

全国网络安全与执法专业系列教材

# 网络安全与 执法导论

徐云峰 王靖亚 邵翀 王斌君 编著



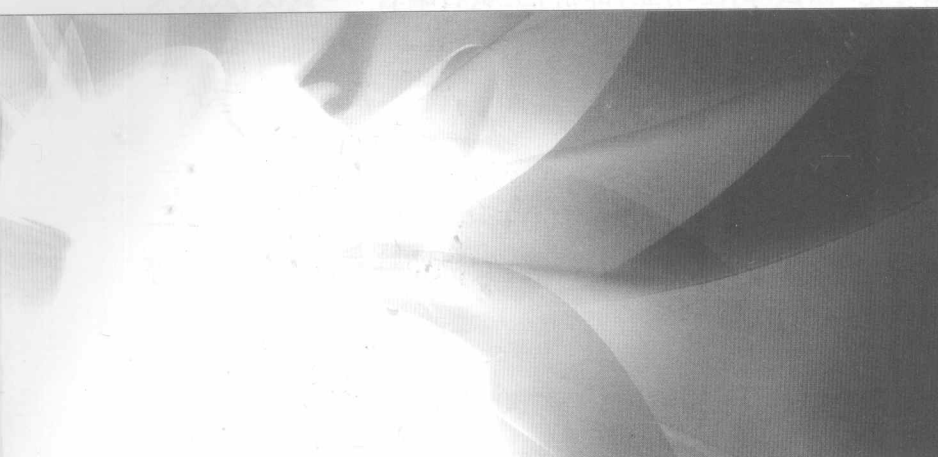
WUHAN UNIVERSITY PRESS

武汉大学出版社

013069702

D631  
41

全国网络安全与执法专业系列教材



# 网络安全与 执法导论

徐云峰 王靖亚 邵翀 王斌君 编著



D631  
41



北航

C1677784



WUHAN UNIVERSITY PRESS

武汉大学出版社

图书在版编目(CIP)数据

网络安全与执法导论/徐云峰,王靖亚,邵翀,王斌君编著. —武汉:武汉大学出版社,2013.8

全国网络安全与执法专业系列教材

ISBN 978-7-307-11343-5

I. 网… II. ①徐… ②王… ③邵… ④王… III. ①计算机网络—安全技术—高等学校—教材 ②计算机网络—公安机关—行政执法—高等学校—教材 IV. ①TP393.08 ②D631

中国版本图书馆 CIP 数据核字(2013)第 154730 号

责任编辑:林 莉      责任校对:王 建      版式设计:马 佳

出版发行:武汉大学出版社 (430072 武昌 珞珈山)

(电子邮件:cbs22@whu.edu.cn 网址:www.wdp.whu.edu.cn)

印刷:湖北省荆州市今印印务有限公司

开本:787×1092 1/16 印张:15.5 字数:390千字 插页:1

版次:2013年8月第1版      2013年8月第1次印刷

ISBN 978-7-307-11343-5      定价:39.00元

版权所有,不得翻印;凡购买我社的图书,如有质量问题,请与当地图书销售部门联系调换。

## 前言

公安机关肩负着维护中国共产党的执政地位、维护国家长治久安、保障人民安居乐业的重大政治责任和社会责任。根据我国行政体系的职能划分，“预防、制止和侦查违法犯罪活动”<sup>①</sup>是国家赋予公安部门的神圣职责。在网络化的虚拟信息社会中，维护其稳定、安全、防、控、打各种新型的计算机犯罪是公安机关义不容辞的责任。

本书共分为7章。第1章（引论）描述了信息化的发展而形成的“虚拟社会”中各种技术安全、社会安全、网络犯罪等严重的形势，我国法律和国家赋予公安机关治理“虚拟社会”面临的巨大挑战和艰巨任务，以及网络安全与执法技术专业的知识体系结构。第2章（网罗天下）阐述了 Internet 网络、电信网络、电视网络、物联网络和三网合一等各种网络促进社会信息化情况，以及由于网络发展而促使的第四媒体和“虚拟社会”的发展变化情况。第3章（网安天下）阐述了管控“虚拟社会”涉及的法律、管理、技术、标准和伦理等方面的新挑战和亟待解决的问题。第4章（网管天下）阐述了微观层面的技术管理和宏观层面的行政管理内容。第5章（网情天下）阐述了“虚拟社会”中网情、舆情和情报等主要工作。第6章（网控天下）阐述了“虚拟社会”中突发舆情和安全事件的预防、控制与处置。第7章（网侦天下）阐述了网络犯罪以及侦查取证和检验鉴定等内容。

徐云峰负责本书的整体框架构思和设计。具体分工为：徐云峰和王斌君负责第1章的撰写工作，徐云峰和王靖亚共同负责第3、4、6章的撰写工作，徐云峰和邵翀共同负责第2、5、7章的编写工作。徐云峰负责整本书的统稿工作。

在本书出版之际，对关心和支持我们编写和出版工作的所有同志表示感谢。在本书的写作过程中，得到王斌君教授以及多位实战部门专家的悉心指导，在此对他们无私的帮助表示诚挚的感谢。

由于作者水平有限，欢迎大家多提宝贵意见。

作者

2013年5月于北京

<sup>①</sup>中华人民共和国人民警察法（中华人民共和国主席令第40号），1995。



## 目 录

第1章 引 论	1
1.1 网络安全保卫的形势和任务	1
1.1.1 网络安全现状	1
1.1.2 公安机关对网络安全保卫的神圣职责	1
1.2 网络安全保卫工作的光辉历程	2
1.2.1 网络安全保卫部门的发展	2
1.2.2 网络安全保卫部门的职能定位	3
1.2.3 网络安全保卫部门的光辉业绩	4
第2章 网罗天下	14
2.1 社会信息化	14
2.1.1 Internet网	16
2.1.2 电信网	21
2.1.3 电视网	26
2.1.4 三网融合	28
2.1.5 物联网	30
2.1.6 其他网络	32
2.2 信息社会化	35
2.2.1 第四媒体	36
2.2.2 虚拟社会	38
第3章 网安天下	48
3.1 网络安全隐患及其威胁来源	48
3.1.1 硬件系统的脆弱性	48
3.1.2 软件系统的脆弱性	48
3.1.3 网络和通信协议的脆弱性	49
3.1.4 人员的因素	50
3.1.5 网络安全威胁及其来源	51
3.2 信息网络安全法律法规	52
3.2.1 信息安全法律	52

3.2.2	信息安全法规	57
3.2.3	信息安全部门规章	59
3.2.4	信息安全地方法规	61
3.2.5	保证信息安全的部分规定	61
3.3	信息网络安全技术	61
3.3.1	信息系统防御策略基本原则	62
3.3.2	系统安全的工程原则	62
3.3.3	身份认证技术	63
3.3.4	访问控制技术	63
3.3.5	防病毒技术	64
3.3.6	防火墙技术	66
3.3.7	漏洞扫描技术	66
3.3.8	入侵检测技术	69
3.3.9	安全审计技术	69
3.4	个人计算机系统的安全和管理	70
3.4.1	个人计算机安全注意事项	70
3.4.2	个人计算机保护措施	71
3.4.3	常用文件加密操作	75
3.5	信息安全标准	79
3.5.1	可信计算机安全评价标准TCSEC	79
3.5.2	信息技术安全评估标准ITSec	81
3.5.3	信息技术安全评价通用准则CC	82
3.5.4	中国的信息安全管理标准	83
3.5.5	中国的信息安全产品评测标准	83
3.5.6	中国的网络信任体系标准	84
3.5.7	中国的网络安全应急处理标准	84
3.5.8	中国的信息安全风险评估标准	84
第4章	网管天下	85
4.1	互联网管理概述	85
4.1.1	互联网管理相关概念	85
4.1.2	互联网管理的指导思想	86
4.1.3	互联网管理的基本原则	87
4.1.4	互联网管理的主要任务	87
4.2	互联网单位的备案管理	88
4.2.1	互联网单位备案管理依据	88
4.2.2	互联网单位备案管理管辖	89



4.2.3	互联网单位备案管理内容	89
4.2.4	备案管理流程	91
4.3	互联网上网单位日常监督管理	93
4.3.1	对互联网单位的监督管理流程	93
4.3.2	对互联网单位管理的基本内容	94
4.3.3	对互联网单位的分类监督管理	95
4.3.4	对互联网联网单位的监督管理	101
4.3.5	对互联网上网服务营业场所的监督管理	102
4.4	互联网信息管理	106
4.4.1	对互联网信息管理的法律依据	106
4.4.2	互联网信息监督管理的主要任务	107
4.4.3	互联网信息搜集	107
4.4.4	互联网信息分析研判	109
4.4.5	互联网信息编报	111
4.4.6	互联网有害信息处置	113
4.5	恶意代码的管理	114
4.5.1	恶意代码管理法律依据	115
4.5.2	恶意代码管理内容	115
4.5.3	恶意代码管理具体要求	116
4.6	计算机信息系统安全等级保护	116
4.6.1	等级保护的基本思路	116
4.6.2	等级保护的保障	118
4.6.3	等级保护的标准体系	118
第5章 网情天下		
5.1	概述	123
5.1.1	情报	123
5.1.2	大数据	124
5.1.3	搜索引擎	125
5.1.4	数据仓库	125
5.1.5	数据挖掘	126
5.1.6	社会网络	126
5.1.7	社会计算	127
5.2	网情	129
5.2.1	网情现状	129
5.2.2	上网接入方式	133
5.2.3	整体互联网应用状况	137



98	5.2.4 互联网安全形势	138
105	5.3 情报	141
129	5.3.1 情报的基本属性	141
129	5.3.2 公安情报信息	142
130	5.3.3 网络公安情报搜集的必要性	143
130	5.3.4 网络公安情报搜集的对象	143
101	5.3.5 网络公安情报搜集的内容	144
101	5.3.6 网络公安情报搜集体系建设	145
601	5.3.7 互联网环境下公安情报搜集方法	148
801		
	<b>第6章 网控天下</b>	<b>150</b>
101	6.1 网络舆情概述	150
101	6.1.1 舆情的具体含义	150
111	6.1.2 网络舆情主要生成载体	151
111	6.1.3 网络舆情的积极意义	152
111	6.1.4 网络舆情的负面影响	153
211	6.1.5 网络舆情应急处理误区	154
211	6.1.6 网络舆情预警措施	155
311	6.1.7 网络舆情预警流程	156
311	6.1.8 网络舆情预警体系	158
311	6.1.9 网络舆情监控	161
311	6.1.10 网络舆情导控	163
411	6.2 特殊网络机构和特殊网民的管控	168
	6.2.1 网络公关公司的管控	168
431	6.2.2 “意见领袖”的识别和管理	170
431	6.2.3 “网络推手”的识别和管理	173
431	6.2.4 “网络水军”的识别和管理	175
411	6.3 网络安全突发事件的控制	178
431	6.3.1 网络安全突发事件概述	178
431	6.3.2 网络安全应急响应组织	180
431	6.3.3 网络安全应急响应处置	183
431	6.3.4 网络安全应急响应关键技术	185
431	6.3.5 网络安全事件应急预案举例	187
431	6.3.6 网络安全应急响应展望	192
431		
	<b>第7章 网侦天下</b>	<b>194</b>
101	7.1 概述	194



7.2 网络犯罪	194
7.2.1 网络犯罪的特点	194
7.2.2 网络犯罪的类型	198
7.2.3 网络犯罪的管辖	199
7.2.4 网络犯罪的法律适用	204
7.3 网络侦查	208
7.3.1 工作流程	208
7.3.2 现场勘查	210
7.3.3 网络取证	215
7.4 检验鉴定	219
7.4.1 电子数据概述	219
7.4.2 电子数据的特点	220
7.4.3 常见电子设备中潜在的电子证据	221
7.4.4 电子证据的检验鉴定方法	222
参 考 文 献	237





# 第1章 引 论



## 1.1 网络安全保卫的形势和任务

信息技术是 20 世纪最伟大的发明之一,随着计算机、计算机网络和通信等关键信息技术的飞速发展,计算机以从纯粹的科学计算领域,发展到工业控制、事务管理等广泛领域的应用,深入到政治、国防、外交、工业、金融、商业和教育等社会的方方面面,深入到人们工作、学习和生活的角角落落,正在深刻影响着人们的工作模式和生活方式,乃至整个社会的协作模式和结构。信息在社会发展和人民生活中的隐形和从属地位,逐渐变为显式的主导地位,信息与物质和能源一起构成当今社会的三大基础元素,已成为推动社会发展的巨大原动力。计算机和计算机的通信网络已发展成为现代社会的“中枢神经”,人类社会正在、已经、将来必将更加依赖于由计算机、计算机网络和通信网络构成的网络化的虚拟社会。

### 1.1.1 网络安全现状

然而,信息技术也是一把双刃剑,它在给人类带来文明、进步和便利的同时,也带来了新的安全隐患和威胁。敌对国家和组织利用计算机网络煽动国家分裂、民族仇恨,制造各种政治危机;网络上各种信息良莠不齐、鱼目混珠、泥沙俱下,流言蜚语、黄色信息充斥;敌对势力和黑客利用网络针对网络上的信息大肆进行攻击和各种破坏活动;网上信息的真伪难以辨认,在电子政务、电子商务和网上银行等各类社会活动中数据的真实性、可靠性无法保障,各种合同纠纷层出不穷;计算机病毒肆意泛滥,严重影响了信息化社会的正常运转和健康发展;在虚拟的“网络空间”中也滋生一种新型的计算机犯罪,犯罪分子利用高科技手段,大肆窃取国家机密,涉及金融犯罪的数量剧增、数额巨大,产生了严重的社会危害。由于我国关于计算机犯罪的法律法规尚不健全,对计算机犯罪的防御、控制、侦查取证、定罪量刑等尚待研究,这方面的专业技术人才严重匮乏。在网络化的信息社会中,国家机密、企业秘密和个人隐私的保护显得尤为重要,信息化社会中的这些安全问题使国家安全、社会安全面临新的严重挑战。网络化空间(称为“领网”)已经继领地、领海、领空之后,成为国家安全的重要组成部分,备受各国政府和人民的关注,它是国家意志、政府行为的体现,必须引起高度重视,需要全社会的广泛参与。

### 1.1.2 公安机关对网络安全保卫的神圣职责

公安机关肩负着维护中国共产党的执政地位、维护国家长治久安、保障人民安居乐业的重大政治责任和社会责任。根据我国行政体系的职能划分,“预防、制止和侦查违法犯罪活动”<sup>①</sup>是国家赋予公安部门的神圣职责。维护网络虚拟社会的稳定、安全,防、控、打

<sup>①</sup>中华人民共和国人民警察法(中华人民共和国主席令第40号),1995。

各种新型的计算机犯罪是公安机关网络安全保卫部门必须深入研究和探讨的问题。

为适应信息化社会的发展要求,公安部党委根据国家赋予公安机关的事权,以邓小平理论和“三个代表”重要思想为指导,全面落实科学发展观,牢固树立政权意识,认真研究了信息化技术对未来社会的影响,分析了新形势下国家和社会安全的新要求,以及各种传统犯罪在信息化社会的新特点,及时作了战略部署,成立了公共信息网络安全监察警种,建制从公安部到省公安厅(局)到地市局的公共信息网络安全监察局、处、科等组织机构,以网上侦察和情报信息为主线,以监督管理和技术手段为支撑,以有效控制网上有害信息传播和恶意操作、有效防止网上组织策划非法活动和组党结社、有效打击网络违法犯罪、有效保障信息网络安全为目标,不断加强专业队伍、专业手段、专门知识和专门机制,不断提高网上发现处置、侦察打击、主动进攻和防范控制能力,争取网上斗争的掌控权和主动权,全面开展公共信息网络安全监察工作。

## 1.2 网络安全保卫工作的光辉历程

网络安全保卫部门以维护国家安全和社会政治稳定为首任,以网上侦察情报为主线,充分发挥安全监察管理和网络技术手段两个优势,及时发现、严密侦控、有效防范、依法打击境内外敌对势力、敌对分子以及各种违法犯罪分子利用网络进行的各种煽动、渗透和破坏活动。通过 20 多年的网上斗争和历练,网络安全保卫部门职能不断明确、队伍不断充实、法律法规不断完善、信息网络控制能力不断增强,网络安全保卫警种也已经成为公安部机关开展网上斗争,维护信息化的虚拟空间安全,乃至国家安全和社会稳定的重要力量。

### 1.2.1 网络安全保卫部门的发展

1983 年 9 月,国务院批准公安部成立计算机管理监察司。同年末,计算机管理监察司改名为计算机管理监察局(公安部第十一局),标志着公安机关正式肩负起计算机管理和监察任务。

1988 年 12 月 21 日,公安部印发了《全国公安计算机安全监察工作会议纪要》,要求各省、自治区、直辖市公安厅、局迅速建立起一支公安计算机安全监察队伍,为全国计算机管理和监察工作提供组织保障。

1998 年 9 月,经中编办批准,公安部原计算机管理监察局改名为公共信息网络安全监察局。其主要职责是:指导并组织实施公共信息网络和国际互联网的安全保卫工作;掌握信息网络违法犯罪动态,提供计算机犯罪案件证据;研究拟定信息安全政策和技术规范;指导并组织实施网络安全监察工作。

2001 年,经部领导批准,政治部做出了《关于同意十一局调整内设机构职能的批复》(公人[2001]273 号),将十一局的职责调整为:指导并组织实施公共信息网络和国际互联网的安全保护工作;指导并组织实施信息网络安全监察工作;参与研究拟定信息安全政策和技术规范;依法查处在计算机网络中制作、复制、查阅、传播有害信息和计算机违法犯罪案件;依法按照严格的批准手续,对计算机信息网络中的特定对象和目标实施技术侦察。

2002 年 4 月,公安部召开全国公安公共信息网络安全监察工作会议,进一步明确了公共信息网络安全监察部门是以网络技术为主要手段,集情报收集、侦察监控、打击犯罪和防范管理于一体的综合实战部门。



2003年,根据胡锦涛总书记的批示和国务院信息办的要求,公安部十一局组建了国家网络与信息安全信息通报中心,承担我国网络与信息安全的分析、研判和通报任务。

根据2003年中央27号文和2004年召开的国家信息安全会议精神,公安部公共网络信息安全监察局将负责全国的国家信息安全等级保护工作,承担信息安全等级保护的实施,并肩负相关的监督检查任务。

### 1.2.2 网络安全保卫部门的职能定位

从1983年公安部计算机管理监察司成立,到今天的公共信息网络安全监察局,在公安部党委的正确领导下,开创了我国信息化社会中“网上斗争”的先河,针对技术和形势的变化,不断调整工作重点,明确工作思路,确立了公共信息网络安全监察部门是我国开展网上斗争实战部门的职能定位:

开展互联网信息监控和处置,及时发现、处置网上反动、有害信息和煽动破坏活动;

依法加强信息网络安全监督管理,监督、检查互联网安全管理制度和安全保护技术措施落实情况,维护信息网络安全秩序;

防范和查处针对信息网络的违法犯罪和主要违法犯罪行为信息网络中实施的其他违法犯罪,协助查处利用信息网络的违法犯罪;

建设、管理和使用互联网侦查手段,依法对网上特定对象、特定目标和特定信息展开技术侦察;

开展网上舆情控制工作,防止网上恶意炒作影响社会稳定;

监督、检查、指导重要信息系统的信息安全等级保护工作,承担国家网络与信息安全的通报任务。

公共信息网络安全监察部门认真落实了胡锦涛总书记、温家宝总理、罗干和周永康等中央领导同志关于网上斗争的一系列重要指示精神,经过20多年的艰苦创业和开拓进取,公共信息网络安全监察部门能适时分析网上斗争形势,及时提出应对措施,不断总结经验,取得了骄人的成绩。

公共信息网络安全监察部门的机构不断完善,队伍不断扩大。全国所有的各省(自治区、直辖市)公安厅(局)和地公安局,以及三分之二的大中城市均设立了公共信息网络安全监察机构。全国公共信息网络安全监察民警超过4500人,这支年轻的队伍,文化层次较高,年龄结构合理。

加强网上斗争技术手段和装备,网上斗争能力进一步加强。通过网上斗争技术手段的研制和大规模的装备,使得获取网上案件线索、挖掘情报、预防和发现犯罪、阵地控制、获取证据、协助侦查办案等方面的能力极大提高,为公安机关精确打击、有效打击各类网上犯罪发挥了重要作用。

公共信息网络安全监察部门通过互联网信息监控、舆情控制和情报侦察,基本能控制网络上信息和舆情的主动权,净化了网络空间,维护了信息化社会的秩序,维护了国家和社会政治稳定。

在全国实行计算机信息系统等级保护。对全国涉及国家安全的重要领域和重点单位的计算机系统实行等级保护,增强了其信息安全的防御能力和管理能力。根据国家赋予公共信息网络安全监察部门的事权,依法对这些单位的信息系统等级保护工作进行监督、检查和指导,降低了信息安全事件的风险,有效地确保了国家重点领域和重点单位信息系统的安全。



2002年以来,网络安全保卫部门年均办案上万起;集中力量打击淫秽色情网站和网络赌博等专项活动;协助有关业务部门开展命案侦察、网上追逃、“两抢一盗”等活动,破获了一大批重、特大案件,有效打击了计算机和其他各类违法犯罪活动,维护了信息化社会的公共秩序,保障了国家安全和社会政治稳定。

### 1.2.3 网络安全保卫部门的光辉业绩

#### 1. 加强对策研究,信息安全监察法律法规不断完善

信息化社会需要计算机互联、互通、互操作,以便信息共享与交换,单位和部门内部需要互联互通的计算机局域网,单位和部门之间、国家内部不同地域之间都需要互联互通的计算机广域网和城域网,之至最大的全球范围内的国际互联网。人们在互联互通的网络上,可以便捷地办公、学习和娱乐,传统的社会协作和工作模式发生了本质性的变化,电子政务、电子银行、电子商务、电子教育等应运而生,形成了以计算机快速计算和大量存储信息,以网络快速传递信息为特征的虚拟化信息社会。

在网络化的虚拟世界中,存在着国家利益、集体利益和个人利益,需要通过法律的方式平衡和协调它们之间的关系,维护信息化社会的正常秩序;存在着国家机密、企业秘密和个人隐私等需要保护的信息;几乎所有传统的犯罪形式都在信息社会中存在各种新的表现形式,需要法律适度地惩治犯罪活动,保护合法权益人的利益,维护网络社会的稳定,保障网络社会持续、有序的发展。

面对信息化社会的新形势,网络安全监察部门及时研究新问题、新情况,借鉴信息化发达国家的教训和先进经验,采取相关的对策,除了技术和管理的保障意外,不断出台各种适宜的法律、法规和部门规章,通过法律从国家层面和宏观层面对信息化社会生活进行有效调控,对信息化社会的各种社会资源进行第一次分配,对信息化社会中人的行为进行规范,有力地保障了信息化社会的稳定。通过这些年不断的努力,已经建立起了一套适合我国国情的、较完备善的法律法规和部门规章。

1982年12月第五届全国人大第五次会议通过了《中华人民共和国宪法》,相关条款规定了维护国家安全,维护社会秩序;制裁危害社会的违法犯罪活动;保护通信自由和通信秘密;保守国家秘密;保护公民、法人和其他组织的合法权益等与信息安全相关的内容。《中华人民共和国宪法》是我国制订相关信息安全法律法规的根本和依据。

1994年,经过公共信息网络安全局近十年对信息化社会的深入研究和酝酿,促成了我国第一部关于信息化社会的法规《中华人民共和国计算机信息系统安全保护条例》(中华人民共和国国务院147号令)的出台。该条例明确规定我国的信息系统的建设和管理应该实行安全保护,特别是涉及国计民生的国家事务、经济建设、国防建设和尖端科学技术等重要领域的计算机信息系统的安全保护。具体的保护制度包括:安全等级保护制度、国际联网备案制度、计算机媒体出入境制度、安全枪支报告制度、计算机病毒和有害信息专管制度以及信息安全专用产品销售许可制度。该条例还明确了公安机关对危害计算机信息系统安全的违法犯罪安全进行依法查处。该条例针对我国当时和未来可能存在的信息安全隐患和对社会带来的危害,较全面地规范了信息化社会中各方的利益和责任,明确了公安机关对信息化社会的安全保监督、检查、指导以及对计算机犯罪实施打击的职责。该条例对我国的信息化建设和信息化社会的安全智力方面具有划时代的历史意义。

1997年3月14日第八届全国人大第五次会议修订了《中华人民共和国刑法》,增补的第



285、286 和 287 条分别规定了非法侵入计算机信息系统罪、破坏计算机信息系统罪和利用计算机进行传统犯罪等条款。

1995 年 2 月 28 日第八届全国人民代表大会常务委员会第十二次会议通过了《中华人民共和国人民警察法》，将人民警察监督管理计算机信息系统安全保护的责任明确写入了人民警察法中。

针对国际联网在我国的迅速发展及其对社会的影响，公共信息网络安全监察局及时研究了相关的对策，促成发布了《中华人民共和国计算机信息网络国际联网管理暂行规定》（1996 年）、《计算机信息网络国际联网安全保护管理办法》（1997 年，国务院令 195 号）、《互联网信息服务管理办法》（2000 年，公安部）、《互联网上网服务营业场所管理办法》（2001 年，信息产业部、公安部、文化部、国家工商行政管理总局）、《计算机信息网络国际联网安全保护管理办法》（1997 年，公安部）等一系列的行政法规和部门规章。这些行政法规和部门规章对国际联网上国际出入口信道提供单位、互联单位的主管部门或者主管单位、互联单位、接入单位及使用计算机信息网络国际联网的个人、法人和其他组织的行为进行了规范，对从事信息服务和上网服务单位的责任和义务进行了规范，明确了互联网上的五类危害活动：煽动抗拒、破坏宪法和法律、行政法规实施的；煽动颠覆国家政权，推翻社会主义制度的；煽动分裂国家、破坏国家统一的；煽动民族仇恨、民族歧视，破坏民族团结的；捏造或者歪曲事实，散布谣言，扰乱社会秩序的；宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖，教唆犯罪的；公然侮辱他人或者捏造事实诽谤他人的；损害国家机关信誉的；其他违反宪法和法律、行政法规的等九类威胁信息。具体规定了未经允许，进入计算机信息网络或者使用计算机信息网络资源的；未经允许，对计算机信息网络功能进行删除、修改或者增加的；未经允许，对计算机信息网络中存储、处理或者传播的数据和应用程序进行删除、修改或者增加的；故意制作、传播计算机病毒等破坏性程序的；其他危害计算机信息安全的等。这些法规和部门规章对促进国家互联网的健康发展、净化网络空间起到了积极的促进作用。

公共信息网络安全监察局针对我国信息安全产品技术水平参差不齐、国外信息安全产品可能存在安全隐患、信息安全市场管理无序等局面，1997 年 12 月，促成发布了《计算机信息系统安全专用产品检测和销售许可管理办法》（1997 年，公安部），通过对信息安全专用产品的检测要求，促进了我国信息安全技术的规范化发展；通过对信息安全专用产品的市场准入制度和销售许可，规范了信息安全产品的市场，提高了国家对信息安全行业的监管力度和整体管理水平。

随着软件产品在信息化中的地位越来越重要，为了保护软件这类特殊信息产品的知识产权，调节软件在开发、传播和使用中各方的权益，公共信息网络安全监察局促成发布了《计算机软件保护条例》（2001 年，公安部）。该条例界定了软件产品，规定了软件产品的相关法律责任，规范了软件制作和使用的合法行为。

计算机病毒从最初的游戏演变为单机病毒、网络病毒，从最初的破坏计算机软硬件资源演变为破坏网络资源、盗窃信息系统的敏感信息，截至目前为止，计算机病毒是对信息化社会构成的最大威胁之一。面对日益猖獗的计算机病毒肆虐，公共信息网络安全监察局研究并促成发布了《计算机病毒防治管理办法》（2000 年，公安部），进一步细化了国务院 147 号令中关于计算机病毒的相关条款，界定了计算机病毒；明确了公安机关主管全国计算机病毒防治的管理工作；严令杜绝任何单位和个人不得制作、传播计算机病毒，及其相关的法律责任；规定了相关责任单位关于计算机报警、检测、治理的权利和义务。



除了上述一些法律、法规和部门规章以外,公共信息网络安全监察局还促成公安部与其他部委联合发布了一系列部门规章,如:《金融机构计算机信息系统安全保护工作暂行规定》等;制定了一系列关于国家法律法规具体操作的实施意见和规范性文件,如:《贯彻落实国务院办公厅关于进一步加强互联网上网服务营业场所管理通知的意见》、《关于对“中华人民共和国计算机信息系统安全保护条例”中涉及的“有害数据”问题的批复》等。

“法网恢恢,疏而不漏”。通过上述的公安机关信息网络安全监察部门直接和参与的立法活动,从法律角度确立了信息网络安全监察部门的法律地位和职责,填补了我国关于信息化社会法律法规的一些空白,有利地震摄了信息化社会的各种犯罪活动,规范了信息化社会的行为。尽管这些法律法规还不够完善和细致,但这些法律法规与国家的其他法律法规一起勾勒出了我国对信息化社会治理的基本框架,有力地保障了我国现阶段信息化社会的秩序和可持续发展,维护了国家安全和信息化社会的稳定和治理,为进一步的发展打下了坚实的基础。

## 2. 加强网络空间的治理,牢牢掌控制网络权

继广播、电视之后,网络被称为第三大媒体,成为了人们信息发布和获取的主要平台。而且,与广播和电视相比较,鉴于计算机网络的交互性,任何人可以在任何地点、任何时间访问网络上任何国家和地区的信息,信息获取更加方便、灵活,计算机网络已成为当今世界最主要的信息发布和获取渠道。各国政府将虚拟化社会的制网络权、制信息权均放在国家安全、社会安全的战略高度加以重视,纷纷制定了相关的管理办法。网络舆情的管理是我国公安机关管理信息化社会面临的新问题,对公安工作提出了新的挑战。

公共信息网络安全监察部门按照党中央、国务院、人民的要求,肩负起历史的责任,积极开展相关工作,掌控网络基础设施的基本情况和网上舆情,开展网络情报收集和研判,加强网上有害信息的治理能力和网上突发事件的处置能力,净化了网络空间,有效保障了我国信息化虚拟社会的健康有序、可持续发展,有力地促进了虚拟社会的稳定,乃至整个社会的稳定和国家安全。

### (1) 加强互联网单位的监督管理能力

国际互联网是最大、最广泛使用的公共信息网络,对互联网单位的监督管理是治理网络空间的基础性工作。中国的互联网从20世纪80年代开始,90年代开始大规模建设,进入21世纪后得到飞速发展,截至2007年年底,中国已有2.1亿国际互联网用户,网民数量仅次于美国的2.15亿人,位于世界第二;基础资源方面,中国的IP地址数达到1.35亿个,中国域名总数是1193万个,中国网站数量已有150万,中国网页总数已经有84.7亿个<sup>①</sup>,中国互联网国际出入口带宽数达到368,927Mbps;互联网服务提供商(Internet Service Proxy, ISP)单位、互联网内容服务提供商(Information Service Proxy, ICP)的数量急剧增加;中国家庭上网计算机数为7800万台;网吧数量超过10万2千个<sup>②</sup>,有7119万人选择在网吧上网;博客用户3000多万个。对于中国如此巨大互联网单位、网民和网页信息量,互联网监督管理任务之艰巨可想而知。加强互联网空间的治理,规范人们在网络空间的行为,是国家赋予公共信息网络安全监察部门的事权,是社会和人们对公共信息网络安全监察部门的企盼,是公共信息网络安全监察部门义不容辞的责任。

① 数据来源:第21次中国互联网络发展状况统计报告, <http://www.cnnic.org.cn>。

② 数据来源:公共信息网络安全监察业务管理指挥教程。



面对复杂多变的互联网环境和巨大的互联网安全管理工作,公共信息网络安全监察局借鉴公安机关对现实社会的“群治群防、综合治理”管理经验,制定了“谁主管、谁负责,谁经营、谁负责,谁运营、谁负责”的国际互联网监督管理指导方针,充分调度网络运营商、信息服务商、联网单位和广大网民的积极性和主动性,构建全社会共同参与、群治群防的公共信息网络安全监督管理工作新局面,实现了对信息化网络空间的综合治理。

首先,依据《中华人民共和国计算机信息系统安全保护条例》(国务院第147号令)、《中华人民共和国计算机信息网络国际联网管理暂行规定》(国务院第195号令)、《计算机信息网络国际联网安全保护管理办法》(公安部第33号令),公安部相继颁布了《关于规范“网吧”经营行为坚强安全管理的通知》、《贯彻落实国务院办公厅关于进一步加强互联网上网服务营业场所管理通知的意见》、《公安部关于加强互联网上网服务营业场所安全管理工作的通知》、《公安部关于执行“计算机信息网络国际联网安全保护管理办法”中有关问题的通知》、《公安部关于加强政府宣传网站安全保护管理工作的通知》、《公安部关于严厉打击利用计算机技术制作、贩卖、传播淫秽物品违法犯罪活动的通知》等一系列部门规章,加强对互联网接入服务单位即(ISP)、互联网数据中心(IDC)、互联网信息服务单位即(ICP,包括网站、聊天室、论坛、搜索引擎、电子邮件、互联网娱乐平台、点对点服务、短信息、电子商务、网上音视频、声讯信息等服务单位)、互联网单位和和个人、互联网上网服务营业场所(包括网吧、电脑休闲室等)的备案管理,备案率逐年升高,从而对我国的互联网上各种单位及其基本情况做到“底数清、情况明”;督促这些单位依据相关规定制定本部门的安全管理制度,对重点单位、重点部门和安全管理薄弱环节实施集中整治。例如,2002年,文化部、公安部、信息产业部、国家工商总局联合发布了《关于开展“网吧”等互联网上网服务营业场所专项治理的通知》等,这些措施有力地提高了互联网单位的安全管理能力。目前,全国互联网单位绝大部分落实了安全组织和安全责任制;指导这些单位采用相关的安全技术措施和对各种信息资料的安全管理,指导这些单位制定突发安全事件和事故的应急处置方案,要求信息服务单位严格实施用户登记制度和内容审查制度。互联网备案、互联网单位安全制度、信息服务单位的用户登记和内容审查制度从源头上加强了互联网的安全,是公共网络安全监察机关全面开展互联网安全管理的基础性工作。

其次,按照法律和相关规定赋予公共信息网络安全监察机关的事权,全面展开对互联网单位的监督检查工作。通过及时检查互联网备案单位定期报送的数据,掌握本地ISP、IDC、ICP等联网单位的运行情况和网络拓扑变化情况;通过定期日常检查、不定期抽查和专项检查等方式到互联网单位实施检查,以及加强联系、便民服务、组织宣传教育和培训、技术监管和整改查处等多种方式,加强对互联网单位安全管理的监督,将隐患消除在萌芽状态,减少安全损失。公共网络安全监察机关实行“7×24”小时值班制度,及时处置各类信息网络上的各种突发事件和事故。同时,加大单位安全事件的执法和处罚力度,确保互联网单位按照规定加强和维护其信息系统的安全。

## (2) 开展网上舆情监督管理和情报工作

网上舆情监督管理工作坚持把维护国家安全和社会稳定放在首位,为国家的经济建设和改革开放营造一个良好的虚拟社会环境。当前,互联网日益成为西方敌对势力对我进行反动宣传的“主渠道”,颠覆破坏的“主阵地”,渗透、颠覆的“主战场”,他们利用互联网宣传西方意识形态、价值观念,妄图用看不见的硝烟,与我争夺群众;密切关注境内的热点问题和突发事件,插手民间的“维权”活动,妄图使之发展成“中国民主进程的突破口”,他们直接

进行网络攻击、网上窃密、网上策反等活动；境内外的“法轮功”、“三股势力”、“民运”在网络上活动猖獗；网络上各种流言蜚语、造谣欺骗泛滥、充斥，各种黄色等有害信息良莠不齐、泥沙俱下，使得在网络化的虚拟社会中防范“西化”、“分化”和各种有害信息的任务更加艰巨。同时，随着我国改革开放进程的加快，经济体制、社会结构、利益格局的深刻变化，使得人们思想活动的独立性、选择性、多变性和差异性明显增强，互联网已经成为各种社会群体表达利益诉求的重要、主要平台，各种社会矛盾和热点问题通过互联网的放大、扩散，网上不和谐因素极易成为影响社会和谐和稳定的导火索，及时发现问题、疏导网络舆情、化解矛盾也是公共信息网络安全监察部门面临的重大课题。

公共信息网络安全监察部门面对新形势、新任务，锐意进取，积极开拓，加强网络舆情的监督检查工作，逐步从不适应走向有所适应，从完全被动扭转到有一定的主动权，探索了许多新做法，取得了许多新经验，开创了公共信息网络舆情监控管理工作的新局面。

首先，积极推动制定了《计算机信息网络国际联网安全保护管理办法》、《互联网信息服务管理办法》、《中华人民共和国计算机信息网络国际联网管理暂行规定》、《互联网新闻信息服务管理规定》等一系列法律法规和部门规章，规范了网络上人们的行为，明确了各方参与人的责任和义务，同时，也使得公共信息网络安全监察民警执法活动有法可依、有章可循。

其次，在公共信息网络安全监察部门建立了专门的网络安全监控组织机构和信息安全通报中心，对网上舆情的日常监督管理的提供组织保障，对重大信息安全事件和国内外信息安全技术发展的重大动态进行编报，直接对国务院信息办负责，为高层的决策提供依据。

再次，公共信息网络安全监察民警根据上述法律、法规和部门规章，积极及时收集敌情、社情和民情信息，包括：反动言论、维护社会秩序、淫秽色情、暴力赌博等违法信息，重大政治活动、重要事件等社会热点和网上动态信息，计算机病毒、黑客攻击和其他信息安全事件以及最新信息安全技术发展情况等信息，以及各种专题、专项信息等，对这些信息进行分类汇总、统计分析和情报研判，为进一步的网上情报工作提供丰富的情报源，为及时治理网上有害信息提供基础保障，增强网上有害信息的治理能力。

然后，积极探索各种形式的网上斗争模式和监控措施，推行“双责任制”（运营单位和监督管理单位共同负责），开展“两快两多”（对网上有害信息发现快、处置快，对网上非法犯罪受理举报多、立案侦查多）的活动；在互联网上推行“虚拟警察”，对虚拟社会实施 24 小时上网巡查；建立“虚拟社区”，实行属地化管理，对本地网站、网页定期巡查，加大对重点对象的监控力度，在突发事件和特殊、敏感时期实行重点目标的实时监控；建立网上舆情情报的分析研判机制，规范情报分析流程；建立有害信息的发现和处置流程，对有害信息采取删除、过滤、临时断网、封堵、通报移交和上报等措施，有力地遏制了网上有害信息的传播和蔓延，净化了网络空间。

面对互联网上非法从事组党结社、政治渗透、反动宣传、煽动民族仇恨、分裂祖国的活动，互联网上各种有害信息泛滥和网上各种影响社会稳定的热点问题，公共信息网络安全监察部门开展网上舆情监督管理和情报工作以来，成效显著。仅 1998 年，各级公共信息网络安全监察机关重点监控境外杂志、报刊、论坛、宗教网站等站点 300 余个，监控信息 1.5 万条，不少信息受到上级领导和有关部门的高度重视。2007 年，发现可能影响社会稳定的网上情报 200 多起，通过及时上报、及时处置、及时疏导等措施，“大事化小、小事化了”，避免了重大事故的发生，化解了社会危机和社会矛盾；通过及时删除、及时封堵、上报和处理，净化了网络空间，维护了虚拟社会的正常秩序。总之，公共信息网络安全部门通过对互联网上信