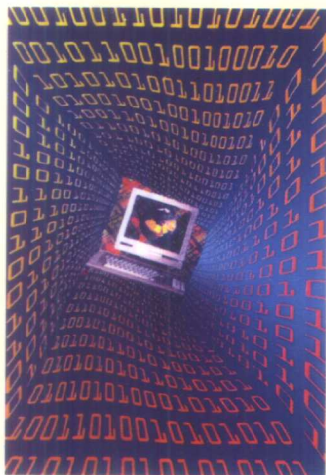


国家信息安全报告

GUOJIA XINXI ANQUAN BAOGAO

张春江 倪健民 主编



人民出版社

国家信息安全报告

张春江 倪健民 主编

人民出版社

图书在版编目(CIP)数据

国家信息安全报告/张春江,倪健民著.
-北京:人民出版社,2000.5
ISBN:7-01-003209-2

I. 国… II. ①张…②倪… III. ①信息资源-国家安全②计
算机网络-安全 IV. G202

中国版本图书馆 CIP 数据核字(2000)第 60696 号

国家信息安全报告

张春江 倪健民 主编

人民出版社出版发行

(100706 北京朝内大街 166 号)

北京第三印刷厂印刷 新华书店经销

2000 年 5 月第 1 版 2000 年 5 月第 1 次印刷

开本:850×1168 毫米 1/32 印张:10

字数:237 千字 印数:5000 册

ISBN:7-01-003209-2/T·2

定价:18.00 元

<http://www.peoplespace.net>

构筑面向 21 世纪的国家信息安全体系

(代序)

吴苍凌

当今世界，科学技术飞速发展，特别是信息技术，正在以前所未有的速度广泛应用于社会经济生活的各个领域，引起了人们生活方式、生产方式和思想观念的巨大变化，有力地推动着人类的社会发展和文明进步，信息化水平已成为衡量一个国家现代化和综合国力的重要标志。伴随着信息技术与信息产业的发展，网络与信息安全问题及其对经济发展、国家和社会稳定的重大影响，正日益突出地显现出来，受到越来越多国家的关注。我国是发展中国家，信息产业尚处于起步阶段，必须加强信息安全工作，构筑面向 21 世纪的国家信息安全保障体系，这在世纪之交的今天，无疑具有十分重要的战略意义。

近年来，我国信息产业持续快速发展，通信网络规模、技术层次和电子信息产品制造业综合实力发生了质的飞跃，通信与信息服务的普及程度有了很大提高，信息技术的应用范围不断扩大。到 1999 年底，全国固定电话和移动电话用户分别达到 1.1 亿户和 4324 万户，电话普及率为 13%，城市电话普及率为 28.4%，通电话的行政村比重达到 79.8%；计算机拥有量约 1400 万台；因特网专线及拨号用户达到 890 万户，国内网上中文站点超过 15000 个，已注册的各级政府网站达到 2300 多个；

金融、外贸、海关、税务、科技、教育等近百个部门和行业组建了全国性计算机应用系统。信息产业在促进经济发展、调整经济结构、改造传统产业和提高人民生活质量等方面发挥了不可替代的重要作用。

同时也要看到，互联网络是以统一的 TCP/IP 协议为规则运作的，是一个对全世界所有国家开放的网络，任何团体或个人都可以在网上方便地传送和获取各种各样的信息，而由于网络迅速发展而自身的安全防护能力很弱，许多应用系统处于不设防状态，存在着极大的信息安全风险和隐患。网络在为人们提供便利、带来效益的同时，也使人类面临着信息安全方面的巨大挑战。近年来，利用网络进行意识形态与文化观念的渗透，以及从事违反法律、道德的活动等问题日益突出，各类计算机犯罪及“黑客”攻击网络事件屡有发生，手段也越来越高技术化，从而对各国的主权、安全和社会稳定构成了威胁。这些问题在我国也程度不同地存在，有些方面还相当突出，特别是随着加入 WTO 的临近，我国将进一步对外开放，各方面的国际交流日益增多，我们在信息安全方面将面临更大的压力和挑战。

计算机互联网络涉及社会经济生活各个领域，并直接与世界相联，可以说是国家的一个“政治”关口，一条经济“命脉”。网络与信息安全已上升为一个事关国家政治稳定、社会安定、经济有序运行和社会主义精神文明建设的全局性问题。从这一意义上讲，信息安全保障能力是 21 世纪综合国力、经济竞争实力和民族生存能力的重要组成部分。因此，我们必须在进一步提高认识的基础上，跟踪世界信息技术发展趋势，面向下个世纪我国信息化建设的需要，努力构筑一个技术先进、管理高效、安全可靠、建立在自主研究开发基础之上的国家信息安全体系，以有效地保障国家安全、社会稳定和经济发展。为此，要从多方面入手，提高信息安全管理整体水平：

第一，加强国家信息安全管理机构及职能，加快信息安全立法。信息安全关系国家利益，必须实行强有力的政府管理。我国政府对网络与信息安全问题一贯给予高度重视，近年来出台了一

系列法规和政策，有关主管部门做了大量工作，收到了积极的成效。今后，要在国务院统一领导下，进一步加大政府对信息安全管理力度，加强各部门之间的协调与配合，研究确定有关信息安全的规划、政策及技术规范、标准等，及时处理有关的重大问题。作为国务院信息产业主管部门，信息产业部要认真履行国家赋予的职责，下大力气加强管理，维护网络与信息安全。同时，要加快信息安全立法，逐步建立信息安全法律体系，以充分发挥法律在打击网络犯罪、维护信息安全方面的作用。还应努力倡导建立公正、公平的国际信息安全体系，在国际社会的范围内为我国信息安全争得一个有利的外部环境。

第二，各运营者要强化防范意识，切实保障网络与系统的安全。作为网络和应用系统的建设、运行和维护单位，网络运营者是信息安全保障的主体，必须在思想上高度重视，真正负起责任。信息基础网络正在积极向下一代网络演进，在这一过程中，应从维护国家信息安全的高度出发，从网络组织、技术装备、运行维护等方面采取有效措施，保证网络的安全性、可靠性，增强网络在各种情况下的抗打击能力。各应用部门要从技术、管理等方面加大力度，建立和完善规章制度，尽快解决安全隐患，改变目前许多应用系统普遍存在的不设防状态，对引进的信息技术设备也要从保护信息安全出发，进行必要的技术改造，以提高网络和系统自身的安全防范能力。

第三，建立专业化服务机构，加强信息安全的社会保障。网络与信息安全属于高科技领域，涉及技术、管理等各个方面，需要大量专门的知识经验，因而发展专业化的经营服务机构，对于有效防范和及时解决各类信息安全问题，是必不可少的。国外在这方面有一些有益的作法，我们应认真借鉴，并结合国情积极探索。针对我国网络与信息安全方面存在的问题，当务之急，是要建立一批企业化运作的信息安全服务机构，其职责主要是通过技术手段，对网络和应用系统的运行进行经常性的巡查、搜索、监测，预防可能出现的安全问题，帮助解决存在的安全隐患，对“黑客”和病毒入侵网络问题及时进行有效的治理，从而起到

“网络警察”和“网络医院”的作用。这样，就可以实现自我防范与外部保障的有机结合，有效地提升我国信息安全的整体能力。

第四，以核心技术攻关为重点，加大信息安全技术研发力度。一个国家的信息安全能否得到有效的保障，根本问题在于其综合国力的高低，在于信息基础设施的发达程度，在于自主研发与创新能力的强弱，这些是构筑信息安全体系的物质基础。目前我国网络与信息安全的防护能力处于发展的初级阶段，应立足于发展信息安全产业，加强基础研究，抓好当前急需的关键技术的科研攻关，重点是大力发展独立自主的软件产业，提高信息安全技术自主研发能力，全力推进技术创新，尽快改变核心技术受制于人的状况。应实行国家投入、部门投入与社会融资相结合，建立发展基金，引进风险投资，推进科研成果的产业化，同时加强国际合作，实行引进、消化吸收与自主创新相结合，以形成有我国自己特色的、先进可靠的信息安全技术和装备体系，为国家的信息安全提供强有力的技术支撑。

第五，高度重视人才问题，提高全社会信息安全意识。信息安全属于高技术范畴，防范和抗击各种网络犯罪活动，离不开一支高素质的信息安全专业队伍，离不开一大批能够跟踪世界先进技术发展的骨干力量，特别是在相应的软件开发方面，对人才的要求比一般操作软件、运行软件更高，而这正是我们当前一个突出的薄弱环节。必须下大力气，采取多种形式，加强信息安全专业人才的培养，努力为专业人才的成长创造必要的科研和生活条件，并采取政策措施，鼓励出国人员和华人、华侨为国服务或归国服务，以吸引人才，留住人才，更好地发挥各类专业人才的作用。同时，要加强信息安全知识的普及和教育，提高各部门、各单位和广大人民群众保护信息安全、防止网络泄密的意识，在全社会形成关心信息安全、维护信息安全的良好氛围。

构筑国家信息安全体系是一项跨世纪的战略任务，也是一项艰巨复杂的系统工程。在新世纪即将来临的今天，对信息安全问题进行全方位、深层次的研究和探讨，从战略的高度提出对策和

建议，有助于各方面统一思想认识，有助于制定正确的符合实际的方针政策，是一件很有意义的工作。我相信，在以江泽民同志为核心的党中央正确领导下，有各方面的广泛参与，信息安全和信息化建设一定会开创新的局面，从而促进我国改革开放和现代化建设事业在新世纪取得更大的发展。

目 录

构筑面向 21 世纪的国家信息安全体系(代序)…… 吴基传

绪论 信息化发展与我国信息安全战略	(1)
信息化的发展态势与趋势	(1)
信息化对国家安全、社会稳定和 民族文化的影响	(3)
世界主要国家信息安全战略与信息安全研究	(6)
我国信息安全面临严峻形势	(11)
我国信息安全战略对策的几点建议	(16)
第一章 信息时代的世界格局与中国的 信息安全战略	(23)
人类进入信息时代	(23)
信息社会的七大特征	(24)
信息时代的新内涵	(25)
信息技术对世界格局的影响	(27)
信息垄断与信息霸权国家	(29)
霸权周期的理论	(29)
信息技术优势与制信息权	(30)
信息霸权的基本特性	(32)
信息时代的信息主权国家	(37)
从“三个世界划分”理论谈起	(37)

信息主权国家的主要特征	(38)
全球化与信息殖民地国家	(41)
经济全球化与全球信息化	(41)
因特网与电子殖民主义	(43)
信息殖民地国家的基本特征	(44)
信息时代中国的信息安全面临严重挑战	(46)
对信息安全概念的几种解读	(47)
我国信息安全目前存在的问题	(50)
紧约束环境	(52)
捍卫信息主权是中国在信息时代的战略选择	(54)
中国捍卫信息主权的优势	(55)
捍卫信息主权应做几件大事	(57)
第二章 信息安全在国家经济安全中的作用	(59)
信息化带来的契机	(59)
海外折射出来的信息化光环	(59)
中国紧跟国际信息化的大潮	(67)
信息安全存在的问题严重威胁着经济安全	(71)
“千年虫”(Y2K)问题	(71)
系统软件硬件存在缺陷:一个比 Y2K	
更持久的风险——“臭虫”(BUG)	(76)
计算机病毒猖獗泛滥	(82)
黑客行为和白领犯罪对信息化环境的威胁严重	(88)
数字化信息空间秩序混乱令人担忧	(99)
信息战成为关注的焦点	(105)
信息安全对国家经济安全的作用	(118)

第三章 我国各领域的信息安全问题分析	(121)
经济领域的信息安全问题	(122)
经济秘密成为间谍活动的新焦点	(122)
电子商务安全问题	(126)
通信安全问题	(131)
在信息革命背景下,中国战略产业面临考验	(136)
信息安全问题是金融电子化成败的关键	(137)
意识形态领域的信息安全问题	(142)
电子媒介成为国际意识形态斗争的主导工具	(142)
新闻媒体是西方宣扬其主流意识形态的利器	(146)
当今国际信息传播的主流仍然被西方所控制	(148)
美国要控制国际传媒的意图从来没有改变过, 在因特网上更是如此	(149)
军事领域的信息安全问题	(151)
网络泄密是军事信息安全问题的重要表现	(151)
黑客攻击对军事信息安全危害极大	(152)
信息战是影响军事信息安全的极端表现形式	(160)
第四章 信息与网络安全体系的构建	(173)
信息安全及信息与网络安全体系的构成	(173)
信息安全的技术支柱	(177)
密码是核心	(177)
安全体系结构是基础	(201)
协议是桥梁	(218)
芯片是关键	(227)
管理监控是保障	(231)
检测评估是考验	(234)

高技术信息安全人才	(238)
-----------------	-------

第五章 中国信息安全管理与自主的

信息产业建设	(243)
中国信息产业发展的现状	(243)
独立的信息产业已经形成并初具规模	(243)
信息产业发展环境日益改善,信息市场初步形成	(244)
信息产业国际化发展步伐不断加快	(246)
中国信息产业发展过程中存在的主要问题	(246)
信息产业与信息安全管理	(249)
信息产业的几个重要特点	(250)
信息安全的分层管理	(251)
信息安全管理本身就是正在发展的信息产业	(254)
关于信息系统中的“后门”问题	(255)
政府与设备生产厂家之间的约定	(256)
信息产品国产化有利于信息安全	(256)
信息产品国产化不等于信息安全	(256)
信息安全的发展必须产业化	(257)
信息安全几个值得注意的问题	(257)
信息安全管理对策	(259)
信息产业国产化的必要性和可行性分析	(260)
从信息安全对信息产业的影响分析	(260)
从信息产业的特点分析	(261)
从国际合作关系分析	(261)
从计算机网络安全等级分析	(262)
我国自主雅息产业建设的思考	(262)
积极创造条件,建设我国的自主信息产业	(262)

根据信息安全等级确定信息产业国产化重点·····	(267)
信息安全的对策主要是建立自主的安全快速 防范体系·····	(268)
大力扶植操作系统的国产化,目前的重点是 扶植嵌入式操作系统的国产化·····	(268)
信息安全的科研项目必须与信息安全产业从 开始就紧密结合·····	(269)
建立一套严格而有效的信息安全认证体系·····	(269)
以有限的政府资源带动无限的社会资源·····	(269)
第六章 信息安全的法制建设 ·····	(271)
各国信息安全管理与法律法规 ·····	(271)
我国的信息安全管理与法制建设 ·····	(284)
信息犯罪及其预防 ·····	(292)
信息犯罪形势严峻·····	(292)
信息犯罪的基本类型·····	(293)
信息犯罪的主要特征·····	(296)
信息犯罪的法律对策·····	(299)
现代信息法制建设 ·····	(301)
信息法的特征·····	(301)
信息法的体系结构·····	(303)
信息安全立法的思考·····	(303)
后记 ·····	(307)

绪论

信息化发展与我国信息安全战略

信息是社会发展的**重要战略资源**。在信息社会中，信息是维持社会活动和经济活动以及生产活动的重要资源，并成为政治、经济、社会、文化等一切领域的基础。谁更多地掌握和控制信息这一重要资源，谁就能取得信息社会的主动权。当前，国际上围绕信息的获取、使用和控制的斗争愈演愈烈，网络与信息安全已成为影响国家安全和社会稳定的重大关键问题。

信息化的发展态势与趋势

人类文明起源于“沟通”，电信科技连接全世界，促成了现代文明，而未来文明将由网络主导潮流。90年代以来，信息化的狂潮席卷全球。人类无可置疑地向着信息时代迈进。生产活动与社会活动的通信化、电脑化与自动化，从而构成强大而又灵活的信息网络是这个时代的主要特征。信息产业在国民经济中起着主导作用，通过终端设备和计算机网络，通过因特网，把所有的产业部门、企业都联系起来，形成一种新的生产格局，知识成了

经济活动的“血液”。

电话自发明以来，花了 75 年才累积了 5 千万名用户。达到这个数目，收音机用了 35 年，电视与移动电话则各用了 13 年与 12 年；但是，网络却只花了 4 年的时间。据预测，到 2005 年时，全球因特网用户将超过 5 亿人。

在美国，酝酿于 80 年代的信息高速公路，在克林顿政府的倡导下成为其国策。他们于 1993 年提出了国家信息基础设施 (NII) 的国家规划，继而又提出全球信息基础设施的构想，引起国际上的高度重视。美国商务部发表的一份报告认为，数字世界正在推动美国经济的增长，并抑制了通货膨胀率，改变着美国人的工作环境。报告指出，信息技术业，在 1995 年至 1998 年间虽然只占国家经济总产出的 8%，但占国家经济增长率的 1/3 强。报告预计，到 2006 年，将有半数的美国工人受雇于信息技术业或是信息技术的主要使用者。在数字技术的推动下，随着因特网等网络技术的深入发展，电子商务已从概念步入人们的实际生活，出现了网络经济的概念。电子商务作为一种新型的商业运作模式，是当代信息社会中网络技术、电子技术和数据处理技术在商贸领域中综合应用的产物，是国民经济和社会信息化的一个重要组成部分。作为一种崭新的推动未来经济增长的关键动力，它必将成为 21 世纪经济活动的核心。信息革命对于经济的深远影响将足与工业革命带来的社会变化相匹敌。电子网络不久即可使人们跨越时空障碍，将再次鼓变人类的生活。

21 世纪，信息化必将成为全球的重要特征。信息化空前地提高了人类认识世界和改造世界的的能力，将带来经济管理、思想观念、生活方式等各方面的重大变化。处在工业化进程中的我国也将不可避免地被推进到信息化的世界大潮中，这种大趋势是不可逆转的，如果我们不采取积极有力的措施，必然会丧失主动，再度落后。只有采取工业化和信息化并举、以信息化促进工业化

的方针，才能带动国民经济健康、持续发展。

在信息时代，知识即意味着财富和实力。信息时代的到来，从多方面影响着世界各国国家利益的构成和内涵。信息本身成为国家利益的一个组成部分，信息量成为衡量国家间利益均衡的一个重要参数，对信息的开发、控制和利用成为国家间利益争夺的重要内容。可以肯定地说，互联网已经成为继南极洲、外层空间之后，引发新一轮国际竞争的新的战略空间。

在信息化的进程中，国家的安全与经济的安全越来越不可分割，经济安全越来越依赖于信息化基础设施的安全程度。高度发达的电子信息系统将成为国家经济发展的重要支柱和动力，成为提高社会生活质量的基础设施，在国家经济安全中有着举足轻重的地位和作用。数字化、网络化和计算机的广泛应用是电子信息系统的显著特征，信息的采集、存储、处理、传输、认证等方面和传统方式有着根本的区别，因此，保证电子信息的有效性、安全性成为突出的重大问题。如果不能保障信息安全，就不可能获得信息化的效率和效益，在国际“信息战”威胁和国内外高技术犯罪的干扰破坏下，社会的经济生活就难以健康、有序地进行，国家的安全更无法确保。

信息化对国家安全、社会稳定 和民族文化的影响

信息安全保障能力是 21 世纪综合国力、经济竞争实力和生存能力的重要组成部分，是世纪之交各国奋力攀登的制高点，各国都给以极大的关注与投入。在不远的将来，网络将成为人类基本的工作方式和生活方式，并将决定个人、企业、国家乃至全球的生存方式，全球网络基础设施将成为未来人类文明的全新平

台，而信息技术是这一基础设施的支柱。因此，信息技术的国家发展战略，早已从一个产业问题上升为一个事关国家的社会、文化、军事等各方面的核心问题。今后，各国信息技术的高下将成为重新界定国家实力、国家安全、国家地位和国家主权的实质依据。同时，也只有从信息技术的发展走势入手，才能真正洞察国际关系和国内社会各领域的全新内涵。

当代社会进入信息社会，出现了三类国家：一是信息霸权国家，以信息技术与网络技术为基础推行霸权主义，主要表现在电信霸权、软件技术霸权、信息利润霸权和网络霸权几个方面。二是信息主权国家，有独立的信息主导权、独立的信息利润和防范信息霸权的手段。三是信息殖民地国家，被动地接受别国的信息，受到霸权国家的信息剥削，没有防范信息霸权的能力。

我国信息技术和信息产业发展与技术先进国家存在较大的差距，我国信息化建设需要的大量基础设备依靠国外引进，这种状况在今后相当长的时期内还不能彻底改变。引进设备中的核心芯片和系统内核逻辑编程都掌握在他人之手，无法保证我们的安全利用和有效监控。当前复杂多变的国际形势，进一步暴露了霸权主义国家亡我之心不死。他们除了利用传统的军事经济优势达到他们的目的外，正在利用他们拥有的信息技术优势实施信息霸权，企图遏制我们的发展，剥夺我们的资财，摧残我们的文化，打击我们的政治、军事和经济。

信息安全涉及到政治、经济、军事、文化等方方面面，由于互联网发展在地域上极不平衡，信息强国对于信息弱国已经形成了战略上的“信息位势差”，居于信息低位势的国家的政治安全、经济安全、军事安全乃至民族传统文化传统都将面临前所未有的冲击、挑战和威胁，互联网成为超级大国谋求跨世纪战略优势的工具。“信息疆域”不是以传统的地缘、领土、领空、领海甚至领天来划分，而是以带有政治影响力的信息辐射空间来划分。“信