于国家安全的认识得到了深化和扩展。今天，信息安全已经成为国家安全的一个重要因素，与其他安全要素之间的联系更为紧密，由此上升为直接影响国家政治稳定、社会安定、经济有序发展的全局性战略问题。中国共产党第十八次全国代表大会报告中有19处表述提及信息、信息化、信息网络、信息技术与信息安全，并且首次明确提出了"健全信息安全保障体系"的目标。可见，信息安全已成为信息时代国家安全中最突出、最核心的问题，成为国家总体安全的重要基石。

目前，信息空间已成为领土、领海、领空之外的“第四空间”，是国家主权延伸的新疆域，成了整个国家和社会的“中枢神经”，其战略地位日趋重要。如果信息安全问题解决不好，将会危及一国的政治、军事、经济、文化、社会生活的各个方面，使国家处于政治动荡、信息恐怖和经济混乱的威胁之中。正因如此，信息空间已经成为各国政治、军事等力量角逐的新战场。这场竞争必将改变国际政治的现有格局，引起国际关系范式的变化，对民族国家的主权和政治、经济、文化构成新的挑战，并会因此影响社会的稳定、整合和发展。

为了在这个竞争中处于主动地位，世界各国都从国家发展战

略、安全战略和军事战略的高度制定信息安全战略，并采取包括外交、军事、经济等在内的多种手段保障信息安全战略的落实和实施。随着这场竞争的逐步展开，世界将进入一个“信息争霸”的新时代。

作为一个正在逐步崛起的发展中大国，中国在这场竞争中面临着来自内外多方面的考验，既要面对外部对中国崛起的遏制，又要应对内部社会转型的种种挑战，中国的信息安全形势异常复杂，这就更需要制定前瞻、完整、科学的信息安全战略，以应对目前多变、动态、多层次的复杂局面。只有把信息安全提升到与国土安全同等重要的地位，把信息化和信息安全作为基本国策，从顶层进行科学的设计，才有可能从根本上改变消极防御、消极应对的局面，才能实现依靠后发优势加速超越的目标。

对中国而言，在当前和未来一段时期，我国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。

第一个核心是关键信息基础设施安全保障。重要的信息基础设施可以概括为“1＋7网络”，1是指一个网络，传统意义上的网络包括电信网、广播电视传输网和互联网三个基础网络，随着三网融合的发展，这三网可以合并为1个网络；7是指金融、电力、交通、税务、海关、党政军及其他要害部门七个重要的应用系统的系统。信息安全保障的关键战略措施包括：加强密码技术的开发利用；建设网络信任体系；加强信息安全风险评估工作；建设和完善信息安全监控体系，提高对网络安全事件的应对和防范能力，防止有害信息传播；高度重视信息安全应急处置工作，健全完善信息安全应急指挥和安全通报制度，不断完善信息

安全应急处置预案；从实际出发，促进资源共享，重视灾难备份建设，增强信息基础设施和重要信息系统的抗毁能力和灾难恢复能力等，通过这些运营措施再加上法律、资金、人才等资源支持，确保关系国计民生的重要信息基础设施的安全、可用。

互联网内容对社会主义意识形态、价值观念和道德规范带来了严峻挑战，因此，信息安全战略的第二个核心是加强互联网内容治理工作，重点战略措施包括：尽快建立网络舆论监测工作机制，深化网络舆情监测和不良信息管理，加强网络舆论的监测、研判和引导工作；加快信息收集、趋势跟踪等网络舆情监测的技术手段和平台建设，加强网络舆情监测和应急处置，建立部门间的舆情共享机制和联动处置机制；加强重点新闻网站建设和安全管理；引导互联网企业对不良内容进行过滤，加快建立网络内容分级管理标准，逐步建立内容分级管理制度等。通过这些措施确保网络信息空间的健康、有序，确保国家的政治和文化安全。

信息安全对军事安全的作用日益突出，“制信息权”对战争全局意义重大，信息威慑、网络信息战、黑客攻击与军事泄密严重威胁军事安全，因此信息安全战略的第三个核心是信息战。在信息战的浪潮中，网络和信息系统正成为实现战争胜利的一道利器。信息战的重点战略措施包括：信息战部队的建设、人才的培养；信息武器的研发；信息战战略、战术的研究与演练；信息战的防御与对抗；信息指挥系统的开发与集成等。通过这些措施确保我国在新的军事对抗中处于主动地位，打赢新时代的信息战争，为经济建设保驾护航。

总之，信息安全战略体系的建立和完善是衡量国家实力、国家主权、国家安全和国际地位的重要依据。在今后很长一段时间内，信息安全都将在国家信息化建设、社会生活、经济生活及国防建设等方面得到体现。我们要站在国家战略的高度做好顶层设计，理顺组织、管理关系，建立健全相应的法律体系，解决好理论和技术创新突破问题，使信息安全工作走上更加健康发展的轨道。

目录

CONTENTS

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

1980年，美国未来学家阿尔温·托夫勒在他所著的《第三次浪潮》一书中，向世人预言：一个迥异于人类历史上前两次重大文明变革的崭新时代——信息时代即将呈现。他将这一巨大的时代变革称之为继农业革命和工业革命之后的第三次革命浪潮。[①] 两年后，约翰·奈斯比特在《大趋势》一书中再次强调指出："目前我们的社会正在发生重大变化，其中最为微妙，也最具有爆炸性的变化是从工业社会向信息社会的转变，一个新的文明正在我们生活中出现；世界并没有面临末日，人类的历史才刚刚开始。"[②]

这一被称为历史上重大变革的信息化社会，代表着人类的经济结构正从以物质与能量为重心向以信息与知识为重心的转变，而以计算机、微电子和通信技术为主的信息技术革命则是社

---

① 阿尔温·托夫勒. 第三次浪潮. 北京：生活·读书·新知三联书店，1980.

② 约翰·奈斯比特. 大趋势. 北京：科学普及出版社，1985.

会信息化的主要推动力量。奈斯比特认为工业社会结束和信息社会来临有两个标志性的事件：一个是1956年美国白领人员的数字首次超过了蓝领工人，另一个是1957年苏联发射了全球第一颗人造地球卫星，开辟了全球卫星通信的新时代。

国际上普遍认为，信息化革命起自20世纪70年代，微电子计算机技术和通信技术的结合标志着世界信息化时代的发端。1971年美国的英特尔公司研制出了第一块微处理器，组成了由大规模集成电路构成的微型计算机是这一变化的历史性事件。而全球信息化浪潮的开始，则以1993年克林顿政府提出“国家信息基础设施”(National Information Infrastructure)计划为标志，也就是所谓的《国家信息高速公路计划》。1994年美国政府在此基础上又提出“世界信息基础设施计划”(Global Information Infrastructure)，这一宏伟的计划在2010年已经基本实现。法国、英国、德国、加拿大等西方国家及日本、韩国、新加坡以及中国台湾地区也先后提出了各自的信息高速公路计划。“信息高速公路”建设，将全球信息化推向了一个崭新的阶段，是世界进入信息经济时代的主要标志。①

1.1.2 高信息依赖导致高安全风险

现代信息技术的高度普及和应用，特别是互联网的广泛使用，极大地改变了人们的生产、生活和思维方式。在信息化日益深入的大趋势下，人们对信息的依赖程度越来越高，对伴随而来的信息安全威胁的担忧也越来越大。各种病毒、漏洞、信息窃取、网络攻击等威胁呈不断上升趋势，重大失泄密案件逐年上升，给国家政治、经济、文化和国防安全带来了新的挑战。通过

① 张琼，孙论强. 中国信息安全战略研究. 北京：中国人民公安大学出版社，2007.

这样几则散见于报章中的案例我们可以看到信息安全给我们带来的重大影响：

2009年1月，法国海军内部计算机系统的一台电脑受病毒入侵，迅速扩散到整个网络，一度不能启动，海军全部战斗机也因无法“下载飞行指令”而停飞两天。仅仅是法国海军内部计算机系统的时钟停摆，法国的国家安全就出现了一个偌大的“黑洞”，如果是一个国家某一系统或领域的计算机网络系统出现问题或瘫痪，这种损失和危害将是不可想象的。

2011年2月，伊朗突然宣布暂时卸载布什尔核电站的核燃料，但未披露具体原因。由于在核工业领域卸载未使用的核燃料非常罕见，因此舆论猜测原因是核电站系统遭受“震网”病毒攻击。据称，2010年夏季，伊朗纳坦兹核电站被一波又一波的“病毒”击中，伊朗近1 000个离心机一度瘫痪，这是美国首次使用网络战武器致使他国基础设施瘫痪。

美国于2012年发布的一份报告显示，在最新一轮的全球网络攻击中，黑客们将目标对准全球各地的企业和个人存款数额高的银行账户，从欧洲、美国和世界其他地区的共60多家银行中卷走6 000万欧元(约为人民币4.77亿元)。报告指出，这次名为“挥金如土者行动”的大规模网络攻击利用自动化等“成熟”技术，攻击银行的基于云计算服务器。在得手之后，被盗走的存款会以每笔数百至10万欧元的数额转移到派生账户上。据悉，最先遭到攻击的是欧洲银行，之后拉丁美洲和美国也相继出现账户被黑的情况，信贷协会、大型跨国银行和地方银行均未能幸免。

在信息时代，信息系统不安全，也就谈不上国家的整体安全，国家信息系统的不安全会使国家建设受到毁灭性的打击，并引发一系列连锁反应，例如政治动荡、经济紊乱、文化迷失、国防危机等，会使整个国家陷入危险的境地。人们越来越认识到，信

息安全已不仅仅是一个面向应用的单纯的技术问题，也不仅仅是某些黑客随意发动的个人行为，而是世界各国所共同面对的一个普遍和现实的问题，一个影响国家安全和长远利益的、亟待解决的重大关键问题。因此，对信息安全的研究已迫在眉睫。

1.2 信息安全的研究现状

现代信息安全是一个综合利用了数学、物理、通信、计算机、管理、政治、军事、经济等诸多学科成果的交叉学科领域，是一个典型的交叉学科。到目前为止，人们对信息安全的研究集中在如下几个层面：

信息安全技术领域的研究

信息安全技术是这个领域中成果最为丰富，研究也最为充分的一个领域，具体内容包括：密码理论与技术；安全协议理论与技术；安全体系结构理论与技术；信息对抗理论与技术；网络安全与安全产品等。据不完全统计，自 1979 年以来，在中国期刊全文数据库 CNKI 收录的国内学者关于“信息安全”的文章总数约数万篇，硕博士论文库所收文章数千篇；其中大部分都是从技术层面研究的成果。

信息犯罪和网络恐怖主义领域的研究

有的学者在分析现今网络固有特点后指出，随着网络技术的不断更新以及黑客技术与病毒传播的提高，网络恐怖主义和各种攻击日趋复杂多样，正成为国家安全、国际政治与国家关系中一个新的突出问题，世界各国都在普遍加大防范。①

---

① 俞晓秋. 全球信息网络安全动向与特点. 现代国际关系. 2002(2).

军事领域的“信息战”理论

信息战是为夺取和保持“制信息权”而进行的斗争，亦指战场上敌对双方为争取信息的获取权、控制权和使用权，通过利用、破坏敌方和保护己方的信息系统而展开的一系列作战活动。1992年美国国防部颁发的《国防部指令》首次提出信息战概念，掀起了世界性的信息战理论研究热潮。在该领域，美国和中国均走在了世界各国研究的前列。如今，信息战理论、方法和技术已日趋成熟，成为现代战争和高烈度对抗的主要模式，因此也是国家信息安全战略理论体系的重要来源。

政治领域的“信息主权”理论

信息主权是在国家主权概念上演化而来的，是信息时代国家主权的重要组成部分，它是指一个国家对本国的信息传播系统进行自主管理的权利。从政治视角看，信息主权是国家具有允许或禁止信息在其领域内流通的最高权威，包括通过国内和国际信息传播来发展和巩固本民族文化的权力，以及在国内、国际信息传播中维护本国形象的权力，还包括平等共享网络空间信息和传播资源的权利；从法律视角看，信息主权是指主权国家在信息网络空间拥有的自主权和独立权。它具体包括：主权国家对跨境数据流动的内容和方式的有效控制权；一国对本国信息输出和输入的管理权，以及在信息网络领域发生争端，一国所具有的司法管辖权；在国际合作的基础上实现全人类信息资源共享权。当前，国家信息主权作用日益凸显，相关理论更加丰富成熟，成为国家信息安全战略的重要理论基石。

信息安全运营管理方面的研究

为了保障信息安全，除了要进行信息的安全保护，还应该重