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，引发又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饲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

息疆域”的大小、“信息边界”的安全，关系到一个民族、一个国家在信息时代的兴衰存亡，因此，拓展“信息疆域”，加强信息辐射的广度和深度，保卫“信息边疆”，加强国家信息安全保障能力，构筑强固的“精神防线”成为至关重要的问题。在知识经济时代，一个国家的信息获取能力及在社会生产生活领域中的“制信息权”将成为这个国家在新世纪的生存与发展竞争中能否占据主动的关键。

信息技术的飞速发展，尤其是“全球信息高速公路”即国际互联网络的迅猛发展，使国际间的信息交流日益便利、迅捷，有力地促进了经济全球化趋势的发展，给发展中国家带来了机遇，但同时也带来新的问题与挑战。有些西方大国利用信息及信息传输技术优势，妨碍、限制、压制和破坏其他国家对信息的自由运用，甚至利用信息把本国的价值观念、意识形态强加于别国头上，以谋求政治军事手段难以得到的霸权利益。它们利用在信息领域的主宰地位，通过互联网络上的电子邮件、电子报刊及其他信息媒体展开新一轮的宣传战、心理战。政策渗透、“文化侵略”严重威胁着发展中国家的政治、科技、文化安全。可见，在全球信息化浪潮推动下，社会日益网络化，政治、经济、军事、科技、文化联为一体，互为目的，互为手段，它们之间的传统界线正变得越来越模糊，国家面临着严峻的信息安全问题。

从本质上讲网络属于人类。它不属于某个国家、某个政府或某个国际组织，从而也不存在以上意义的行政主管。但是现实世界是由不同的国家组成的。政治、经济、军事利益使他们要维护各自的疆界，信息空间跨越了传统意义的原有疆界，即便出于和平与发展目的的应用，在许多实际应用操作中也需要国家之间的配合与协调。国际上出现有关跨国跨地区的组织，就商业和经济目的商讨信息安全对策的现象说明了这是历史的必然。我们要在维护国家主权的前提下参与国际合作，提出代表自身利益和发展

中国家利益的主张，对抗信息时代的信息霸权主义、网络霸权主义，维护世界和平与发展。

世界主要国家信息安全战略与信息安全研究

从国际现状看，各国政府逐渐意识到信息安全风险对其国家利益可能带来的威胁，因此都在为自身的安全进行努力。一些国家由于信息系统应用早，范围广，安全事件已经多次发生。这迫使他们必须重视安全，加强安全措施。

美国一方面重视其国家信息安全，另一方面积极谋求其信息霸权。美国提出的“全球信息基础设施”中有这样一段话：“高速发展的‘全球信息基础设施’将促进民主的原则，限制极权主义的政权形式的蔓延；世界上的公民，通过‘全球信息基础设施’，将有机会获得同样的信息和同样的准则，从而使世界具有更大意义上的共同性。”美国不仅要使自己的经济和科技在新世纪站在世界前沿，而且要利用因特网使自己的价值观成为全球的标准，维护其政治、经济、军事和信息霸权利益。为保障其国家信息安全，美国提出了“国家信息安全保障“的政策，也是一个类似全民防御的政策。它的基本观点是：用支持信息空间安全的意识培训和教育来作为国家这一领域的启蒙；在信息系统和网络中使用强密码来实现包括数字签名（认证和完整性）和加密技术（个人隐私）；开发和使用良好的商业化安全信息技术产品和服务；全球信息安全管理基础设施；防御基础设施，包括国家攻击判断和预警能力及协调响应技巧。他们认为， 21 世纪初期国家防御系统将严重地依赖于同样是商业的民用的信息基础设施。因此，他们把信息安全保障的希望首先寄托于人才培养。同时，为

适应信息化应用的社会化、国际化的形势，从 80 年代开始，建立了一些社会性的安全机构，体现了信息安全的群防群治的趋势。与别的国家相比，美国无疑是信息安全方面的法案最多而且较为完善的国家。它早在 1987 年就再次修订了计算机犯罪法。该法在 80年代末至 90年代初被作为美国各州制定其地方法规的依据，这些地方法规确立了计算机服务盗窃罪、侵犯知识产权罪、破坏计算机设备或配置罪、计算机欺骗罪、通过欺骗获得电话或电报服务罪、计算机滥用罪、计算机错误访问罪、非授权的计算机使用罪等罪名。美国现已确立的有关信息安全的法律有：信息自由法、个人隐私法、反腐败行径法、伪造访问设备和计算机欺骗滥用法、电子通信隐私法、计算机欺骗滥用法、计算机安全法、正当通信法、电讯法等。

德国是欧洲信息技术最发达的国家，其电子信息和通讯服务已涉及该国所有经济和生活领域。由于因特网在电子信息和通讯服务行业中的重要性，德国政府在其发展的初始阶段即对其立法进行规范。1996 年夏，德国政府出台了《信息和通讯服务规范法》,即《多媒体法》。此外,该国政府通过了电信服务数据保护法，并根据发展信息和通讯服务的需要对刑法法典、治安法、传播危害青少年文字法、著作权法和报价法作了必要的修改和补充。

法国作为欧洲大陆的主要国家之一，在因特网的使用上却起步较晚。此前，它使用的是自建的一套商业电讯系统。在意识到因特网的重要性及其存在的问题之后，法国政府积极地关注因特网的发展并制定了有关法律。1996 年 6 月，法国对一部有关通讯自由的法律进行补充并提出修正案。该法案根据互联网的特点，为在互联网从业人员和用户之间自律解决互联网带来的有关问题提出以下三方面措施：迫使上网服务的网络信道提供者向客户提供封锁某些信道的软件设备，从而使成年人通过技术控制对

未成年人负责；建立一个委员会负责制定上网服务的职业规范，对被告发的服务提出处理意见，特别是重新负责原由网络信息委员会管辖的终端视讯服务；若网络信道提供者违反技术规定，为进入已存异议的上网提供信道，或在知底的情况下为被控告的服务进入网络提供信道，则追究其刑事责任。

英国为了打击网上犯罪活动，政府采取了以下一些监管措施：加强法律规范，加大打击力度；对网络提供者提出具体、严格的要求；网络监察部门对网上内容进行合法性鉴别；对网上非法资料作出严肃处理；加强研究开发工作，研制适合国情的监控软件和电子设备。1996 年 9 月 23 日，英国政府颁布了第一个网络监管行业性法规《三 R 安全规则》。“三 R”分别代表分级认定、举报告发、承担责任。法规旨在从网络上消除儿童色情内容和其他有害信息，对提供网络服务的机构、终端用户和编发信息的网络新闻组，尤其对网络提供者作了明确的职责分工。英国政府 1999 年又公布了《电子通信法案》的征求意见稿。这一草案酝酿已久，其主要目的是为促进英国电子商务发展，并为社会各界树立对电子商务的信心提供法律上的保证。

俄罗斯于 1995 年颁布了《联邦信息、信息化和信息保护法》。法规强调了国家在建立信息资源和信息化中的责任是“旨在为完成俄联邦社会和经济发展的战略、战役任务，提供高效率高质量的信息保障创造条件”。法规中明确界定了信息资源开放和保密的范畴，提出了保护信息的法律责任。

新加坡于 1996 年 7 月 11 日宣布对互联网络实行管制，宣布实施分类许可证制度。该制度自 1996 年 7 月 15 日起生效。它是一种自动取得许可证的制度，目的是鼓励正当使用互联网络，促进其在新加坡的健康发展。它依据计算机空间的最基本标准谋求保护网络用户，尤其是年轻人，免受非法和不健康的信息传播之害。新加坡新闻与艺术部还成立了一个“全国互联网络咨询委员

会”，以便处理有关互联网络和电子信息服务的事务。

日本目前已经编制出一套准则：防止越权访问计算机网络。建议计算机使用者避免以出生日期和电话号码作为口令，并定期变更口令，提出应像防止计算机病毒的扩散一样，防止黑客对网上数据的窃取、替换及破坏。

在信息安全研究方面，美国国防部基于军事计算机系统的保密需要，在 70 年代的基础理论研究成果计算机保密模型的基础上，制订了“可信计算机系统安全评价准则”（TCSEC），其后又制订了关于网络系统、数据库等方面的系列安全解释，形成了安全信息系统体系结构的最早原则。至今美国已研究出达到 TCSEC 要求安全系统（包括安全操作系统、安全数据库、安全网络部件）的产品 126 种。90 年代初，英、法、德、荷四国针对 TCSEC 准则只考虑保密性的局限，联合提出了包括保密性、完整性、可用性概念的“信息技术安全评价准则”（ITSEC）。但是，该准则中并没有给出综合解决以上问题的理论模型和方案。近年来，六国七方（美国国家安全局和国家技术标准研究所、加、英、法、德、荷）共同提出了“信息技术安全评价通用准则”（CC for ITSEC）。CC 综合了国际上已有的评价准则和技术标准的精华，给出了框架和原则要求。然而，将作为取代 TCSEC 用于系统安全的评测的国际标准，它仍然缺少综合解决信息的多种安全属性的理论模型依据。

安全协议作为信息安全的重要内容，其形式化方法分析始于 80 年代初，目前有基于状态机、模态逻辑和代数工具的三种分析方法，但仍有局限性和漏洞，处于发展提高阶段。

由于在广泛应用的国际互连网上，黑客入侵事件不断发生，不良信息大量传播，网络安全监控管理理论和机制的研究受到重视，黑客入侵手段的研究分析，系统脆弱性检测技术，报警技术，信息内容分级标识机制，智能化信息内容分析等的研究成

果，已经成为众多安全工具软件的基础。

研究中揭示出存在许多设计缺陷，存在情报机构有意埋伏的安全陷阱的现实可能。例如，在 CPU 芯片中，在发达国家现有技术条件下，可以植入无线发射接收功能，在操作系统、数据库管理系统或应用程度中，能够预先安置从事情报收集、受控激发破坏的程序。通过这些功能，可以接收特殊病毒；接收来自网络或空间的指令来触发 CUP 的自杀功能，搜集和发送敏感信息；通过特殊指令在加密操作中将部分明文隐藏在网络协议层中传输等。而且，通过唯一识别 CPU 个体的序列号，可以主动、准确地识别、跟踪或攻击一个使用该芯片的计算机系统，根据预先设定收集敏感信息或进行定向破坏。

作为信息安全的关键技术的密码学，近年来空前活跃。美、欧、亚各洲举行的密码学和信息安全学术会议频繁。 1976 年美国学者提出的公开密钥密码体制，克服了网络信息系统密钥管理的困难，同时解决了数字签名问题，并可用于身份认证，它是当前研究的热点。电子商务的安全性是当前人们普遍关注的焦点，目前正处于研究和发展阶段，它带动了认证理论、密钥管理等的研究。1977 年美国颁布使用的国家数据加密标准 DES，由于密码分析和攻击手段的进步，已不能满足安全需要，美国正在征集作为 21 世纪的新的数据加密标准。计算机运算速度的不断提高，各种密码算法面临着新的挑战。新的密码体制如量子密码、DNA 密码、混沌理论正处于探索中。基于密码理论的综合研究成果和可信计算机系统的研究成果，构建公开密钥基础设施，密钥管理基础设施成为当前的另一个热点。

我国信息安全面临严峻形势

改革开放 20 年来，我国信息产业有了飞速的发展，取得了巨大的成就。至 1998 年，我国电话机总数达 1.35 亿部，占世界第二位；微型计算机产量 299 万台，占世界总量 3%多。软件产业年销售额为 138 亿元，其中国产软件约占 1/3。电视人口覆盖率为 87.7%，电视机年产量 4275.9 万台，为世界第一位。集成电路年产量 16.3（27.1） 亿块。1998 年信息产业占 GDP 约为 3%左右。截止到 1999 年 12 月底，因特网上网用户达到 890 万。总的来说，取得了巨大的成就。

但是，随着全球信息化的飞速发展，我国大量建设的各种信息化系统已经成为国家关键基础设施，其中许多业务要与国际接轨，诸如电信、电子商务、金融网络等。网络信息安全已成为亟待解决、影响国家全局和长远利益的重大关键问题。它不但是发展信息革命带来的高效率、高效益的有力保证，而且是对抗霸权主义、抵御信息侵略的重要保障。网络信息安全问题如果解决不好，将全方位地危及我国政治、军事、经济、文化等各方面的安全，使国家处于信息战和经济金融风险的威胁之中。

目前我国信息安全面临严峻形势：在信息产业和经济金融领域，电脑硬件面临遏制和封锁的威胁；电脑软件面临市场垄断和价格歧视的威胁；国外电脑硬件、软件中隐藏着“特洛伊木马”；信息与网络安全的防护能力很弱，许多应用系统处于不设防状态，具有极大的风险性和危险性。在意识形态领域，电子媒介成为国际意识形态斗争的主导工具；新闻媒体是西方宣扬其主流意识形态的利器；当今国际信息传播的主流仍然被西方所控制，信息、新闻领域里“西强我弱”的局面短时期还难以改变；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。在军事领域，网络泄密是军事信息安全问题的重要表现；黑客攻击对军事信息安全危害极大；信息战是影响军事信息安全的极端表现形式。

我国信息安全研究经历了通信保密、计算机数据保护两个发展阶段，正在进入网络信息安全的研究阶段。安全体系的构作和评估，通过学习、吸收、消化 ITSEC的原则，进行了安全操作系统、多级安全数据库的研制，但由于系统安全内核受控于人，以及国外产品的不断更新升级，基于具体产品的增强安全功能的成果，难以保证没有漏洞，亦难以得到推广应用。在学习借鉴国外技术的基础上，国内一些部门也开发研制了一些防火墙、安全路由器、安全网关、黑客入侵检测、系统脆弱性扫描软件等，但是，这些产品安全技术的完善性、规范性、实用性还存在许多不足，特别是在多平台的兼容性、多协议的适应性、多接口的满足性方面存在很大距离，理论基础和自主技术手段也需要发展和强化。

当前，我国信息安全的形势是严峻的，主要表现在：

1.信息与网络安全的防护能力很弱，许多应用系统处于不设防状态，具有极大的风险性和危险性。

我国国民经济信息化提上政府议事日程，随着 1999 年“政府上网工程”的全面启动，我国各级政府将陆续设立自己的网站，电子商务也正以前所未有的速度迅速发展，由于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。金融领域中这一现象更为突出。在我国，高技术犯罪的案件已呈直线上升，金融银行业计算机犯罪屡有发生，个案金额已从数十万上升到上百万。

对我国金融系统计算机网络现状，专家们有一些 形象的比喻：使用不加锁的储柜存放资金（网络缺乏安全防护）；使用

“公共汽车”运送钞票（网络缺乏安全保障）；使用“邮寄托寄”的方式传送资金（转帐支付缺乏安全渠道）；使用“商店柜台”方式存取资金（授权缺乏安全措施）；使用“平信”邮寄机密信息（敏感信息缺乏保密措施）。在银行计算机犯罪案件中，最具破坏性的犯罪类型是篡改数据，而各银行对计算机数据的保护、操作密码保护和储户密码保护都缺乏有力的措施。以证券系统为例，这个系统采用的 Novell 服务器是在 DOS 平台上的。DOS 系统是个开放的系统，稍懂计算机的人就可以在系统上做手脚。证券系统的电脑人员或大户们一屋一机关起门来，轻而易举就可以把别人的钱拿过来炒一把，这种案例不是没有。证券系统的安全直接牵涉股民的利益，如果不及时防范，一旦出现问题，后果严重。证券系统每天的交易量达几百亿元，而这几百亿元交易的基础却是建立在缺少安全性的系统上的，实在令人担忧。

2.对引进的信息技术和设备缺乏保护信息安全所必不可少的有效管理和技术改造。

在信息化过程中，对发达国家或跨国公司在提供的关键装备中可能预做的手脚无从检测和排除，可能造成既花费大量资金又买来经济运行中的隐患、买来国家不安全的后果。

由于国外电脑硬件、软件中可能隐藏着“特洛伊木马”，一旦发生重大情况，那些隐藏在电脑芯片和操作软件中的“特洛伊木马”就有可能在某种秘密赘令下激活，或使民用电脑全部无法启动，或使我国政府、军事电脑网络、电信系统瘫痪，侦成灾难性的经济、社会和军事后果。

我国积极推进经济建设，银行系统、政府部门全都处在信息化和网络化进程中，却很少人有关注安全，我们就等于敞开门让人攻击。现在没有人攻击我们，不等于将来永远太平。美国袭击我驻南使馆事件告诫我们绝不能掉以轻心。未来的战争绝不会是单纯使用武力攻击军事目标，很可能利用信息武器直接攻击国民

经济。一颗用打印机携带的信息定时炸弹，仅仅用病毒就摧毁了伊拉克的防空系统，使伊拉克的飞机飞不上天，任凭美军狂轰滥炸。谁能保证我们的系统不会受到攻击？现在，美国大量推销信息化产品到中国，包括软件、硬件、网络和操作系统。这些东西是我们需要的，但是我们也不能不警惕这些商业行为背后可能隐藏的美国的全球性战略。现在他们不打草惊蛇，将来搞出些名堂就很容易。他们根本不用派人弄情报，你用电脑在工作，他可用电脑在窃取。因此，我们在推进信息化建设的同时，绝不能不警惕它将对国家信息安全构成的严重威胁。

3. 基础信息产业薄弱，严重依赖国外。

我国的信息化建设，基本上是依赖购买国外技术设备进行的。在国际财团涌向我国信息化建设的市场，大举推销电子信息设备，而我们又相对缺乏知识和经验的情况下，信息化建设进程中存在花钱买淘汰技术和不成熟技术的现象，潜在着国外势力埋伏信息安全隐患的极大危险。

我们的电脑软件面临遏制和封锁的威胁。虽然我国的电脑制造业有很大的进步，但其中许多核心部件都是原始设备制造商的，我们对其的研发、生产能力很弱，关键部位完全处于受制于人的地位。我们的电脑软件面临市场垄断和价格歧视的威胁。美国微软已垄断了我国电脑软件的基础和核心市场。离开了微软的操作系统，国产的一切软件都失去了操作平台。

在我国信息化建设的工程中，外国公司成为最大的获利者。在我们决心运用市场招标的机制来解决工程设备时，他们不但利用拥有先进设备，有建设多个工程的经验的优势地位，和我国实力不强的电子信息系统产业争夺市场。而且，用高薪雇用我国在行政管理机关和科研技术单位工作的有经验人员，充当他们的打开市场之门的先锋。他们用送高级礼品、出国考察为诱饵等手段，在激烈的竞争中抢占有利地位。虽然目前没有具体的统计数

据，但是，我国的计算机、通信、广播电视等与信息化相关的市场，已被国外公司垄断的事实不证自明。最危险的是，他们已经把发财的欲望投入到有关信息安全的领域，这是关系国家安全、民族存亡的极为重要的领域，我们必须加以警惕。

4.国家信息安全管理机构缺乏权威，协调不够。

国家经济信息安全管理条块分割、各行其是、相互隔离，极大地妨碍了国家有关法规的贯彻执行，难以防范境外情报机构和“黑客”的攻击。国家在信息安全问题上缺乏一个具有最高权威的统一机构。信息安全相关的管理机构与国家信息化领导机构之间还没有充分沟通协调。缺乏一个国家级的与国家信息化进程相一致的信息安全工程规划。

5.信息犯罪在我国有快速发展蔓延的趋势。

外国情报机关的情报手段现代化的程度越来越高。他们可以在传真机、电话交换机中运用远程诊断、远程修复功能进行信息窃取。他们拥有技术手段从泄露的电磁信号中提取信息。我国极高层次、极小范围的核心机密有被窃的危险。金融银行业计算机犯罪屡有发生。我国从1986年发现第一件银行计算机犯罪案起，案件呈直线增长。调查表明每年计算机犯罪发案率递增30%。1996年重要案件估计有100件之多。证券市场上通过计算机炒买他人股票的事件也已发生多起。在因特网上存在一批制黄贩黄的黄徒，他们利用因特网全球可达的特点，从事国际化的黄毒散布。直至今日，在我国与国际互连网连接的计算机上，不堪入目的黄色图片还能被调阅下载，甚至还可下载黄色影片和电视。因特网上还频频发生用电子手段散发反对我国的言论。

6.全社会的信息安全意识急需提高。

信息安全意识淡薄，是当前存在的一个十分严重的问题。一部分人有盲目乐观情绪。他们认为我国信息化程度不高，更没有广泛连网，上因特网的只是极少数人。报刊报道的发达国家的信

息安全事件，在我国不可能。要发生也是多少年以后的事，不必大惊小怪，处在“居危思安”的心态中。一部分人满足于拿来主义。他们认为，现在因特网上就有许多加密软件可以卸载。随便拿一个来用，就比我们现在的水平提高了不知多少。而且，有些人在使用密码中还存在误区，认为有变换就是密码，有算法就能安全，缺乏密钥管理意识。还有一部分人对国外公司的宣传盲目信任。在国外公司的推销攻势中，盲目听信商业性的广告宣传。盲从地相信他们吹嘘的什么全面解决方案，他们推销的密码多好。不知道外国政府对我国出口信息安全技术设备和密码算法的强度有着严格的限制，我们能够得到的只是人家可以监控的功能弱化了的产品。凡此种种，都说明人们的信息安全意识急需提高。

另外，信息安全领域在研究开发、产业发展、人才培养、队伍建设等方面和迅速发展的形势极不适应，在国家级研究开发计划中，至今没将信息安全单列，只是做为信息化的研究分支立项，投入很少，和国外差距越来越远。

以上问题如果不能切实解决，我国的信息安全将面临严重威胁，在激烈的信息争夺和信息战中我国就会处于被动挨打的软弱地位。因此，充分重视我国的信息安全问题已迫在眉睫。

我国信息安全战略对策的几点建议

信息安全是一个国家的综合集成系统，它的规划、管理要求国家进行科学的、强有力的干预和导向。为加强我国信息安全建设，保障我国经济的安全运行和国家的根本利益，特提出以下对策建议：

1.确立信息安全的战略目标和任务。

要确立我国信息安全的国家战略目标：保证国民经济基础设施的信息安全，抵御有关国家、地区、集团可能对我实施“信息战”的威胁和打击以及国内外的高技术犯罪，保障国家安全、社会稳定和经济发展。

信息安全战略防御的重点是国民经济中的国家关键基础设施，包括金融、银行、税收、能源生产储备、粮油生产储备、水电汽供应、交通运输、邮电通信、广播电视、商业贸易等国家关键基础设施。重中之重是支持这些设施运作的电子信息系统。我们认为党、政、军和银行清算、支付、交换信息系统，金融证券信息系统，税务信息系统，海关信息系统等信息系统已经构成了我国的关键信息基础设施。他们的信息安全应该是我们工作的重点。党政军的信息系统有传统的机要机关服务把关，但是金融银行的信息系统还缺乏信息安全的系统管理，是信息安全的薄弱环节。这些部门是我国的经济命脉，并且信息化的发展速度最快，使用的国外设备多而杂，他们有些业务需要与国外接轨，外商在信息安全方面介入深，这些部门信息安全的专业队伍还没有真正形成。以上情况造成了这些关键信息基础设施存在较大的安全风险。

2. 加强国家信息安全机构及职能。

为了强化国家的统一领导，建议成立具有高度权威的国家信息安全委员会，研究确定国家信息安全的重大决策，发布国家信息安全政策，批准国家信息安全规划，对国家面临的重大信息安全紧急事件作出决断。在国家信息安全委员会领导下设立国家信息安全技术委员会，任务是提出国家信息安全规划，审批重大信息化工程的信息安全技术路线和措施，组织制定信息安全需要的密码算法、接口、协议和信息安全系统的规范、标准，并对实施进行监督。同时，针对信息安全中的犯罪活动，建议在国家执法部门建立高技术刑事侦察队伍，汇总高技术犯罪案例，研究分析