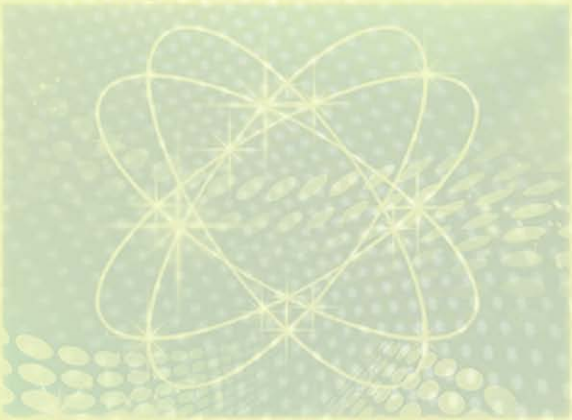
基层公安机关网络安全保卫理论与实务



内 容 简 介

《基层公安机关网络安全保卫理论与实务》是一本由四川警察学院教学一线教师王刚副教授在基层公安机关网安大队挂职锻炼期间参加网络安全保卫执法工作后撰写的警务实践方面书籍。

该书内容包括县（区）级公安机关网安工作的总体要求和职责、计算机网络在涉网案件中扮演的角色、上网服务场所管理理论与实务、网络侦查基础知识、主侦案件侦查步骤和线索发现、配侦案件侦查思路和关键环节、网络轨迹发现、网警现场勘察、涉网案件线索查找和拓展、线索落地、电子数据检验和鉴定、侦查羁押种类和期限、防范网络非法侵害措施、网络舆情管理理论与实务等。

本书既适合公安政法院校网络安全与执法、侦查等公安类专业的学生使用，又适合基层公安机关的民警（尤其是从事网络安全保卫工作的网络警察或派出所民警）使用，也适合从事国内安全保卫、国家安全局侦查的人员使用。

前　言

王刚副教授所著的《基层公安机关网络安全保卫理论与实务》一书，得到了四川警察学院挂职锻炼科研项目“基层公安机关网监工作的现状、存在问题和解决对策”（SCJYXJ005）和四川警察学院2013年度专著经费资助（川警院发〔2013〕85）。该书是作者于2011年6月至2012年6月期间在成都市公安局锦江区分局网安大队挂职锻炼期间取得的工作成果之一，该成果的取得与四川省公安厅和四川警察学院党委的正确领导、成都市公安局锦江区分局领导的关心帮助以及办案民警的业务指导密不可分。经过作者近一年的理论提炼和实践总结，完成了该书的撰写和完善等一系列工作。

区县（市）公安局网络安全保卫大队（简称网安大队）是基层公安机关的重要职能部门，是维护社会稳定、打击网络犯罪的一支重要力量。虽然各地网安大队成立的时间不长，但其发挥的作用却与日俱增、不可低估。随着计算机技术和网络技术的快速发展，网络已经逐渐深入到人们的工作生活之中，出现了规模庞大的网络用户群，据中国互联网络信息中心（CNNIC）的调查数据显示，截至2013年6月底，中国网民规模达到5.91亿，互联网普及率为44.1%，网民数量占全世界第一。网络是一把双刃剑，网络的快捷性和高科技性，在给人们工作生活带来便利的同时，也给违法犯罪分子提供了隐蔽的作案平台。

近年来，网络诈骗、网络色情、网络赌博、网络盗窃等案件频频发生，因跨地区作案、网络实名制的滞后、有些单位在经营过程

中的不规范以及网络无国界等问题，给公安机关打击网络犯罪增加了很大的工作难度。另外，互联网上网服务非经营场所（如宾馆、咖啡馆等）的在线审计管理、网络舆情监测与管理、重要信息系统等级保护，给网安大队的行政管理工作带来了新的挑战。

本书以作者在基层公安机关警务实战和基层调研为蓝本，以区县（市）公安局网安大队行政职能为切入点，以网络犯罪侦查、上网服务场所管理、网络舆情管理为研究视角，以网络犯罪侦查理论与操作实务为研究重点，以基层网安民警实战建议为补充，详细论述了基层公安机关网络安全保卫理论，并结合八类实际案例，给出了相应的办案手续、法律依据和法律文书等办案实务。本书在2013年1月1日之前开具的部分法律文书，以旧版的刑事诉讼法条文为准；其他则以2012年3月14日第十一届全国人民代表大会第五次会议审议通过的《关于修改〈中华人民共和国刑事诉讼法〉的决定》修正后的新内容为准，即新版的刑事诉讼法从2013年1月1日起正式实施之后，法律文书中涉及刑事诉讼法内容均以修改后的为准，所以本书其他地方出现的刑事诉讼法内容均是指新修订的内容。

理论与实践相结合是本书的显著特点。该书仅在公安系统内部发行，可供中央司法体制改革招录的各专业学生和网络安全与执法、侦查、治安等公安类专业学生及基层公安机关网安民警、派出所民警、国安侦查员使用，也可用于公安机关的其他警种民警拓展知识。

在编写本书过程中，作者除了自己参加网络安全保卫执法工作实践体会和总结之外，还学习并引入了《中华人民共和国刑事诉讼法》《中华人民共和国刑法》《高检规则》《高法解释》《最高人民法院、最高人民检察院、公安部、国家安全部、司法部、全国人大常委会法制工作委员会关于实施刑事诉讼法若干问题的规定》（简称《六机关规定》）《公安机关办理刑事案件程序规定（2012）》《公安机关电子数据鉴定规则》《中华人民共和国计算机信息系统安全

保护条例》《信息安全等级保护管理办法》等相关法律法规文献，引用了成都市公安局、眉山市公安局等公安机关相关案例资料。

由于作者水平有限，加之时间仓促，本书内容如有不当之处，敬请读者或同行批评斧正。

王　刚

2013 年 12 月

目　　录

第一章　网络安全保卫绪论

第一节　概　述

随着近年来计算机网络违法犯罪的频发，作为中国最年轻的警种——网络警察（以下简称“网警”）在公安机关办理涉网案件中的作用越来越突出，以成都市锦江区为例，据不完全统计，目前有20%的案件与网络有关，并需要网络警察介入侦查。

区县（市）公安局网络警察部门在不同地方有不同的称呼，如公共信息网络安全监察大队（简称网监大队）、网络警察大队（简称网警大队）和网络安全保卫大队（简称网安大队），本书对此不作区分。不管什么样的称呼，其职责一样，都是作为网络违法犯罪侦查、信息安全管理、网络舆情管控的主体，它们是公安机关的重要职能部门，在信息网络社会中发挥着重要作用。

当今，随着网络技术和信息技术不断进步，各行各业都建立起了自己的网络应用系统平台，实现了无纸化管理和数据科学管理，提高了工作效率。但一些违法犯罪分子也利用网络平台的特点实施了多类型和跨区域的网络违法犯罪，如网络合同诈骗案、网络赌博案、网络征婚诈骗案、网络招嫖案、网络吸毒案、网络传销案、网上贩卖枪支弹药案、网上传播淫秽物品牟利案、网上贩卖假币案、网上贩卖个人身份信息案和网上购买飞机票或火车票诈骗案。同

时，也因不法分子寄生于互联网虚拟平台而衍生出很多新型犯罪，如利用网络故意传播虚假恐怖信息案、利用网络付费平台套取银行卡资金案、利用黑客技术盗窃网上银行资金案、入侵外贸企业电子邮箱并篡改账号套取国外客户汇款案、利用网络炒黄金诈骗案等。

也必须看到，在派出所、刑侦和经侦等部门立案的很多案件，都需要网监部门进行侦查。因此，多警联动、网上网下、合成作战，共同打击网络违法犯罪，是信息网络时代公安机关办案的一大特点。

第二节　县（区）级公安机关网监工作的总体要求

以科学发展观为指导，认真践行人民警察核心价值观，贯彻落实省厅和市局对网监工作的总体要求，指导并组织实施公共信息网络的安全监察、安全保卫工作，保持对网络违法犯罪活动严打高压态势，为打击网络违法犯罪活动提供电子取证技术支持和系列侦查措施。

第三节　县（区）级公安机关网监大队职责

（1）监督、检查、指导本辖区内互联网上网服务场所和企业重要信息系统等级保护等信息安全管理工作，以及对 ISP、ICP 的行政监察工作。

（2）组织、负责辖区破坏计算机信息系统等互联网违法犯罪案件的受案、立案、主侦工作。

（3）协助经侦、刑侦、派出所等办案部门开展相关案件的配侦工作以及开展有些涉网案件的网络侦查工作。

（4）对涉案电脑进行数字证据提取和在线取证，并保证数字

证据的合法性。

（5）负责对辖区网吧、电脑休闲室等互联网上网服务经营场所的计算机进行上网安全审计、换证等工作，检查网络安全管理及技术措施的落实情况，对违法违规的上网服务场所依法进行处罚。

（6）负责检查辖区旅馆、酒店等互联网上网服务非经营场所的上网审计系统、上网地址转换接点和上网出口处是否落实上网审计联网报警措施。

（7）负责辖区计算机信息网络国际联网的互联单位、接入单位和用户的备案工作，包括对跨地区互联网接入服务企业的内外网络地址转换管理、网络运行安全防范、基础数据定期报送、接入网站违法信息屏蔽过滤、违法犯罪线索配合调查和突发事件应急处置等信息安全管理制度措施制订落实情况。

（8）加强互联网的网络巡查工作，收集涉及本地区的网络舆情信息，并及时上报到系统；对影响辖区稳定的热点网络舆情必须在第一时间向局领导汇报。

（9）承办上级机关交办和异地公安机关协办的其他事项。

上述九项职责只是作者结合基层挂职实践得出的观点。四川省公安厅对县（区）级公安机关网安部门承担的职责有明确的规定，因涉密，请民警参见“川公发〔2011〕24号”文件。

第四节　计算机网络在涉网案件中扮演的角色

计算机网络在各类案件中扮演的角色通常有三大类，各类案件中网监部门在案件侦查中发挥的作用略有差别，具体如下。

一、计算机网络作为犯罪嫌疑人用于从事社会、经济、文化娱乐等活动的平台

通常表现为犯罪嫌疑人使用网络进行聊天、购物、登录论坛、

打游戏等，其显著特点是犯罪行为自身与计算机网络并无直接关系，如马加爵案件。

网监部门发挥的主要作用：依靠专用信息系统，分析相关电子数据和使用技术手段，排查犯罪嫌疑人涉网线索，并落地查证。

二、计算机网络作为违法犯罪过程中用于实施宣传、勾连等非主要犯罪事实的平台

通常表现为在网络上建立网站销售假药、枪支、窃听器材等禁售产品或传销产品（如××公司生产的营养餐），其制造、销售假药、枪支、窃听器材的犯罪行为主要发生在现实生活中，网络只是其宣传平台和联络平台。

网监部门发挥的主要作用：发现涉网犯罪线索，梳理犯罪团伙的组织结构和网络关系；通过网侦手段获取嫌疑人相关网上信息，为案件侦查确定方向；通过网络定位，确定犯罪嫌疑人上网地点，以配合其他警种抓获犯罪嫌疑人。通过电子数据分析、提取、固定等技术措施，部分认定嫌疑人犯罪事实，成为证据链中的一环。

案例：本书第三章第九节的“8·27”网络贩卖枪支案。

三、计算机网络作为违法犯罪过程中主要犯罪事实的平台

(1) 利用网络非法提供、发送、传播、获取电子信息。通常表现为利用网络传播淫秽色情电子信息、侵权电子信息、诽谤信息、谣言等，利用网络盗窃电子信息（如网络银行账号、虚拟货币、虚拟财产、涉密电子文档等）。通过网络传输涉案电子信息是犯罪的主要行为，该行为自身是犯罪的主要构成。

案例：本书第三章第九节的利用互联网传播淫秽物品案件。

(2) 利用网络非法提供、获取网络服务。通常表现为利用网络提供淫秽色情视频表演服务、赌博投注服务、游戏私服服务、骗取手机注册费用服务，利用网络盗窃网络电话服务、网络空间服

务。这种犯罪行为的实施主要依赖计算机网络，此类案件是传统案件在计算机网络环境下的异化，是新技术的引入给传统案件带来全新的表现方式，其案件的特点、侦察方式、取证方式与传统的同类案件完全不同。

网监部门发挥的作用：从线索的发现、拓展、落地定位犯罪嫌疑人，到发现和提取电子物证等各个环节的主要工作由网监部门承担。

案例：本书第三章第四节的网络赌球案件。

(3) 仅把网络作为传输破坏工具的通信链路。此类案件与计算机网络相互依存，离开计算机网络此类犯罪就不会发生，如入侵计算机信息系统、破坏计算机信息系统功能和数据、传播病毒等破坏性程序。

网监部门发挥的作用：此类案件的侦查、打击、移送起诉等各环节完全由网监部门承担。

案例：本书第三章第四节的非法侵入计算机信息系统案件。

第五节　派出所配合网监大队需要完成的工作

派出所（警署）是公安机关的派出机构，其在打击犯罪、解决辖区治安纠纷和维护社会稳定等方面发挥了不可估量的作用。就目前而言，县（区）级公安机关网监大队与其他业务大队相比，民警数量相对较少，因此，必须充分利用辖区派出所的力量，来配合网监大队开展工作。以 2011 年初成都市公安局为例，成都市锦江区公安分局网监大队民警人数在全市五个主城区公安机关网监大队中是最多的，但也仅有 10 位民警。与该分局的经侦大队、刑侦大队、治安大队、法制科等 16 个业务科室相比，网监大队民警人数明显偏少。锦江区有网吧 85 家、梳理和排查网络社区 500 余个，辖区虚拟社会较为发达。为了加强网络虚拟空间有效管理、促进上

网服务营业场所规范建设，促进网络社区和谐发展，辖区派出所（警署）需要配合网监大队履行下列职责：

（1）负责对本辖区内互联网上网服务营业场所使用法定有效证件实名上网情况的日常检查工作和辖区之间的交叉突击检查工作（在网监大队或上级有关部门指导下），建立健全互联网上网服务营业场所基础管理台账，摸清辖区内网站和人员详细信息。

①摸清网站的信息。主要包括域名、IP 地址、名称、网站类型、网站主要功能、网站属地、开办单位（创建者）、单位地址、单位联系电话、ISP、网监部门的备案号等。

②摸清人员的信息。在网络虚拟空间，主要分为三类，具体如下：

网站管理员。主要摸清其管理的网站名称、域名、真实姓名、身份证号、联系方式、工作单位、现居住地、网络虚拟身份标识等。

论坛版主。主要摸清论坛版主管理的论坛名称、虚拟账号、真实姓名、身份证号、联系方式、工作单位、现居住地等。

QQ 群群主。主要摸清群主所在的 QQ 群号、个人 QQ 号、真实姓名、身份证号、联系方式、工作单位、现居住地等信息。

（2）负责本辖区内互联网上网服务营业场所消防安全检查与保护工作。

（3）负责本辖区内互联网舆情信息的收集和上报工作。

（4）对违规违法的互联网上网服务营业场所进行证据固定，制作询问笔录。

（5）与工商行政管理部门、文化部门、网监大队一起，加强辖区黑网吧的管理工作。

（6）履行法律、法规所赋予的其他职能和网监大队、网监处交给的临时任务。

第六节　本书相关术语

在网监大队侦查办案中，往往涉及一些新的概念名词，需要读者对这些名词有个大致的了解。本书可能涉及下列相关术语。

一、网络社区

网络社区是指现实社会中的单位、企业、居民小区及公民个人在一定地域内开办的为网民提供上网服务的场所（如网吧、宾馆、饭店等）和现实社会中的单位、企业、居民小区及公民个人在互联网上开设的网站、论坛、QQ 群、博客、微博等虚拟空间。[1]

二、虚拟主机

虚拟主机，简称“虚拟机”，是运行在电脑中的一组软件集合。虚拟主机服务，往往运行在装有 Windows Server 操作系统或 Linux 操作系统的服务器中。一台服务器可以运行多个虚拟主机服务，系统根据用户账户、密码和权限对用户进行隔离和实施资源限制。

三、托管主机

托管主机是一台独立的包含操作系统环境、拥有独立 IP 并联网的服务器。

四、VPS 主机

VPS（Virtual Private Server），中文含义是虚拟专用服务器。VPS 主机继承虚拟主机和托管主机的优点，用户不仅可以享受到与托管主机相同的高品质服务，还可尽享虚拟化技术带来的先进管理体验。每个 VPS 主机都拥有自己独立的资源配置和独立的 IP 地

址。每个 VPS 都是一个独立的环境，可以实现安全的隔离，确保用户资源的私密性。

五、博客

博客源于“Weblog”的缩写，中文意思是网络日志。网络上的博客则是指写网络日志的人。

六、微博

微博，即微博客（MicroBlog）的简称，是一个基于用户关系的信息分享、传播以及获取平台，用户可以通过 WEB、WAP 等各种客户端组建个人社区，以 140 字左右的文字更新信息，并实现即时分享。[2]

七、微信

微信是腾讯公司于 2011 年初推出的一款通过网络快速发送语音短信、视频、图片和文字，支持多人群聊的智能手机聊天软件。微信不存在距离的限制，即使是在国外的好友，可以使用微信对讲。微信“扫一扫”就是微信里面的一个工具，对着二维码一扫就可以拍照并分析二维码信息；微信“摇一摇”，可以随机发现附近同时在摇的信友。

八、ISP、ICP 和 IDC

本书中的 ISP（Internet Service Provider），是指互联网接入服务提供商。常见的 ISP 有三大电信运营商（中国电信、中国移动、中国联通）、四川艾普网络公司、长城宽带网络服务有限公司等。

本书中的 ICP（Internet Content Provider），是指互联网信息服务商，即向广大用户综合提供互联网信息业务和增值业务的公司，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，例如腾讯公司、新浪公司、百度公司、天涯论坛、麻辣社区等。

本书中的 IDC（Internet Data Center），是指互联网数据中心，其主要包括主机托管、主机租赁、虚拟空间租用和域名解析等服务。

对于 ISP、ICP 和 IDC，必须纳入公安机关网安部门监管。

九、网络舆情

从广义上讲，网络舆情是在互联网环境下，网民对各种社会现象和问题所表达的信念、态度和情绪的总称。从狭义上来看，它是指在互联网中发布的有可能影响国家安全、社会稳定和涉及民生的苗头性、预警性的信息。

十、“收信息”

网监部门所称的“收信息”，是指利用搜索引擎工具按关键词收集网络上相关的互联网舆情信息[3]。搜索引擎工具通常有两类：一是 Internet 上提供的免费通用引擎，例如百度、Google、新浪等；二是技术侦察部门专用的搜索引擎工具。

十一、虚拟身份信息

虚拟身份信息是指上网人员在互联网上留下的网络账号和网络编号等信息，例如 QQ 号码、MSN、BBS 账号、E-mail、微信、微博、游戏账号等。

十二、Cookie 和 Flash Cookie

Cookie 是一种方便用户上网的网络身份自动识别程序。该程序自动记载用户浏览网站时的浏览记录、IP 地址、网卡号、用户名、密码等信息，并存放到用户电脑一个叫 Cookie 的数据包中，当用户再次登录该网站时，网站便可以利用 Cookie 文件自动识别用户。

有些网站利用 Cookie 可以获取网络用户 Cookie ID、所在地域、兴趣爱好、年龄、月家庭收入甚至 IP 地址等个人信息。

Flash Cookie 是第三方机构加在网页广告上的代码程序，利用 Flash Cookie 同样可以获取用户信息，但是一般用户很难阻止 Flash Cookie 窃取个人信息。

十三、即时通信软件

即时通信软件包括 QQ、WebQQ、YY、MSN、Yahoo Messenger、UC、E 话通、Gtalk、Skype、ICQ、POPO、阿里旺旺、微信、飞信、9158 多人视频、阿里通、百度 Hi、QT 语音等工具软件，用户将这些软件安装在联网的计算机或智能手机上实现通信联系。常见的即时通信软件名和图标如图 1-1 所示。

图 1-1　常见的即时通信软件及对应图标

十四、网上交易平台

本书指的网上交易平台是能提供网上购物和支付服务的网站，例如淘宝网、当当网、拍拍网、赶集网、京东商城、Tmail 网等。

十五、IP 地址

IP 地址（IP Address）是联网计算机必需的逻辑地址。根据版本划分，IP 地址分为 IPv4 和 IPv6 地址。IPv4 地址是 32 位（bit）逻辑地址，转换成十进制后用四组数据表示，每组数据（其取值范围为 0~255）之间用英文句点“.”隔开，例如 220.166.97.98；IPv6 地址是 128 位（bit）逻辑地址，一般用 32 个十六进制数据表示，分为八组，每组数据取值范围为 0000~FFFF，组与组之间用