美国国家信息安全战略

蔡翠红 著

U.S. National Information Security Strategy

U.S. National Information Security Strategy

学林出版社

本书获复旦大学美国研究中心出版资助

美国国家信息安全战略

蔡翠红 著

U.S. National Information Security Strategy

ional Information Security Strategy

学林出版社

图书在版编目(CIP)数据

美国国家信息安全战略/蔡翠红著. —上海:学林出版社,2009.1

ISBN 978-7-80730-643-6

Ⅰ.美… Ⅱ.蔡… Ⅲ.信息系统—国家安全—战略—研究—美国 Ⅳ.D771.235

中国版本图书馆 CIP 数据核字(2008)第 171518 号

美国国家信息安全战略

著　　者——蔡翠红
责任编辑——乐惟清
特约编辑——唐发铙
封面设计——王国樑
出　　版——学林出版社(上海钦州南路 81 号)
　　电话:64515005　传真:64515005
发　　行——新华书店上海发行所
　　学林图书发行部(钦州南路 81 号 1 楼)
　　电话:64515012　传真:64844088
印　　刷——上海市印刷四厂
开　　本——640×965　1/16
印　　张——19.25
字　　数——25 万
版　　次——2009 年 1 月第 1 版
　　2009 年 1 月第 1 次印刷
印　　数——3000 册
书　　号——ISBN 978-7-80730-643-6/D·30
定　　价——30.00 元

内 容 提 要

本书选择以“美国国家信息安全战略”为题，对网络源起国美国的国家信息安全战略进行了全面系统的分析。作者首先从信息安全与信息安全战略的概念以及美国所面临的信息安全现实状况着手，概括了美国国家信息安全保障框架，分析了美国信息安全所关注的个人隐私权、密码政策、网络经济、网络执法等具体问题。接着又从国家战略层面剖析了美国信息安全战略三要素，即国家信息基础设施的保护、信息战、心理战与公共外交，比较了“9·11”事件前后的美国信息政策与信息安全战略方面的转变，即从克林顿政府的“主张发展优先”逐渐变化为布什政府的“主张安全优先”，从讲“适度安全”到“先发制人”。最后则解读了美国的《网络空间安全国家战略》，总结了各方对该战略的反应与评价，以及该战略的实施原则。综览全书，作者从不同侧面对美国国家信息安全战略进行了深度剖析，无论是对美国国家安全的研究还是对中国当前如何面对信息化挑战都具有一定意义。

U. S. National Information Security Strategy
ABSTRACT

This book explores the national information security strategy of the United States, which was the founder of the Internet and the pioneer in the information revolution. Starting with the concepts of information security and information security strategy, as well as the information security status quo confronting the U. S. , the book summarizes the framework of U. S. national information security protection and points out several key aspects concerning American policy such as privacy, encryption, Internet economy, as well as law enforcement in cyberspace. Then the book analyzes the three essentials of U. S. national information security strategy, i. e. , the protection of the national information infrastructure, information war and public diplomacy. The book also examines the transformation of U. S. national information security strategy before and after "9 • 11". While the Clinton administration focused more on development than security and adopted moderate information security measures, the Bush administration is more inclined to practice a preemptive strategy in information security. Finally, the book tries to shed light on U. S. *National Strategy to Secure Cyberspace*, and draws together the different views and comments on the Strategy before the conclusion of the principles underlining the strategy. In short, with the U. S. national information security strategy addressed from different aspects, this book is of great significance for the study of the U. S. national security as well as for the challenges faced by other nations including China in the information age.

序

20世纪90年代以来，计算机与互联网的迅猛发展给人们的生活方式、商贸的交易方式以及政府的运作方式、军队的作战方式都带来了革命性的变化，并加快了国家现代化和社会文明的发展。然而，互联网在为人们提供便捷、高效服务的同时，也对依赖其进行的国家关键信息系统和网络基础设施带来了巨大的风险。由于信息技术本身的特殊性，特别是信息和网络无国界性的特点，信息安全问题已成为信息产业发展的一大挑战。传统的信息安全概念已经被彻底改写，信息安全不仅是一个技术问题，而且是一个管理与控制问题，它涉及到国家安全、社会公共安全和公民个人安全的方方面面，是一个事关国家根本利益的战略问题。

本书作者选择了《美国国家信息安全战略》这一重要课题，从不同侧面对美国国家信息安全战略进行了深度剖析，对信息安全保障框架、国家信息安全战略要素、“9·11”事件前后美国信息安全战略转变以及战略实施原则等进行了研究分析与概括总结，因而无论是对美国国家安全的研究还是对中国当前如何面对信息化挑战都具有重要意义。具体而言，本书的重要性可以从如下三方面来理解：

首先是全球化网络化的趋势。从20世纪90年代开始，世界已经进入了信息化网络化时代，不仅人们的日常生活日益依赖于关

联和庞大的信息网络，而且国家的通信、能源、交通、航空、消防、金融等基础设施系统越来越多地利用信息网络传输数据并进行管理。由于网络自身的普遍性、跨国性、不可控性以及各系统之间的相互关联和依赖，信息安全已成为各国不得不面对的巨大安全威胁，成为一个现实而突出的安全问题，它直接涉及和影响到政治、经济、军事、文化等各个方面。正是因为一国的信息获取能力以及在社会生产和生活领域中的信息制控权或信息优势，成为这个国家在生存与发展竞争中能否占据主动的关键，所以信息安全问题逐渐受到世界许多国家政府和企业等方面的高度关注。信息安全战略因而成为整体国家安全战略的重要部分。

其次是传统安全向非传统安全的转变。冷战结束以来，世界战争，尤其是核战的威胁逐渐减弱，军备竞赛的吸引力逐渐下降，而全球经济和跨国公司的发展、各国经济的相互依赖、区域内经济合作及一体化的加快，以及生态环保、难民救助、走私贩毒、恐怖主义、信息爆炸等“全球性问题”的出现，使得各国安全面临着越来越多的全球性共同问题的影响和威胁，传统政治与军事安全问题逐渐让位于非传统安全。而“9·11”事件中恐怖分子对信息技术的纯熟运用使得人们开始重新思考信息传媒在政治输入输出系统中的意义，更使得国际恐怖主义以及与恐怖主义密切相关的信息安全等非传统安全因素作为一种非传统安全威胁，第一次取代传统军事安全威胁成为主要大国安全战略的重要议题。

最后是美国在全球安全及信息安全中的重要位置。美国是当今世界唯一的超级大国，它在政治、经济、军事、安全等方面处于独一无二的霸主地位，同时也占据了全球信息霸权地位。网络技术与标准诞生于美国，信息化浪潮最先发端于美国，并为美国所主导。在全球信息资源中，大部分都在美国发起、终结或通过，而英语也在网络资源用语中占了压倒多数中的一大半。全球网络管理中所有的重大决定也仍由美国主导作出。通过上述得天独厚的先天条件和这些丰富的网络资源，美国牢牢地占据了信息霸主的地位。它可以向全世界全方位、全天候地推销其意识形态从而提高

其软实力，可以借助信息技术手段为其国家安全提供服务。美国的信息霸权地位无疑是其他国家信息安全的威胁。因此，对于中国这样一个“后起之秀”和处于信息低位势的国家，适时抓紧对美国国家信息安全战略的研究对自身综合国力的提高和国家的安全稳定无疑有着相当的迫切性与必要性。

所以，从以上几个方面出发，我认为本书具有重要的研究意义。作者是我多年的学生、同事，从事该课题研究也有数载，如今能够以著述的形式将其思考凝聚成体系，实乃一大欣事。这不仅代表了作者个人的思想结晶，同时也是对传统侧重于政治、经济与外交的美国研究的重要补充。

是为序。

倪世雄*

2008年10月8日

---

* 倪世雄：曾任复旦大学国际关系与公共事务学院、国际问题研究院首任院长，美国研究中心主任，现为复旦大学美国研究中心教授、博士生导师，兼任教育部社科委委员、全国高校国际政治研究会副会长、上海市国际关系学会副会长、上海美国学学会副会长等职。先后出版《美国国际关系理论流派文选》、《国际关系理论比较研究》、《当代西方国际关系理论》等著作8部，并在国内外学术期刊上发表论文80多篇。

前　言

自古以来，信息就是政治活动的一个极为重要的组成部分。社会越发达，获取和散布各种政治信息（包括谣言）的方式就越多，政治宣传的手段就越有效。在现阶段，大大小小的信息战此起彼伏，甚至出现全球信息对峙和地区性信息冲突，信息战的形式早就不局限于散布谣言。信息安全问题不仅是一个纯技术性的问题，或一种恶意的个人行为，而是已经成为世界各国一个普遍的和共同的问题，成为信息时代中最基本、最核心、最重大的安全问题之一。信息安全也因此成为国家战略不可分割的重要组成部分。

媒体是信息的最有效载体。而第四媒体互联网的出现则使信息安全威胁与竞争越发严重与激烈。国家在网络空间享受着巨大的经济和政治利益，同样也在网上行使着它的权力，这个空间是国家生存和发展的新空间，与领土、领海、领空具有同等的经济、政治和军事意义。作为互联网的源起国，同时也作为当今世界的信息大国，美国的国家信息安全战略更加引人瞩目。

20 世纪 60 年代产生于美国的互联网将人类真正带入信息时代，“信息在我们的生活中非常重要而且很容易获得”①。信息是社会发展需要的战略资源，信息化已成为世界主要国家当今及今后

---

① Definitions of English Words “Information Age”, available at 〈http://www.antimoon.com/words/information_age-n.htm〉.

整体发展战略最优先的方面之一。国际上围绕信息的获取、使用和控制的斗争愈演愈烈，信息安全成为维护国家安全和社会稳定的一个焦点，各国都给以极大的关注与投入。各个关键性部门、产业和领域正在被网络连成一体，形成信息化国家的“关键性基础设施”，它包括政府部门，以及电力、交通、能源、通信、航空、金融、传媒、军事等领域和部门运作、计划、清算、支付、交换的信息系统。这使信息安全从一个产业问题上升为一个事关国家政治、经济、社会、文化、军事等各方面的核心问题。信息技术发展水平的高低和信息安全保障能力的强弱，成为重新界定国家实力、国家安全、国家主权和国际地位的实质依据。

约瑟夫·奈说，权力的性质已经由“高资本含量”变为“高信息含量”①。能够占据领导地位的国家并不是拥有最多资源的国家，而是那些可以控制政治环境并使别的国家“做其所想”的国家。他在1996年的《外交》双月刊中更明白地指出，美国在信息方面的优势将使21世纪成为最辉煌的美国世纪：“实际上，是21世纪，而不是20世纪，将会成为美国最辉煌的时期”。② 但与此同时，美国也意识到，美国的信息优势必须建立在信息安全的基础上，国家安全战略的主要内容之一就是维护信息安全。为此，20世纪80年代至今，美国已建立起一整套信息安全防范体系框架，并初步构建了其国家信息安全战略。

信息安全是一门技术科学，也是一门社会科学，它包括管理、行为动机等等。甚至有人说是一门艺术，因为没有一成不变的信息安全规则，也没有全球通用的信息安全解决方案，某种程度上安全只是安全管理人员、技术人员与信息使用者之间的一种妥协。但无论如何，信息安全战略，都可以被认为是信息系统的免疫系统。如果免疫系统不健全，整个系统将是无能的，甚至有害的。信息安全已成为亟待解决、影响国家大局和长远利益的重大关键问

---

① Joseph Nye, “Soft Power”, *Foreign Policy*, Fall 1990, p. 164.

② Joseph S. Nye, Jr. and William A. Owens, “America's Information Edge”, *Foreign Affairs*, March/April 1996, p. 21; p. 35.

题。如果信息安全问题解决不好，将全方位地危及一国的政治、军事、经济、文化、社会生活的各个方面，使国家处于信息战、信息恐怖和高度经济金融风险的威胁之中。

本书的目的就是以美国信息安全战略为考察对象，从美国信息安全状况、关注的问题、信息安全保障框架与战略要素，以及“9·11”事件前后信息安全战略的演变等方面全面分析美国国家信息安全战略，解读美国当前适用的“网络空间安全国家战略”，以期对我国信息安全发展有所借鉴与帮助。

本书共分七章。第一章为信息安全概论，对信息安全的实质与威胁、信息安全中需要处理的几对矛盾关系以及信息安全战略与传统安全战略之区别等基本问题进行了交代。信息安全需要应对的矛盾关系包括信息化与信息安全、管理与技术、应急处理与长效机制、信息安全体系的整体性与个别性、信息安全的成本与效益、国内信息安全与国际合作、信息安全与信息共享等等。

第二章针对美国的信息安全状况包括其现实严峻性、信息安全保障框架及关注的主要具体问题进行了初步分析。处处是前线的信息边疆使得美国无法享受天然的安全保障剩余；信息安全威胁的潜在性、瞬间性和多样性将非国家力量推向了美国国家信息安全的威胁主体之位；同时，美国对信息网络的高度依赖等因素使美国的国家信息安全更具严峻性和挑战性。美国信息安全是一个集技术、管理与法规于一体的综合框架。这一章还分析了美国信息安全的具体关注点，如个人隐私权、密码政策、网络经济问题与执法问题等。

第三章主要分析了美国国家信息安全战略三要素，即国家信息基础设施的保护、信息战、心理战与公共外交等方面。这些方面与美国国家安全目标，如提升网络恐怖活动的可抗性、进一步提高其制信息权，以及将信息战从军事领域转向全社会等初衷息息相关。

第四章和第五章对美国“9·11”事件前与“9·11”事件后的信息政策、信息安全措施与战略调整进行了比较分析。虽然“9·11”

事件前美国也提倡适度信息安全，在立法、行政与司法方面都推出了一些举措。然而总体来讲，出于冷战的经验和传播美国观念的传统，“9·11”事件前的美国还是更加注重推进信息自由流动与信息化发展，并为此提出了诸多计划与设想，如信息高速公路计划、全球信息基础设施计划、数字地球设想等。然而，“9·11”事件的发生彻底改变了美国的国家安全战略，信息安全的优先性得到了调整，布什政府为此推出了一系列的立法措施，以应对新的全球信息安全环境。

第六章主要对当前的美国国家信息安全战略文本，即《网络空间安全国家战略》进行了分析，总结了几方面的反应与评价，并归纳了该战略的实施原则，即公众参与原则、重点保护原则、风险预防为主原则、政府引导原则、国际合作原则、战略前瞻性原则等。

最后一章则将美国置于全球背景中，分析了其信息霸权地位，并对其他国家包括中国的信息安全政策进行了简要介绍。信息安全与信息自由流动有利于国际体系的和谐，而全球化时代国际体系的稳定也依赖于信息与信息安全的合作。因此，该章还简要介绍了目前一些国际信息安全合作机制。

由于笔者在信息安全技术知识方面的匮乏，所以本书仅仅从政策与战略层面对美国国家信息安全进行了剖析。当然，这也正是本书希望有别于一般信息安全著作的初衷所致。如果本书能够对关心美国国家安全、信息安全、国际政治等领域的相关学者同仁和读者朋友们有所帮助与启发，笔者将深感欣慰。

目　录