信息安全技术发展研究

Information

陈 宇 著

Xinxi Anquan Jishu
Fazhan Yanjiu

电子科技大学出版社

信息安全技术发展研究

Xinxi Anquan Jishu
Fazhan Yanjiu

陈宇 著

电子科技大学出版社

图书在版编目（CIP）数据

信息安全技术发展研究 / 陈宇著. — 成都：电子科技大学出版社，2017.6
ISBN 978-7-5647-4468-7

Ⅰ. ①信… Ⅱ. ①陈… Ⅲ. ①信息安全－安全技术 Ⅳ. ① TP309

中国版本图书馆 CIP 数据核字（2017）第 116749 号

信息安全技术发展研究

陈 宇 著

出　　版：电子科技大学出版社（成都市一环路东一段 159 号电子信息产业大厦 邮编：610051）
策划编辑：罗　雅
责任编辑：罗　雅
主　　页：www.uestcp.com.cn
电子邮箱：uestcp@uestcp.com.cn
发　　行：新华书店经销
印　　刷：成都市火炬印务有限公司
成品尺寸：185mm×260mm　　印张 8.75　　字数 240 千字
版　　次：2017 年 6 月第一版
印　　次：2017 年 6 月第一次印刷
书　　号：ISBN 978-7-5647-4468-7
定　　价：35.00 元

前　言

随着计算机技术和通信技术的发展，网络将日益成为重要的信息交换手段，渗透到社会生活的各个领域。因此，认清网络的脆弱性和潜在威胁以及现实客观存在的各种安全问题，并采取强有力的安全策略，保障网络信息的安全，是每一个国家和社会团体以及个人必须正视的事情。

本文以信息安全发展现状为切入点，围绕信息安全面临的威胁、攻击手段、防护理念、安全措施、相关前沿技术研究等方面进行了深入浅出的阐述，既有理论研究，又有实际应用，力图为读者描绘一个比较完整的信息安全攻防体系。

本文针对网络应用相关的基本信息安全问题和解决方案进行了调查研究。从信息安全的基本概念和存在的安全问题入手，简单分析了加密技术、网络安全技术、防火墙技术、网络入侵检测技术、应用系统安全防护等内容。

由于编者水平与能力有限，不能将所有技术进行深入的总结和研究，文中也难免有遗漏或不足之处，感谢为本文提供素材及相关技术资料支持的各专家、学者，如未尽引用还请作者给予谅解。最后，欢迎各位专家、学者与广大读者批评指正。

编　者

目　录

第1章　信息安全发展现状研究

1.1　我国信息安全的现状分析

1.1.1　网络信息安全存在的问题

人类进入21世纪，网络信息安全成为摆在社会发展中的突出问题。21世纪的信息流动，主要是以网络为载体，以电子化的信息流为媒介，以大型计算机为终端的信息获取、交换与分享。网络深刻影响了人类的政治、经济、文化等方方面面。但是，随着互联网的全面渗透和融入每个人的生活、学习、工作和社交活动中，网络安全问题显得非常凸出。没有一个安全的网络环境，个人隐私及商务活动等的安全就无从谈起。随着网络信息已经成为信息传递的主要手段，网络信息技术的发展日新月异，进展迅速，与此同时，对网络信息安全的治理却时常为人们所忽视，造成了网络信息安全漏洞频出，对国家安全造成不利的影响。因此，对网络信息安全的治理，已经成为世界各国不得不加大力强化的重要方面。

我国网络信息安全虽然起步较晚，但是，随着互联网信息的进步以及对网络信息安全重视程度的提升，网络信息安全已经上升为国家战略，并且受到越来越多的重视和关注，与此相关的法律法规不断完善，网络信息安全方面的人才培养也备受关注，网络监管的手段，网络传播内容的控制，网络舆论的监测逐渐成为网络信息安全所采用的常规手段。从世界范围来看，各国都在不遗余力地加强网络信息安全的治理，强化对网络信息的监管和控制，以期维护国家安全和政治经济的稳定。例如欧盟就准备于2017年建立一个新的统筹各国网络信息安全的IT部门，对网络信息加强监管；美国在网络信息安全方面将通过推出网络身份证，构建一个网络生态系统；日本、澳大利亚也加强了网络信息安全的法律监管，加大对破坏网络信息安全的行为的处罚力度。以上都说明网络信息安全已经成为影响一国国家安全，受到世界各国所关注和重视的重要问题。

1.1.2　网络安全的发展和现状

1. 信息技术的发展为信息安全管理增加了新的内容

我国信息技术发展十分迅速。早在2012年，著名咨询机构波士顿(BCG)发布报告指出，中国的互联网经济已经达到了GDP的5.5%，并且仍在加快发展。到2016年，这一数字已达到8520亿美元，互联网经济占GDP的比重将上升到6.9%，保持全球第三的位置。

《2016 年中国互联网产业综述与 2017 年发展趋势》中指出，截至 2016 年 6 月，中国网民规模为 7.1 亿，互联网普及率达到 51.7%，网民数量继续稳居全球首位。移动电话 4G 用户达到 7.14 亿，比去年同期增长 3.86 亿，增幅达到 118%，占移动电话用户的比重达到 54.1%，仍旧保持高速增长。网民数量的平稳增长与移动互联网用户的快速增加，为各类互联网应用的创新成果惠及百姓民生提供了有力支撑。2017 年 1 月 22 日，中国互联网络信息中心（CNNIC）在京发布第 39 次《中国互联网络发展状况统计报告》，报告指出，截至 2016 年 12 月，中国网民规模已达 7.31 亿，手机网民达 6.95 亿，全年共计新增网民 4299 万人。互联网普及率为 53.2%，较 2015 年年底提升 2.9 个百分点。中国网民规模已经相当于欧洲人口总量。中国网民规模和互联网普及率如图 1－1 所示。

图 1－1　中国网民规模和互联网普及率

中国网络信息的发展非常迅速。很多学者提出，中国后发型现代化进程，很大程度上也是得益于信息化的发展。在国际电信联盟发布的全球信息化发展指数研究报告中，中国的信息化位列全球信息化发展最为迅速的 10 个国家之一。2016 年中国电子信息产业发展研究院发布了《2015 年中国信息化发展水平评估报告》。报告中指出，2015 年全国信息化发展指数为 72.45，比 2014 年增长了 7.69。其中，网络就绪度指数为 73.31，增长了 12.25；信息通信技术应用指数为 70.86，增长了 6.1；应用效益指数为 73.93，增长了 1.78。

中国的信息化发展也具备了自身独特的特点，即信息化是与中国制造业和服务业发展紧密相连和相互促动的。中国的产业升级和转型，产业模式的创新，都离不开信息化的推动，而信息化也在中国工业化的发展中得到提升和完善。

网络信息安全技术的发展，主要体现在认证、加密、防火墙以及监测系统几个方面。

（1）认证。

认证是信息安全的第一道防线。认证是指对进入信息网路的用户进行身份的辨明和认证，通过认证后才能够进行网络信息的进一步操作。通过认证能够对信息安全起到初步的防护作用，保证进入信息网络用户的合法性和正当性。认证的方式主要包括身份认证、访问授权、数字签名等。

(2)数据加密。

数据加密是较常用的信息安全手段,通过对网络信息数据进行加密,使得信息难以被破解。常用的数据加密手段有私钥加密和公钥加密等。

(3)防火墙技术。

防火墙技术是比较常用的网络信息安全防护手段,防火墙是一种软件的防护方式,通过设立防火墙对信息的传递提到过滤和防护的作用,特别是在关键和重要的节点,防火墙可以对网络通信数据进行拦截,防止意外的侵入和信息的不法交换。从其防护方式上来看,防火墙主要是一种被动防御系统,通过设立防护屏障起到保护关键信息的作用。

(4)监测系统。

监测系统是随着信息技术的发展而产生和发展的,在信息技术的发展初期,很多信息交流由于没有设立相关的监管系统,信息技术的交换具有很强的随意性和任意性,这对于网络信息的监管和控制都十分不利。因此产生了网络信息的监测系统,通过动态的监测信息流动的状况对信息的流入、交换和流出加以监控,保护信息交换的合法性。

2. 网络信息安全的基础和手段有待提高

虽然网络信息安全的治理已经提升为国家战略的层面,并随着网络信息技术的发展而不断更新,但是目前网络信息安全的技术基础和手段仍有待提高。主要表现在以下两方面。

第一,网络信息安全行业技术比较落后。目前我国信息安全产品核心技术严重依靠国外,缺乏自主创新产品。我国信息网络使用的网管设备和软件基本来自进口,大大减弱了我国网络的安全性能。

第二,网络信息安全监管手段需要完善。目前网络信息监管还是以政府集中管制为主,在发挥个体监控和组织监控方面力度不足。完善的信息安全监管机制,应当发挥个人、组织和国家三者的合力,形成监管的层次体系,从而更好地实现网络信息安全。

3. 网络信息安全事故的不断增多

随着我国网络规模的不断发展,网络信息安全事故也逐渐增多,从事故对象上看,企业和个人都容易受到网络信息安全的威胁。中国电信股份有限公司北京研究院与北京神州绿盟信息安全科技股份有限公司(简称绿盟科技)等单位共同发布了调研产出的《2016 年上半年中国网站安全报告》指出:相比 2015 年上半年,2016 年上半年高危漏洞占比有所增加。2015 年上半年监测发现每个网站平均漏洞数达 658 个,其中,高危漏洞数为 7 个。2016 年上半年监测的网站数据显示,平均每个网站漏洞数达 773 个,其中,高危漏洞数高达 22 个。《2016 年上半年数据泄漏水平指数调查报告》显示,在全球范围内,2016 年上半年已曝光的数据泄漏事件高达 974 起,数据泄漏记录总数超过了 5.54 亿条,而 2015 年下半年数据泄漏事件和数据泄漏记录总数分别为 844 起和 4.24 亿条。数据泄漏成本越来越低,而数据泄漏本身已经快成为互联网安全问题发生的常态。以大型电子商务、金融机构、第三方在线支付网站为主要对象的“网络钓鱼”上升明显。网络“木马”和“僵尸”病毒成为中国网络安全的直接威胁,据中国互联网络信息中心(China Internet Network Information Center, CNNIC)2014

年全球中文钓鱼网站趋势分析报告统计指出,2014 全年共发现中文钓鱼网站 55 063 个,同比 2013 年有所下降,但仍居于高位。全球中文钓鱼网站共涵盖 143 个顶级域,同比 2013 年增长 13 个。因此,随着互联网迅猛发展以及其在各行各业的深入渗透,安全形势与挑战日趋严峻,网络钓鱼已成为威胁网络安全的突出问题,且呈现着严重化趋势。2016 年 8 月最新的钓鱼网站侦测报告中指出,据相关统计显示,共侦测到新增钓鱼网站 34 190 例,涉及 1416 家机构。截至 2016 年 8 月,累计侦测到钓鱼网站 208 444 例。钓鱼网站仿冒对象前五名分别是:京东、建设银行、苹果、工商银行、中国移动。

1.2 国家信息安全发展战略代价研究

随着以信息技术为核心的信息社会的到来,信息安全已经扩展到了国家的政治、经济、社会等各个领域。信息安全的外延不断扩大,包含的内容从最初的信息加密和保证信息的完整性,发展到现在的信息可用性、可控性和不可抵赖性。信息安全技术也在不断发展,从简单的加密技术,到复杂安全协议、安全模型来保证信息系统的安全。为了适应新的安全需要还会开发出更多的安全技术。随着信息技术的广泛应用,人们还会对信息安全提出更多的要求。

自从 20 世纪 90 年代以来,信息安全开始进入信息保障阶段。信息安全的概念发生了以下变化。

(1)信息的安全不再局限于信息的保护。人们需要对整个信息和信息系统的保护和防御,包括保护、检测、反应和恢复能力。

(2)信息安全与应用更加紧密。其相对性、动态性、系统性等特征引起人们的注意,追求适度风险的信息安全成为共识。

信息安全不再是单纯以功能或者机制技术的强度作为评价指标,而是结合了不同主体的应用环境和应用目标的需要,进行合理的计划、组织和实施。信息保障除强调信息安全的保障能力外,还提出了要重视系统的入侵检测能力、系统的事件反应能力,以及系统在遭到入侵破坏后的快速恢复能力。① 传统的加密、计算机安全和信息安全体系都是一种静态的被动的防御体系。从信息保障阶段开始,人们已经注重信息系统的动态主动防御能力。并强调信息系统主体(人)的能动性,将信息系统的拥有者、管理者和使用者视为安全保障体系的核心。

以上可以发现,信息安全是不断发展变化的,同时也是一个信息对抗的过程,是基于高技术、非对称、超常规的一种对抗过程。因此,没有信息技术的不断深化研究,没有对信息技术手段的掌握和运用,没有先进的管理机制对信息高技术人才的支撑是不行的。其关键问题在于,不能将信息安全仅仅局限于信息技术系统内,解决信息安全的手段也不能仅仅局限

① 李明,吴忠. 信息安全发展研究与综述[J]. 上海工程技术大学学报,2005,19(3):258 - 262.

于技术的发展和技术管理的层面，而忽略了国家整体的战略与人、组织间的动态演化关系。如果能在未来的信息安全对抗中争取主动，就要有长远规划的战略和科学的应变策略及不断发展的技术与人才保证，并且准备承担为之奋斗而付出的代价，包括建立和发展相关的自主安全技术和产业需要付出必然性代价、国家信息安全发展与现实经济发展需求之间的冲突而导致的选择性代价。

1.2.1　主要国家信息安全战略发展的比较

随着信息社会的发展，国家间的竞争越来越集中在信息优势方面的争夺上，而信息优势的制高点是国家信息安全战略的制定与实施。国家信息安全战略的制定与实施是一个典型的复杂系统工程。作为复杂的系统工程，信息安全主体和环境形成了协同演化的关系。

我国的信息安全专家曲成义认为：国家信息安全战略是维护国家信息安全全局及长远发展目标和保障国家信息化建设健康发展的纲领性文件，是国家信息安全发展的指导思想、战略目标、推进策略、运作机制和实施路线，目的是统一思想、意志，动员、指导和促进信息安全的全面建设和全面发展。国家信息安全的战略规划就是从帮助国家实施已有的信息化战略和竞争战略或形成新的国家发展战略和竞争战略的角度出发，寻找国家信息安全的关键攻防领域，确定合理的发展模式，以实现国家的信息化战略目标的过程。

国家信息安全的战略规划方法提供一套基本的方法和分析框架来系统地理解和准确地把握国家信息安全对国家信息化发展战略和竞争战略的影响，为国家战略规划部门识别出我国信息安全的发展机会，确定国家的信息化发展的关键应用领域和信息安全保障的合理应用模式，为国家更成功地实现当前的信息安全战略目标提供方法。

国家信息安全的战略目标则是要通过国家意志和国家行为，在进一步完善法律法规的基础上，采取风险评估、等级保护、应急机制、协调机制等多种管理手段，整合配置安全产品、专业服务、技术支撑、信息安全基础设施、信息安全应用设施等各类技术资源，从而建立一个由管理体系和技术体系所构成的国家信息安全保障体系，以应对信息网络环境下国家和社会所面临的安全风险与威胁，进而保障国家信息安全和促进国家信息化的可持续发展。

西欧和美国的信息安全战略是按政府和军方两条线路进行的，政府侧重于国家信息基础的安全保障，军方则更侧重于信息战的防御与进攻。美国的信息安全战略重点是信息基础设施的安全，并以此展开信息安全的研究和部署，特别是信息安全基础设施建设方面，启动了 7 个关于保护美国关键基础设施的计划，即信息共享计划、确定伙伴关系计划、组建工作机构计划、信息安全教育战略计划、保障政府信息安全计划、完善法律法规战略计划以及研究和开发计划。在军方信息安全方面，美国国防部将信息安全对策提高到战略的高度，加强信息攻防能力。目前，美国已经形成较为完整的信息战体系。自 1996 年起，美国军方先后颁布了《信息战野战条令》《信息对抗作战条令》《联合信息战政策》《信息对抗联合条令》等一系列军事条令，这也标志着美国军方的信息对抗能力已经达到了可靠而实用的程度，已经成为与常规军事力量并重的作战方式。美国的信息安全战略，最初是以保护本国的信息

安全为重点，而在“9·11”事件以后，美国信息安全战略已经迅速发展成为以“先发制人”和“向全球扩张”为主要特点的“扩张型”信息安全战略。

1997年，俄罗斯同样开始研究和制定《国家信息安全学说》，并于2000年6月正式颁布实施。该学说首次明确了俄罗斯在信息领域的利益，面临的内在和外在威胁以及确保信息安全应采取的措施。《国家信息安全学说》分为4个主要部分，分别是：保证信息安全是国家利益的要求、保证信息安全的方法、国家在保证信息安全的基本原则、信息安全的组织基础。该学说突出了以“信息战”为重点，强调为确保俄罗斯的生存和发展问题，必须为未来的国家信息安全做好准备。

2000年7月，日本的信息技术战略本部及信息安全会议共同拟定出国家信息安全指导（战略）方针，要求各政府机构制定出适合本单位特点的《信息安全基本方针》和《信息安全对策基准》，明确政策制定和实施的相关人员的责任与义务，强化人员管理，制定严密的安全缺陷对策。

目前，我国国家信息安全整体安全防范技术水平低下，基础信息产业薄弱，严重依赖国外，技术创新不够，安全技术、安全产品低水平重复，缺乏足够的资金投入支持信息安全基础研究和关键技术研究；缺乏市场需求，国家信息安全管理机构缺乏权威，协调不够，信息安全基础设施建设不够，信息安全意识缺乏。

2006年5月8日，我国发布的《2006—2020年国家信息化发展战略》提出了信息化是当今全世界发展的大趋势，是推动经济社会变革的重要力量，是我国现代化建设全局的战略举措，是我国正确贯彻和落实科学发展观、全面建设小康社会、构建和谐社会、建设创新型国家的迫切需要和必然选择。但是，同样指出，要建立国家信息安全的保障体系，还需要在整体、全局和战略上对国家信息安全进行规划和把握。①

1.2.2 信息安全战略发展代价

1. 信息安全发展代价

人类在21世纪以后进入信息化社会，整个社会的生产、生活方式都发生了根本的变革。信息社会的根本特点是信息技术在社会中发挥了重要的主导作用。其中，信息资源的开发和利用对信息技术、设备的依赖性与日俱增。既然未来国家的经济要依赖信息资源以及信息技术的开发、利用，那么，未来国家安全同样需要依赖国家信息安全技术的开发和利用。由于信息安全技术本身也是一类信息技术，它是集计算机技术、通信技术、传感技术、自控技术、材料技术、生物技术等综合于一身的总体综合技术，它是以数学、物理和生物为基础学科的高级信息技术，同时，它也是遵循着摩尔定律的快速发展中的技术。信息安全技术发挥这信息系统的重要支撑和保障作用，它是信息技术的制高点，也是关系到未来国家生死存亡的关键之一。因此，人们将信息安全研究的重点集中在技术防御方面以及入侵检测系统方面，

① 唐晓波，胡深. 国家信息安全保障战略研究[J]. 科技进步与对策，2004，6. 140－142.

而从经济学的角度来研究信息安全较少，尽管 Lawrence A. Gordon 和 Martin P. Loeb 曾经指导人们对信息安全发展的投资比例不能超过预期损失的37%，但是，他们并没有从国家发展信息资产以及公共基础设施建设的角度上来对灾难性的损失和代价问题加以研究。

目前，各个国家的主权不仅仅只在国土资源上，早已延伸到信息网络空间。“信息主权”同样给各个国家主权赋以新的内容。由于信息技术的发展存在不平衡的现象，各信息强国与信息弱国之间的“数字鸿沟”也正在不断的扩大。处于弱势的国家，其在政治、经济、军事、文化乃至网络信息安全等各个方面都面临着前所未有的冲击、挑战和威胁。信息技术已经成为信息强权在新世纪谋求霸权的另一种利器。一个国家的信息管理能力以及相应的“信息制控权”（或者说是“制信息权”），早已成为该国在生存与发展竞争中能否占据角色主动的关键之一。

随着信息网络及应用的不断扩大，中国信息化进程早已从全面推进基础设施建设阶段，向大力加强信息资源开发以及利用的新阶段迈进。信息安全问题所带来的影响和后果也随之增大。信息安全在维护国家安全中的地位日渐显现，已经成为各国家安全的重要组成部分。

中共十六届四中全会《中共中央关于加强执政能力的决定》中明确指出，坚决维护国家安全，确保国家的政治安全、经济安全、文化安全、信息安全和国防安全。信息安全与政治安全、经济安全、文化安全和国防安全相并列为“五大安全”，使之成为国家安全的重要组成部分。从我国和全球各国的信息化发展情况来看，信息安全确实早已成为各国家安全的重要“基石”和“命脉”。以信息技术为核心的新军事革命也在逐步地改变着现代与未来战争的形态，信息网络及信息系统也已经成为一种新型的攻击武器、作战平台和打击目标，网络空间已经成为攸关各个国家安全的重要战场。信息流动与传播的高速性、广泛性以、依赖性，以及信息武器攻击手段、目标、过程的多样化、远程化以及自动化，早已使世界各国都面临着现实与潜在的安全威胁。

如果希望信息安全技术不断快速的发展，以确保国家安全不受制于人，那么，国家必须具备战略性的创新机制，需要时刻创造出领先的信息安全技术，并且通过确立市场驱动机制，如市场全球化，投资多元化，并且在市场经济条件下，使信息安全技术商品化，信息单位企业化。随着市场机制和竞争机制的引入，信息安全产业在快速的发展并日趋完善。另外，由于信息安全产业与其他非信息市场相结合，共同调节了信息资源的供求关系，使政府的信息安全整体竞争水平也得到了逐步提高，这些都为国家安全奠定了坚实的基础。我国目前信息技术创新机制不够完备、快速反应决策机制效率较低、信息共享和合作机制不够灵敏、市场参与机制也有待进一步加以完善、知识产权机制以及法律机制仍存在不健全的方面。而对于国家政府而言，面对各种安全威胁，最重要的战略选择首先应该是建立一套比较完善的国家安全战略规划，发挥全民智慧，并且集中一切优势资源，并在此基础上，我国政府应该完成一项紧迫的任务，要不断地增强政府与整个社会的信息安全防控能力，探索国家信息安全控制方面的基本规律，完善信息安全方面的管理制度。因此，顺应信息社会的发展趋势，

构建一套科学、合理、有效的国家信息安全管理机制，提高国家、政府、企业以及全体公民信息安全应对能力，是我国当前社会信息安全战略管理的现实任务。

2. 信息安全发展代价的特点和机理

(1)从信息化的角度分，信息安全发展代价可以分为必然性代价、人为性代价。其中，必然性代价是指对于信息安全人们应该追求均衡的安全发展目标。由于历史和客观条件受限，在一定的发展阶段，人们只能先去关注一部分主导性发展目标，并且把主要条件、资源和力量等各种要素投入这一目标的发展上来。但是，这样做的结果往往以对其他目标的排斥、抑制、舍弃来作为代价，求得发展。例如，因全力发展网络安全技术，将限制信息资源的开发、共享和利用。人为性代价是指由人的主观局限、失误或故意而造成的损失。人为性代价与发展本身并不存在内在的必然联系，而是由人在主观性判断错误而造成的损失。例如，缺乏信息管理制度、系统技术漏洞、人为疏忽导致的操作失误以及外部网络攻击而造成的损失等。

(2)从国家安全的角度可分为主权代价、社会代价、经济代价、技术代价以及生态代价。其中，主权代价是指信息安全对政治主权的冲击，传统的政治主权是以物理空间作为管辖基础的，由于网络空间是虚拟的，因此，可以对物理空间产生一定影响，但不能一一对应，国家也难以行使管辖权，实现对网络的完全控制。因此，信息安全是对国家政治主权的一种新型的挑战。这种挑战也将使国家执政集团付出各种政治代价，例如：政府更迭、各利益集团破坏性的冲突、外部势力政治操纵等；对经济主权也将产生冲击，未来的网络经济和信息经济同样对依赖信息安全，信息能力强的国家必定控制这信息能力弱的国家经济，使信息弱的国家形成一种信息社会下的新型经济殖民地，从而导致其最终丧失经济主权。信息安全同样对文化主权也造成冲击，信息发达的国家往往借助信息技术上的优势向信息能力弱的国家灌输他们的思想观念和价值标准，这也被称为“殖民文化”，特别是广大发展中国家，由于网络建设本身滞后，内容匮乏，缺乏吸引力，慢慢地使得其国家的人民对发达国家的网络资源产生一种较强依赖心理，慢慢对外国文化产生了认同心理，这样将导致广大发展中国家逐步失去文化的控制权。社会代价是指由于信息安全而引发的公众信任危机、政府信任危机、信任丧失、社会秩序混乱和冲突。经济代价是指经济危机、信息产品更新和重复的消费使得各企业的成本增加、人们的收入减少以及猖獗的非法资金流动。各种信息孤岛、信息系统滥用、不可靠以及病毒的入侵使得人们的工作效率急剧降低。技术代价是指信息技术和标准的依赖化，是指信息弱国的生产、服务、创造能力逐渐丧失，乃至崩溃，以及自主研发能力下降乃至停滞。发达国家的知识产权以及各种数据库等资源将导致信息弱国生产的电子产品增多，从而造成消耗的资源越多，缴纳给信息强国知识产权的费用越多。生态代价是指电子技术产品的不断更新和快速淘汰，从而导致大量电子垃圾流入信息弱国的发展中国家，而致使这些国家的生态环境逐步恶化。

(3)从产生代价的经济机理上来看，长期以来，我国的信息化监管沿用的是传统的管理规章制度，并没有制定出专门的政策法规和规范性文件，对信息系统方面没有一个完整的法

律规章制度，导致信息系统的相关电子产品法律法规缺位、电子交易权责定义模糊，由此产生交易上的纠纷，客户及互联网服务提供商（ISP）法律责任划分不清。一旦因通信系统的故障造成的损失，因现行法律难以找到判别依据，从而导致责任划分不好区分。另外，因系统技术故障、安全维护、员工操作以及客户自身疏忽产生过错等均会造成损失，因缺乏相关法律依据而导致责任人较难划分。

现实社会中，国家可依法逮捕罪犯，让犯罪者承担责任，受到惩罚。这是由于有明确的司法管辖和调查，可执行强制、取证和惩罚的法律程序。而在网络虚拟社会中，犯罪的黑客也应该作为责任实体被逮捕、被惩罚。然而，当黑客身处国外，其司法管辖权与受害地将存在属地管辖冲突。因此，因司法管辖属地冲突，单纯依靠司法将不能解决黑客的入侵问题。

互联网不仅仅是由软硬件技术构成的应用系统，也可以看作是一个经济系统，而且是作为相互依赖、并具有参与动机的经济体，如，ISP、用户、黑客。当前，互联网安全问题也已经被一些经济概念所解释，如，外部性、责任、道德风险等。英国剑桥大学教授 Ross Anderson 曾指出网络信息系统的不安全是因为不好的激励作用产生的。当网络信箱系统出现障碍时，保护系统的人却不必承担其后果，系统尤其容易出现安全问题。美国学者 Hal Varian 在反病毒软件市场观察发现，人们不会花费金钱来保护别人的计算机。Kunreuther 和 Heal 提出网络信息安全是互相依赖的。因此，在单一的技术保护机制下，扭曲的经济激励和缺失的安全责任是导致信息安全问题的主要原因。由于 ISP 本身是为用户提供互联网服务的商业组织，ISP 本身不实施攻击，但一些用户却可以借助 ISP 平台实施攻击。如果让 ISP 作为责任实体，惩罚 ISP 似乎也并不合理。ISP 也不会主动承担他们没有实施的任何一项犯罪行为的责任。因此，需要引入一种机制，赋予 ISP 一种动机，使其愿意并且有责任承担其网络内的安全问题。

目前，并非所有的 ISP 网络实体都愿意承担安全责任和代价，来检查其管理网络中发出的流量，要么是没有采取安全行为，要么仅仅实施防护策略去提高其网内客户的安全。这是因为互联网是由无数的节点（ISP 及其用户）组成，网络中节点的私有性，其防护策略的安全投资是私人产品。但是网络安全是具有相互依赖性的，任何节点采取对其数据流的管控策略，都会减少整体网络的恶意流量，从而提高网络整体的安全性能，而不会排除其他网络节点从该产品和行为中享受安全利益。因此，网络管控策略具有非排他性特点。在网络的信息安全达到一定程度时，任何个体节点面对的网络环境安全程度都是一致的。对于增加一个节点，网络信息安全的边际成本为零。网络信息安全的消费又具有非竞争性特点。因此，在互联网环境下，任何节点提供的管控策略方面的安全投资和安全行为具有公共物品的性质。借用公共物品帕累托最优的萨缪尔森条件（Samuelson，1954）可以证明：互联网管控安全措施的私人供给不足，从而导致网络中信息安全问题的泛滥和悲剧。所以 ISP 只愿意为自己投资，所有 ISP 的安全策略仅仅愿意采取防护策略，没有动力为别人采取管控策略，这样就给其他 ISP 和用户带来潜在的麻烦和安全问题。

1.2.3 国家信息安全发展政策建议

国家信息安全的发展政策建议从两方面提出:第一是信息安全的战略制定及有关政策、法律、法规,这表明了国家对信息安全的决心和意志;第二是信息安全技术手段、相关技术装备和专业人才队伍,代表国家在信息安全方面的实力。

1. 信息安全保障政策

信息安全保障应放在家庭与个人、企业、政府各部门、国家乃至全球这 5 个层面上的。因此,国家的信息安全战略也应该涵盖这些不同层面。政府在信息安全政策管理方面的定位主要是两个方面:一是要保护公民在信息网络中的合法权益;二是要为社会发展提供一个健康、有序的信息化网络环境,涉及个人隐私、密码政策、执法、网络恐怖、信息战、国际经济等方面。具体政策可以为启动国家信息安全新战略的研制工作;增加对信息安全的投入;提高产业界的信息安全的意识和社会责任;改善互联网服务状况,加大执法力度;加强信息安全各部门间的协调和配合;推动信息安全方面的人才培养工作;实行信息安全情况通报和社会告警机制;提出政府专用网络的建议,引导信息安全产业的发展;提出建立信息基础设施模拟中心的设想;加强全社会的网络安全宣传,提高全民的信息安全意识。将信息安全看成所有公民都有责任和义务参与的“整体安全”工程,面向信息网络的所有开发商和使用者,动员全社会参与推动和实现国家信息安全的“社会化”,建立信息安全预警信息系统,建立“对付网络恐怖数据库”,搜集网络恐怖活动信息,开发信息安全评估等基础技术,充分调动各开发公司、技术团体、公民的志愿行动防御足以造成严重损失的潜在攻击。

2. 完善信息安全法律和认证标准

维护信息安全的一个通行做法,就是制定和完善相关的法律、法规。信息安全战略应根据网络威胁新变化随时调整制定和完善相关的法律、法规,包括计算机安全、个人隐私保护、电子签名、反黑客等信息领域的各个方面以保护个人数据和打击非法及有害信息。信息安全保障机构种类要齐全、分工明确。需要研究和制定的是符合国家利益的针对 ISP 安全策略的网络安全环境的认证标准,认证领域跨越了微观的技术层次,上升到宏观的网络管理和经济机制领域。同时,建立一个具有权威性的认证机构和认证实施策略也是非常关键的。

3. 信息安全技术和人才培养政策

美国掌握着核心信息技术及信息安全标准,因此其信息安全技术始终走在各国的前头。目前,美国信息技术开发的重心放在提高网络监控和预警能力方面。日本正全力投入新一代安全保密的高速量子信息通信网的研究。技术的开发与人才的培养密切相关,我国数量众多的大专院校、研究机构是强大的技术后盾和人才培养基地。政府部门可以采用授权认可的管理方式,指定高校和科研所作为“信息保障教育学术中心”,开设从职业培训、学士、硕士到博士的系统课程。

信息安全问题,需要由相应的技术功能和技术规则来控制。技术环境涉及硬件、软件、协议;涉及终端、网络与应用系统;涉及管理的技术设施和有关产品、系统的研究、开发、集

成、测评、配置与运行维护；涉及技术法规与技术标准。信息安全保障的有效实施，最终都依赖于各类必要的人才。人既可以是管理规则的制定者与执行者，也可以是管理规定的遵循者与制约者，然而最终是代表国家实力的人的意志和技术决定了国家的信息安全。

1.3　计算机网络信息安全存在的问题及对策

根据不完全统计，国内网民数量已经超过 5 亿，网络改变了人们的日常生活方式，通过网络进行信息交流，通过网络进行购物等，给人们的生活带来了很大的方便。然而，网络也遭受着日益严重的安全威胁，如，网络的数据窃贼、木马程序的入侵等。近年来，网络威胁越来越猖狂，可以说无孔不入，给网络用户带来了很大的危害。黑客的危害非常大，通常扮演着政治工具，侵入敌方信息系统，获取军事信息、发布假信息；非法入侵金融、商业系统，盗取商业信息；非法侵入他人的系统，获取个人隐私，以便利用其进行敲诈、勒索等。如何更好地确保计算机网络信息的安全，如何确保网络用户的利益，是信息安全技术人员一直研究的问题。

1.3.1　病毒、黑客的特点

威胁网络安全的因素主要有病毒、入侵和攻击。计算机病毒能够执行代码，可以是一个操作系统、是一段脚本，也可以是 Office 打开 Word 文档的时候获得执行权限，破坏性大，下面具体介绍其特点。

破坏性：破坏性是病毒的一个显著特点，并且破坏性是多种多样的，能够损坏数据，破坏计算机系统，或者使系统不能启动，或者窃取用户数据等等。

隐蔽性和潜伏性：计算机病毒之所以这么猖狂，是因为，他们往往是在用户不知情的情况下对计算机系统进行破坏。隐藏起来的方式有很多，如，把自己传到微软 Windows 目录下，或者传到别人不会打开的，比如回收站，系统的临时目录，然后把自己的名字改成系统的文件名，或者把它的名字和系统文件名相类似，用户运行的时候不会发现这个文件是一个病毒文件，会认为这是一个系统文件，达到隐蔽的目的，它隐蔽在后台以后可以不断运行这个程序，进行传播。

传播性：病毒可以通过很多媒介进行传播，如，软盘、硬盘、光盘、计算机网络、邮件等，所以在网络技术迅速发展的时代，计算机病毒的传播性更加明显。

1.3.2　当前网络信息安全尚存较多问题

1. 网络信息安全基础薄弱，对国外依赖性强

由于起步较晚以及国外对信息产业的严格限制，我国信息产业的发展一直处于比较被动和落后的地位，很多发达国家对我国信息产业发展采取遏制政策，阻碍我国信息产品的进口。造成我国信息产业关键部件严重依赖进口，并且在关键领域容易受到攻击和破坏。