

2010

信息 灾害

发展中国家生存战略

沈伟光 著



新华出版社

2010 信息灾害

————发展中国家生存战略

◎沈伟光 著

新华出版社

图书在版编目 (CIP) 数据

2010 信息灾害：发展中国家生存战略/沈伟光著. - 北京：新华出版社，2005.1

ISBN 7-5011-6894-6

I. 2... II. 沈... III. 信息技术-研究-世界
IV. G202

中国版本图书馆 CIP 数据核字 (2004) 第 123497 号

2010 信息灾害
—发展中国家生存战略
沈伟光 著

新华出版社出版发行

(北京市石景山区京原路 8 号 邮编：100043)

新华出版社网址：<http://www.xinhupub.com>.

中国新闻书店：(010)63072012

新华书店经销

北京神剑印刷厂印刷

*

850 毫米×1168 毫米 32 开本 12.5 印张 202 千字

2005 年 1 月第一版 2005 年 1 月北京第一次印刷

ISBN 7-5011-6894-6/E·62 定价：23.00 元

目 录

上卷 战略报告：积极防御——保卫 国家信息疆域

序/3

前 言/11

第一部分 积极防御

第一章 理论/28

第一节 表述/28

第二节 方针/32

第三节 目标/34

第四节 原则/38

第二章 背景/43

第一节 未来的趋势/43

第二节 外来的威胁/46

第三节 内部的隐患/52

第三章 原理/59

第一节 信息空间的特性/59

第二节 积极防御原理/65

第二部分 保卫国家信息疆域

第一章 2010 年前十大目标/72

目标一：全面防范，有效遏制境内外的信息
攻击/72

目标二：加强管理，抑制内部涉密信息的泄漏/73

目标三：保护形象，防止领导人模型战争/75

目标四：落实制度，保护国家核心秘密信息/76

目标五：防反结合，打赢信息空间的局部战
争/78

目标六：搜集跟踪，主动控制有害信息/78

目标七：把握时机，实施专业信息反击/79

目标八：立足长远，建立信息空间的决定力量
层/80

目标九：着眼现实，确保台湾回归时的信息安
全/82

目标十：前沿遏制，形成强大的威慑能力/83

第二章 2010 年前十大任务/84

任务一：重构认知体系，完善战略构想/84	
任务二：设立国家信息安全保障部/86	
任务三：制定、完善现有的政策法规/88	
任务四：展开人才培养的战略行动/89	
任务五：加速构建信息化国防/90	
任务六：实现信息设施的国产化/91	
任务七：催化信息安全市场的成熟/92	
任务八：保持多元化的国际信息安全环境/93	
任务九：以综合演练完善防御/94	
任务十：遏制台湾信息战/95	
第三章 2010 年前十大重点突破方向/97	
突破一：从思维上突破，推进研究论证体系 建设/97	
突破二：从体制上突破，推进国家安全环境 建设/99	
突破三：从人才上突破，推进人才使用机制 建设/100	
突破四：从密码上突破，推进自主知识产权 建设/102	
突破五：从教育上突破，推进国民信息素质 建设/103	
突破六：从协作上突破，推进信息安全市场 建设/104	

突破七：从配置上突破，推进办公器材简化建设/105

突破八：从法律上突破，推进惩恶扬善法制建设/106

突破九：从内容上突破，推进中国信息平台建设/107

突破十：从顶端上突破，推进先进信息技术建设/108

第四章 信息化国防顶层结构设计/110

第一节 信息化国防总结构图/110

第二节 全球侦察情报中心/111

第三节 最高决策中心/115

第四节 中央指挥控制中心/117

第五节 战争资源中心/123

第六节 国家非战争行动中心/125

第七节 国家反恐指挥中心/127

第八节 国家安全教育训练中心/129

第九节 虚拟现实“理想战争”系统/131

第十节 国家信息安全中心/133

第五章 电子政务信息化建设构想/136

第一节 理论基础/136

第二节 几点构想/139

第三节 选择标准/141

第四节 一些建议/142

第六章 互联网建设构想/144

第一节 形成纵深系列的新闻网站发布梯次/145

第二节 以积极的网上引导求得内容的健康/146

第三节 依法管理、维护网上信息传播秩序/147

第四节 加强网站管理人员的培训和资质的评估/149

第五节 以制度与技术相结合来促进互联网的安全/150

第七章 2010 年到 2020 年中国信息安全规划/152

第一阶段：2010 年到 2011 年/152

第二阶段：2011 年至 2014 年/153

第三阶段：2014 年到 2017 年/154

第四阶段：2017 年到 2020 年/155

第三部分 附 件

附件一 电子政务信息安全解决方案/158

附件二 战区物资仓储管理系统整体解决方案/172

附件三 “分布交互式”联合作战虚拟现实系统整体解决方案/184

附件四 反恐指挥控制中心体系解决方案/190

- 第一部分 总论/190
 - 第一节 提出解决方案的背景/190
 - 第二节 方案需要遵循的原则/192
- 第二部分 顶层设计方案/197
 - 第一节 反恐指挥控制中心体系建设的主体思路/197
 - 第二节 顶层设计总体结构图/200
 - 第三节 顶层设计思路/201
 - 第四节 顶层设计的两大要求/203
- 第三部分 技术解决方案/205
 - 第一节 技术需求/205
 - 第二节 总体设计/207
 - 第三节 技术解决拓扑图/208
 - 第四节 系统的软硬件要求(略)/212
 - 第五节 系统性能/212
- 附件五 侦察(情报)参谋个人互联网系统解决方案/214
- 附件六 参谋人员协同办公集成系统 1.0 版解决方案/221

下卷 电视片：大风暴——信息安全与国防

背 景 篇

- 第一集：事件/238
- 第二集：信息化/248
- 第三集：信息战/258
- 第四集：信息安全/267
- 第五集：国家安全/276

挑 战 篇

- 第六集：信息安全与政治/288
- 第七集：信息安全与经济/296
- 第八集：信息安全与军事/304
- 第九集：信息安全与文化/312
- 第十集：信息安全与科技/319

对 策 篇

- 第十一集：信息安全观念/328

第十二集：信息安全战略/335

第十三集：信息安全法制/344

第十四集：信息安全管理/353

第十五集：信息安全技术/360

第十六集：信息安全产业/368

第十七集：信息安全人才/376

第十八集：保卫信息主权/384

积极防御——保卫国家信息疆域

战略报告

上卷



序

今天，分析国外尤其是美国在信息安全上的战略认知历程、政策编制情况、行动纲领执行等方面的经验与教训，再结合中国当前的国情，尤其是信息空间所面临的威胁与挑战，更加深切地感到，制定中国信息安全战略迫在眉睫，刻不容缓。

我从 1985 年开始研究信息战和信息安全问题至今，在所有的研究报告中都提出，应尽快建立有中国特色的信息安全战略。从 2002 年 8 月起，我就着手《中国信息安全战略》的研究和撰稿。我认为，制定中国特色的信息安全战略，目的是要规划中国信息安全领域“跨越式”发展的目标及思路，以利于我们根据这个战略来实施保护国家利益的重要行动——保卫中国的信息疆域，维护国家的信息主权。

据此，制定中国特色信息安全战略的基本依据是：

一、对形势的科学判断

首先是对中国国情的分析。什么叫中国国情？除了地大物博人多底子薄以外，最大的国情是，中国是社会主义国家，是中国共产党领导。因此，我们除了考虑物质上的因素以外，还应着重考虑精神上的因素，多从政治上看待信息安全问题，这样，信息安全的重点就不难把握。

其次是对中国经济及信息化发展的预测非常重要。

尤其是对世界形势的分析，就是对中国发展外部环境的正确把握。像小平同志 1985 年提出“有可能 20 年大战不打”这样的战略判断，对中国的发展很重要。20 年已经到了，现实世界是个什么样子，未来的走向如何？

还有对信息安全形势的正确判断。例如，信息安全是不是无国界的，是不是非传统领域安全问题，这些都应有正确的认识，这对战略的规划有重要影响。我个人认为，信息安全是有国界的，否则就不存在安全问题。和平演变问题，文化的民族性问题，意识形态领域的分歧，都是信息安全范畴内的事，是有界限和有约束的。事实上，世界各国、团体，甚至个人，在信息化这块新大陆上跑马圈地

运动早就开始了，我在 20 年前就说过这个问题。信息安全不从属于信息化，也不是非传统安全领域问题。不搞信息化的时候也有信息安全问题，只是由于信息的社会化和信息战的出现，信息安全的外延扩大了，内涵丰富了，在国家安全的地位也由次要位置上升到重要位置。与其他安全不一样，信息安全可以使一个国家或民族实现精神死亡，文化、宗教、意识形态等方面的冲突都可以归到信息安全范畴。

这些都是关系到我们如何设置战略目标等重大问题。目标永远是手段一致的，有多大能力就办多大事。

二、对战略的正确定位

战略的制定，应包含两大内容：一是战略表述，二是战略计划。具体制定中应把握几点：

第一，应有责任感。信息安全影响是极其深远的，信息安全不能得到保障，国家就会经济紊乱、政治失稳、军事失效、技术落后，进而影响到国家的综合实力和国际地位。信息安全问题是当今世界涉及面最广，危险性最大的社会问题。信息安全战略的选择是关系到我们国家和民族生死存亡的大问题，我们应从维护国家主权的高度去认识信息安全

问题，正确制定我们的战略。美国的飞机、卫星对我进行侦察，这算不算侵犯我国的主权？法轮功分子破坏我鑫诺卫星，这与向我境内丢几颗炸弹有什么区别？我们的战略、法律应该有对策。全世界都知道：信息是财富，是资源。你偷窥我就是侵犯我的隐私，你破坏我获取信息的渠道，你偷我的信息就是掠夺我的财富，这些就是违法的。对此，还没有针对性很强的国际法，取证也较难，但我们要有准备，要有办法。只要我们制定了有关法律，并向世界予以公布，就会有一定的威慑作用。一旦证据确凿，坚决予以反击，任何手段都可以用。

第二，应有未来意识。战略制定的本身就是对未来的研究，信息安全是一个动态的概念，不会静止不变，不可能一劳永逸的。在不同的时代和不同的社会发展阶段，信息安全有着不同的内容和重点。积极防御防谁，是美国还是台湾，重点是防外部还是防内部，应明确界定。例如，信息社会是一个开放性的社会，随着信息化程度的提高，社会的开放性更大。我们在制定信息安全战略时，不能违背这个趋势，更不能做阻挡社会前进和让后代讥笑的事。

第三，应切实可行。首先要搞清楚什么是信息安全，信息安全到底有多大？而更多是一个看不见