全国信息网络安全专业技术人员继续教育培训教材

QUANGUO XINXI WANGLUO ANQUAN ZHUANYE JISHURENYUAN JIXUJIAOYU PEIXUN JIAOCAI

◎ 主　编　马民虎
◎ 副主编　黄道丽　王　玥

HULIANWANG XINXI NEIRONG ANQUAN GUANLI JIAOCHENG

互联网信息内容安全管理教程

中国人民公安大学出版社

全国信息网络安全专业技术人员继续教育培训教材

互联网信息内容安全管理教程

主　编　马民虎

副主编　黄道丽　王　玥

中国人民公安大学出版社

·北京·

图书在版编目（CIP）数据

互联网信息内容安全管理教程/马民虎主编．—北京：中国人民公安大学出版社，2007.1

全国信息网络安全专业技术人员继续教育培训教材

ISBN 978-7-81109-531-9

Ⅰ.互… Ⅱ.马… Ⅲ.因特网-信息系统-安全技术 Ⅳ.TP393.408

中国版本图书馆 CIP 数据核字（2006）第 134092 号

互联网信息内容安全管理教程

HULIANWANG XINXI NEIRONG ANQUAN GUANLI JIAOCHENG

主　编　马民虎

副主编　黄道丽　王　玥

出版发行：中国人民公安大学出版社

地　　址：北京市西城区木樨地南里

邮政编码：100038

经　　销：新华书店

印　　刷：河北省昌黎县第一印刷厂

版　　次：2007 年 1 月第 1 版

印　　次：2007 年 1 月第 1 次

印　　张：11

开　　本：787 毫米×1092 毫米　1/16

字　　数：245 千字

ISBN 978-7-81109-531-9/D·501

定　　价：30.00 元

E-mail:cpep@public.bta.net.cn

www.phcppsu.com.cn　　www.jgclub.com.cn

本书咨询电话：(010)63485228　63453145

《全国信息网络安全专业技术人员继续教育培训教材》编辑委员会

编者的话

党的十六届五中全会提出，我国在国民经济和社会发展第十一个五年规划中将全面落实“以信息化带动工业化、大力发展信息产业”的重要战略。目前，我国国民经济和社会信息化进程全面加快，信息技术得到广泛应用，网络与信息系统的基础性、全局性作用进一步增强，成为国家的关键基础设施。随着信息化的发展，信息安全问题日益增加、日渐突出。网络攻击、病毒传播、垃圾邮件等迅速增长，利用网络进行盗窃、诈骗、敲诈勒索、窃密等案件逐年上升，严重影响了网络的正常秩序，严重损害了人民群众的利益；网上色情、暴力等不良和有害信息的传播，严重危害了青少年的身心健康；针对网络和信息系统的破坏活动，以及网络与系统自身的安全问题严重影响着通信、金融、能源、交通等关键基础设施正常运转和安全；境内外敌对势力利用网络与信息技术手段所进行的捣乱、破坏活动，对社会政治稳定造成威胁。信息安全已经上升为事关国家经济安全、社会稳定的全局性战略问题，是国家安全的重要组成部分。必须从促进经济发展、维护社会稳定、保障国家安全、加强精神文明建设的高度，充分认识信息安全保障工作的重要性，增强做好这项工作的紧迫感、责任感和自觉性。

加强信息安全保障工作，必须立足国情，以我为主，坚持管理与技术并重。当前，进一步加强信息网络安全专业技术人员队伍建设，提高信息网络管理和使用单位信息安全管理和技术防范水平，是做好信息网络安全保障工作，维护信息网络安全的一项重要措施。根据公安部、人事部关于在全国开展信息网络安全专业技术人员继续教育工作的统一部署，结合信息网络安全管理和技术人

员工作实际，我们组织编写了《全国信息网络安全专业技术人员继续教育培训教材》。

本教材以邓小平理论和“三个代表”重要思想为指导，紧密结合国家信息安全保障工作相关法律法规和政策文件精神，以提升信息网络安全专业技术人员专业能力和更新专业知识，加快信息网络管理和使用单位信息安全人员队伍建设为目标，从工作实际出发，分为《信息安全管理教程》、《信息安全技术教程》、《互联网信息内容安全管理教程》和《互联网上网服务营业场所安全管理教程》四个分册，并将根据技术的发展和应用领域的新进展，不断修改完善和编制新教材，供从事不同岗位的信息网络安全专业技术人员使用，旨在通过培训学习，使信息网络安全专业技术人员全面掌握本岗位相关的信息网络安全法律法规、政策要求和基本的专业理论知识，掌握相关信息安全制度、措施、要求和基本技术技能，更好地开展信息安全保障工作。

由于编者水平有限，不足和疏漏之处在所难免，欢迎批评指正。

《全国信息网络安全专业技术人员继续教育培训教材》编写组

2006 年 11 月

目　录

第一章　互联网信息内容安全管理概述

第一节　互联网信息内容安全管理的概念与特征

一、互联网信息内容安全管理的概念

（一）互联网管理的概念

国际计算机互联网，也称因特网（Internet），已有三十多年的发展历史，它的前身是美国国防计算机互联网（ARPA），其最初作为一种技术而出现，当时人们对互联网的研究集中于互联网的物理体系结构、网络协议等，出现了TCP/IP、ISO/OSI模型等成果。经过三十多年的发展，它已经从一个学术和军事的专用网络演变为全球重要的信息基础设施，渗透到政治、经济、贸易、文化、媒体、教育等社会各个领域并产生了巨大的影响。互联网提高了社会的运转效率和生产力水平，给人们的工作、生活带来极大的便利，带来了巨大的文化变革，深度调整了经济结构和产业格局，推动了社会发展的进程。互联网已经成为人类社会必不可少的组成部分，成为知识经济时代国家的重要基础设施。

1995年，我国30个省市共31个节点的CHINANET全国骨干网建设全面启动，打通了以多条高速数字专线形成的相互连接，推动了网络的商业应用和深层次技术的发展。以此为始，互联网在中国的发展已有11年。在这11年中，中国跳过了互联网发展的实验室和科研所阶段，直接驶入商业化的“快车道”，在这个重要的核心技术应用方面与世界保持了同步。11年来，互联网迅速拓展到中国大部分地区，互联网用户从无到有，如今已达到1.23亿（截至2005年6月底），其中宽带接入用户达到7700万，互联网站数达到78.8万个，联网计算机达到5450万台。互联网国际出口带宽总量已经达到214G；在我国，互联网已经从几年前的电子邮件、信息浏览等为主要应用发展为网上商务、网络游戏、视频应用、信息交流等较为丰富的综合应用。

互联网的发展经历了独特的历程。最初，互联网主要是在民间力量的推动下，经过自下而上的技术创新与应用推广而发展起来的，并最终形成了平面化的开放式参与空间。互联网的现有规则大多也是通过自下而上、非集中化的方式形成的，这种模式重视发挥民间团体、私营部门和个体的作用，鼓励创新精神，注重效率、开放性和有效性，强调没有政府参与和限制的自由和平等。其早期的一个设想就是“互联网跨越国家界限，侵蚀主权原则”，即互联网是一个虚拟的世界，是一个无组织、无政府、无国界的数字空间。

这种早期管理模式在互联网发展初期，对于全球互联网的繁荣和发展确曾起到积极的推

动作用。但是，随着互联网的快速发展壮大，它已经演变为重要的全球信息基础设施，并已经全面渗透到社会的各个方面，关系到国家的主权和公众的利益，涉及众多公共政策，如应对和打击垃圾邮件、网络犯罪、消费者权益保护以及国家的政治与经济安全等问题。互联网的这些新发展导致越来越多的人不得不承认互联网是现实世界的一部分，并进一步反思互联网的管理理念。联合国秘书长科菲·安南在2004年的互联网管理全球论坛上的讲话很有代表性，“几年之内，互联网已使贸易、医疗、教育以及人类通信和交流的基础设施发生了革命性变化。而且它的潜力要远远大于自从其诞生以来的短暂时间内我们所能看到的。为了管理、促进和保护互联网在我们生活中的存在，要求我们具有的创造力应绝不少于那些创造了互联网的人们。显然，管理是需要的，但这并不是说，这种管理是传统意义上的，因为它们毕竟是如此的不同”。

目前对互联网的共识是互联网的确需要管理，但不同的团体和组织对互联网管理的范畴存在不同的理解。如电信专家认为互联网管理的重点是转变核心设计理念，发展技术基础设施；计算机专家认为互联网管理的重点是各种标准与应用的发展，如XML或JAVA等；教育界则认为互联网在促进教育普及的同时应保证青少年远离网络上的不良信息；经济界人士则关心如何安全地开展电子商务；人权组织则从保护人们言论自由、隐私以及其他基本人权的角度看待互联网管理；法律专家关心的是如何解决与互联网有关的法律问题；政治家关心的是在互联网全球普及的环境下，如何保护国家利益并消除数字鸿沟；等等。

鉴于目前对互联网管理范畴的不同理解，联合国互联网治理工作组（Work Group on Internet Governance，简称WGIG）2005年6月在博塞堡发表的《互联网治理工作组的报告》中制定了互联网管理的工作定义，其认为互联网管理是政府、私营部门和民间社会根据各自的作用制定和实施旨在规范互联网发展和使用的共同原则、准则、规则、决策程序和方案。这项工作定义强化了政府、私营部门和民间社会共同参与互联网管理机制的概念。确认互联网管理所涵盖的不仅仅只是互联网名称和地址，还包括其他重大的公共政策问题，如重要的互联网资源、互联网安全保障包括垃圾邮件、网络安全、网络犯罪以及互联网使用有关的问题。

2006年3月19日，中共中央办公厅、国务院办公厅印发的《2006～2020年国家信息化发展战略》分析了全球信息化发展的基本趋势和我国信息化发展的基本形势，明确提出了我国信息化发展的指导思想、战略目标、战略重点、战略行动计划和保障措施。其中加强互联网管理是九大保障措施之一。

（二）互联网信息内容安全管理的概念

借鉴联合国互联网治理工作组（WGIG）关于互联网管理的定义，本书的互联网信息内容安全管理，是指政府、私营部门和民间社会根据自己的作用，共同参与对互联网信息内容的管理，在对互联网信息内容进行控制和制约的基础上，以实现信息内容的完整性、机密性和可用性。

（1）完整性，是指确保避免信息的非正当修改或破坏，还包括确保信息的可认可性和真实性；

（2）机密性，是指保留授权访问和信息披露限制，包括个人隐私和私有信息的保护；

（3）可用性，是指确保适时可靠的信息访问和使用。

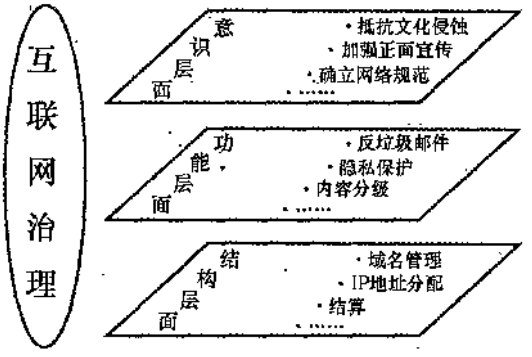
从广泛意义上来说，互联网信息内容安全要控制的信息内容包括：Email 中携带的病毒、恶意代码以及秘密信息；浏览的 web 页的合法性——是否为病毒、恶意代码和色情信息等；下载信息的合法性；垃圾邮件；非法攻击国家、有碍和平的信息等。对于互联网内容的管理，不同国家有不同的标准。在我国，可以用合法、合情、合理来概括管理的标准。首先，不能违反国家法律，也就是说，违反我国宪法和法律的言论当然不能容许在网上泛滥；其次，要合情、合理，合乎中国社会通常公认的伦理道德，合乎中国人民通常的人情。

正如美国著名网络法研究专家，哈佛大学的 Lawrence Lessig 教授指出的那样，电子空间技术性规则同物理性规则的不同之处在于：这些技术性规则是人类的创造之物，人类为了自己的需要可以在一定程度上改变这些技术规则，国家法律完全可以通过支配技术性规则对网络实行信息内容间接管理。在控制网络信息的内容上，可以采取硬件控制和软件控制的方法：

（1）硬件控制。网络空间的行为只有通过电信网络和电子设备才能够完成。政府可以采取的最极端的做法是：当网络信息可能给本国带来毁灭性的影响时，政府可以停止电子设备的使用，以切断电信网络信息同外界的联系。当然这种做法是极端的，成本过高。一般情况下，政府不应该也不会使用这种强制性的权力。另一种做法是：可以进行访问出口控制。例如，我国政府制定的《计算机信息网络国际联网出入口信道管理办法》第 2 条规定，我国境内的计算机信息网络直接进行国际联网，必须使用邮电部国家公用电信网提供的国际出入口信道。

（2）软件控制。通过过滤、终端访问控制等软件，政府可以将已知的反政府的或者色情的内容过滤掉，阻止本国用户对这些网站的访问。

根据互联网的发展阶段，互联网管理（同时也称为互联网治理）划分为三个层面（图一）：



图一 互联网治理的分层模型

第一，早期互联网管理的重点——互联网结构层面的管理。如对域名的管理、对 IP 地址分配的管理、对网络之间的费用结算问题的管理等。第二，目前互联网管理的重点——互联网功能层面的管理。这是随着互联网上各种各样应用的出现而出现的相关的管理措施，如针对垃圾邮件的管理措施、针对隐私保护的措施以及针对网络游戏进行分级的措施等。第

三，今后互联网管理的重点——互联网意识层面的管理。互联网在意识形态领域的不良影响主要表现为两个方面：一是不良信息和有害信息的网络传播。在互联网中，网络的虚拟性、匿名性使传统的道德约束手段失去了根基，于是有人利用网络开始肆无忌惮地宣扬色情、暴力、恐怖主义及极端主义。在我国，互联网上大量不良信息和有害信息的传播，严重影响着未成年人的健康成长，也对社会造成相当大的危害。此外，网络违法犯罪活动也在日益增多，各种违法犯罪分子利用网络的匿名性和监管控制难等特点，将网络作为联络和作案工具进行诈骗、赌博等违法犯罪活动。二是针对主权国家的有目的的、反动的网络宣传和破坏。互联网意识层面的问题更隐蔽、更难于辨别，如一些宣扬资产阶级自由化思想的内容往往披着“和平、民主、自由”的“外衣”，它们通过各种方式渗透进来，包括网络新闻、网络评论、网络游戏、网络影视等方式，有的甚至打着学术探讨的旗号出现。因此，人们既要提高警惕，防止严重情况的出现，也必须清醒地认识到当今世界发展的趋势，不能采用一味封堵的措施，要正确区分正常的学术交流和恶意的攻击诽谤，积极地对互联网的内容进行规范和引导。

二、互联网信息内容安全管理的特征

（一）互联网信息内容安全管理主体多元性

从政治学的角度来说，管理，是指各种公共或私人机构管理其共同事务的诸多方式的总和，它是使相互冲突的或不同的利益得以调和并且采取联合行动的持续的过程。它既包括有权迫使人们服从的正式制度和规则，也包括各种人们同意或认为符合其利益的非正式的制度安排。互联网信息内容安全管理也具备“管理”这一基本的内涵，互联网信息内容安全管理的主体包括了政府部门、私营部门和民间社会，这些主体共同对互联网信息内容进行管理。

互联网信息内容安全管理主体的多元化体现了公众参与原则。公众参与原则，是指在网络安全保护活动中，网络参与的各方都有维护网络安全的权利，同时也负有维护互联网安全的义务。经济合作与发展组织（OECD）成员国通过的《信息系统和网络安全指南》中就规定，“所有参与者都对系统和网络安全负责。参与者依靠相互连接的当地及全球的信息系统和网络，因此应该知道他们应负的责任。参与者应定期回顾他们的政策、惯例、措施和步骤以及评价它们是否适合他们的环境。开发、设计和供应产品和设备者应致力于系统和网络安全，并及时提供适当的包括升级的信息，这样用户就更能了解产品和服务的安全功能及他们的安全责任。”联合国《互联网治理工作组的报告》也强化了政府、私营部门和民间社会共同参与互联网管理机制的概念。报告指出，互联网管理是政府、私营部门和民间社会以及政府间组织和国际组织的作用和责任。报告尤其指出，学术界对互联网的贡献十分宝贵，是启发、创新和创造活动的主要来源之一。同样，技术界及其各组织参与互联网业务、互联网标准制定和互联网服务发展的程度很深。这两类群体在互联网的稳定、安全、运作和发展方面发挥着持久、宝贵的作用。他们同各类利益相关者以及在这些群体内进行着广泛的交往。

公众参与原则要求互联网信息内容安全管理摒弃封闭式的管理体制，建立开放式管理体制。从政府强有力的贯彻向用户的普遍参与过渡，体现积极防御和风险控制思想。风险控制思想的实质是以高效率的互联网安全保障为原则，将风险控制的责任分配给最有能力控制风

险的一方。行业主管部门最熟悉本行业的互联网应用情况，投资者最关心其投资利益，应当给他们分配相应的风险控制责任。给行业、投资者和用户分配控制风险责任还在于认识到政府管理能力的有限性。毫无疑问，政府发现、分析威胁互联网安全需要及时掌握必要的信息，而如果企业知情不报，信息收集、通报和分析的工作就无法落实。只有政府、企业和个人密切配合，才能弥补政府互联网信息内容安全管理能力的不足，使其更好地履行职责，实现保障社会安全的目标。

（二）互联网信息内容安全管理强调系统性

首先，互联网信息内容安全管理涉及到技术、管理、法律、道德等多个方面。其次，它涉及到多方主体，如互联网信息内容安全监管国家专门机构、其他互联网经营管理机构和安全管理机构、互联网普通用户、以黑客为代表的破坏分子、其他国家敌对势力和社会大众。各相关主体的职责、权利、义务均需明确，只有各主体的权利义务明确了，各主体才能依法行为，指导行为，预见其行为后果。最后，它涉及到对多种行为的监管。与互联网信息内容安全相关主体对应，与互联网信息内容安全相关的行为更为复杂多样，具有多面性与复杂性的特征。

（三）互联网信息内容安全管理强调技术性

信息技术尤其是网络技术的发展给人类社会带来了信息安全问题，信息安全问题直接影响一个国家的国防、电力、铁路、银行、证券、税务、海关等国家重要基础设施和信息系统的正常运转。世界各国都高度重视国家信息安全问题，美、俄等国先后调整国家安全战略，使信息安全保障成为国家安全保障战略中不可分割的重要组成部分。信息安全是对高技术的对抗，从根本上讲，信息安全问题由信息技术带来，也要通过信息技术解决。技术是保证信息安全保障工作的物质基础，为信息安全管理提供手段和支持。单纯依靠管理，可以在一定时间、一定范围内解决信息安全问题，但如果没有技术支持，不可能有根本的、长远意义上的解决。互联网上电子邮件、电子公告板系统及电子广告等的设立，原本是以高科技为依托，为用户提供快捷、灵活的信息服务，而现在却成了信息污染传播的媒介，网络环境的污染与高科技的挂钩使得管理工作面临更加严峻的挑战。因此，从技术控制来讲，唯一的出路只能是“以技术对抗技术”。只有采取比网络污染者更先进、更高超的技术手段，进一步加强技术控污能力，才可能清除这些同样是高科技的产物，技术形成的问题才可以通过技术措施予以解决。

西方国家在互联网信息内容安全管理上非常重视技术因素的作用。西方学者认为，网络独特的技术结构形成了不同的信息运用规则，虽然法律也能使科技排除一些困难的选择或限制用户的不当活动，但通过科技自身的控制能形成更有效的政策选择；对于因技术不完善或技术发展而引起的社会问题，可以通过技术进步或技术的进一步发展来控制或解决。

克林顿政府曾经试图利用法律来规范网络内容，但是最后以失败而告终，并宣告以后要用科技的方式来替代法律的限制。麻省理工学院所属的 W3C（World Wide Web Consortium）推动了 PICS（Platform for Internet Content Selection）技术标准协议，设立网络分级制度标准，完整定义了网络分级所采用的检索方式，以及网络文件分级卷标的语法。此分级方式是通过累积不适当网络信息的数据库系统，确定筛选的标准。另外，在以 PICS 为技术核心且最为

成熟的RSAC中，研发RSACi（RSAC on the Internet）分级系统，它主要以网页呈现内容中的性、暴力、不雅言论和裸体表现程度等四个项目作为依据进行分级。1996年微软浏览器Internet Explorer 3.0当中便设置RSACi的标准，而网景（Netscape）公司也于1998年在公司所生产的浏览器中加入此项分级标准。日本通产省与NEC公司也共同开发了过滤系统，防堵犯罪、色情与暴力网站，以保护青少年的身心健康。1999年9月澳大利亚互联网协会公布了《网上业务规范草案》，要求网络服务提供商向用户提供必要的网上内容过滤软件。

第二节　国外互联网信息内容安全管理概况

一、有关国际组织的规定

互联网国际治理问题第一次在联合国层面上进行全面、细致、深入地讨论和协调，始于2003年的信息社会世界峰会（WSIS）日内瓦阶段。2003年12月联合国召开了信息社会世界高峰会议日内瓦阶段（Phase I）的会议，在该次会议及之前的筹备会上，互联网治理成为与会各方关注的焦点问题之一。对此主要有三方面观点：一是以美国和一些发达国家为代表的意见，认为互联网治理的范畴仅仅限于ICANN从事的技术协调工作；在互联网治理领域应继续坚持由私营部门主导，反对政府的介入。二是以中国、巴西、南非、印度、埃及等发展中国家为代表的意见，认为应以广义的观点来看待互联网治理问题，它不仅包括IP地址、域名、根服务器等互联网资源的管理，而且涉及垃圾邮件、知识产权、不良信息管理等诸多公共政策问题，因此，需要各国政府的介入；互联网治理应纳入联合国框架，由政府发挥主导作用；也有些国家明确提出支持ITU作为联合国下的专门管理互联网公共政策的机构。三是民间团体既强烈批评ICANN的垄断，又不支持政府间组织管理互联网的方案，而希望采用非集中的管理机制，使有关各方均能在互联网治理中发挥作用。

与会各方经充分协调和妥协，最终达成了一定的原则共识，承认互联网治理包括技术和公共政策等问题，包括政府在内的各利益相关方均应参与治理；互联网治理过程应是开放和包容的，是多边的、透明的、民主的；与互联网治理有关的公共政策问题是各成员国主权范围内的事情，成员国政府有权和有责任对与互联网有关的国际公共政策事宜进行治理。作为峰会日内瓦阶段会议的成果，这些基本原则被写入峰会日内瓦阶段会议的主要文件："原则宣言（Declaration of Principles）"和"行动计划（Plan for Actions）"。峰会日内瓦阶段会议能达成这些原则共识，标志着互联网国际治理有了历史性的进步，互联网国际治理体系中首次有了联合国的声音。但是，峰会日内瓦阶段会议对于包括互联网治理的具体定义、互联网治理中公共政策的范畴、互联网治理中各利益相关者的作用及角色等实质性问题并未达成一致。为了进一步讨论互联网治理问题，峰会日内瓦阶段会议要求联合国秘书长科菲·安南建立联合国互联网治理工作组（WGIG），其主要任务是研究、阐述互联网治理的工作定义，互联网治理中公共政策的范畴和内涵，各利益相关方（包括政府、私营部门和民间社会等）在互联网治理中的责任和作用。工作组要在2005年11月WSIS第二阶段突尼斯峰会之前，对包括以上问题的互联网公共政策问题进行研究，并向WSIS第二阶段会议提出建议报告。