

计算机 辅助侦查

项振茂 / 著

JISUANJI
FUZHUZHENCHA



中国人民公安大学出版社

计算机辅助侦查

项振茂 著
翁 文 审

(政法机关 内部发行)
中国人民公安大学出版社

图书在版编目 (CIP) 数据

计算机辅助侦查 / 项振茂著. —北京: 中国人民公安大学出版社, 2008. 1
ISBN 978 - 7 - 81109 - 913 - 3

I. 计… II. 项… III. 刑事侦查—计算机应用 IV. D918.2 - 39

中国版本图书馆 CIP 数据核字 (2007) 第 193051 号

计算机辅助侦查

JISUANJI FUZHU ZHENCHA

项振茂 著

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
印 刷: 北京兴华昌盛印刷有限公司

版 次: 2008 年 1 月第 1 版
印 次: 2008 年 1 月第 1 次
印 张: 15
开 本: 787 毫米 × 1092 毫米 1/16
字 数: 329 千字

ISBN 978 - 7 - 81109 - 913 - 3/D · 860
定 价: 28.00 元 (政法机关 内部发行)

本社图书出现印装质量问题, 由发行部负责调换

联系电话: (010) 83903254

版权所有 侵权必究

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

www.phcpps.com.cn

www.porclub.com.cn



前 言

随着计算机技术的迅猛发展和互联网的快速普及,计算机网络已广泛渗透到人类社会的政治、经济、文化等领域。网络改变了世界,世界也离不开网络,人类社会对计算机网络的依赖已达到前所未有的程度,甚至在一定程度上可以说,没有计算机网络,人们已不知道如何工作、生活了。

众所周知,网络是一把双刃剑,在方便人们生活、工作的同时,负面影响也日益严重,尤其是网络犯罪。有人说,10年之后,几乎全部的犯罪都将有计算机参与其中;也有人称,网络上的犯罪活动,除了需要身体接触外的案件,现实生活中的犯罪,在网上全能找到。

现有的刑事侦查类教材,内容很少涉及网络犯罪。从2002年开始,作者试图编写有关网络安全与犯罪的书籍,终因写作跟不上技术和应用的变化而搁浅。2004年后,由于工作的调动,终于有时间可对原来的想法进行重新梳理,从而发现如何利用计算机网络为案件侦查服务,在目前公安教学中很少涉及,但基层公安迫切需要这种技术。为此,作者又花了两年多的时间,终于完成了本教材。

本书是浙江警察学院的特色教材,取名为《计算机辅助侦查》,作者主要出于以下两方面考虑:一是计算机网络与人类社会已密不可分,计算机网络已是人们最常用的工具,因此,其上必然会有对案件侦破有用的信息;二是在现实社会中的大多数案件,已在网络上出现,当然要侦破这些案件必然需要用计算机来辅助。

需要说明的是,在写作过程中,作者已充分考虑了教材的可读性和知识的完整性,对一些重要的知识点,书中以相关知识和相关链接等形式进行补充,以满足不同读者的阅读要求。

本书的出版受到学院领导和教务处的大力支持,同时在本书的撰写过程中,作者得到了靳惠云教授、吴曙文博士、张其前博士、罗宁教授级高级工程师、胡建高级工程师、杨磊和沈建新工程师以及董争鸣、李旭、汤天阿、陶永红、陈潮、于方觉、王亢、余凌云等老师的大力支持和帮助,作者在此表示衷心的感谢。

由于信息技术的日新月异,书中介绍的内容很难跟上技术和应用的发展,加之作者水平有限,在书中难免有错误与不妥之处,恳请读者批评指正。

作 者
2007年9月



目 录

第1章 导论	(1)
1.1 网络改变了世界	(1)
1.2 网民的现状	(2)
1.3 网络与犯罪	(4)
1.4 网络犯罪的特点	(8)
1.5 网络犯罪的对策	(10)
1.6 本书内容介绍	(11)
第2章 预备知识	(14)
2.1 硬盘的基础知识	(14)
2.1.1 硬盘的物理组成	(14)
2.1.2 硬盘的逻辑结构	(16)
2.1.3 硬盘的数据结构	(17)
2.1.4 文件系统类型	(18)
2.1.5 格式化与分区	(18)
2.2 数据存储原理	(19)
2.3 文件与文件夹	(20)
2.3.1 文件名	(20)
2.3.2 文件属性	(20)
2.4 计算机网络	(25)
2.4.1 计算机网络的组成	(25)
2.4.2 IP 地址	(25)
2.4.3 域名服务器	(27)
2.4.4 DDNS	(27)
2.4.5 网关	(28)
2.4.6 代理服务器	(29)
2.4.7 端口号	(30)
2.5 Internet 主要应用	(31)
2.5.1 电子商务	(31)
2.5.2 电子政务	(31)
2.5.3 主机托管与虚拟空间	(31)



2.5.4 BBS 与博客	(32)
2.5.5 电子邮件	(32)
2.5.6 即时通信	(33)
2.5.7 文件下载	(33)
2.6 黑客与病毒	(34)
2.7 网上信息查询	(35)
2.7.1 人员查找	(35)
2.7.2 公开信息查找	(35)
2.7.3 邮编、电话区号查询	(36)
2.7.4 手机号码属地	(36)
2.7.5 IP 地址属地查询	(36)
第3章 计算机调查	(39)
3.1 电子数据	(39)
3.1.1 电子数据的定义	(39)
3.1.2 电子数据的特点	(39)
3.2 计算机调查的原则	(41)
3.3 计算机调查前的准备	(42)
3.4 计算机调查方法	(43)
3.5 计算机调查的程序	(43)
3.5.1 个人计算机的调查	(43)
3.5.2 公共上网场所计算机的调查	(44)
3.5.3 服务器的调查	(44)
3.5.4 编写调查报告	(45)
3.5.5 证据的保存	(45)
3.6 应用举例	(46)
3.6.1 对一般案件的调查	(46)
3.6.2 对需要取证案件的调查	(48)
第4章 数据分析	(52)
4.1 数据分析的步骤	(52)
4.2 文件分析	(53)
4.2.1 搜索助理	(53)
4.2.2 Google 桌面	(54)
4.3 文件特征分析	(55)
4.4 创建文件目录结构图	(56)
4.5 文件唯一性比较	(59)
4.6 文件内容的比较	(60)
4.6.1 FC	(60)



4.6.2	Diff Doc	(62)
4.6.3	Beyond Compare	(67)
4.7	木马程序的检查	(69)
4.8	计算机开关机时间的检查	(69)
4.9	应用程序启动的时间分析	(71)
4.10	注册表分析	(71)
第5章	日志分析	(78)
5.1	日志分析典型案例	(78)
5.2	Windows 日志查看	(78)
5.2.1	日志类型	(78)
5.2.2	事件说明	(79)
5.2.3	事件解释	(80)
5.2.4	特殊事件的查看	(81)
5.3	IIS 日志	(85)
5.3.1	日志存放位置	(85)
5.3.2	日志字段解释	(86)
5.3.3	日志分析	(86)
5.4	NAT 日志	(93)
5.4.1	ISA Server 2004 介绍	(93)
5.4.2	日志查看	(93)
5.4.3	内部 IP 查询	(94)
5.4.4	查询访问某一网页的用户	(96)
5.5	ADSL 日志	(97)
5.6	电子商务日志	(98)
第6章	密码破解	(101)
6.1	密码破解的典型案件	(101)
6.2	常用密码破解方法介绍	(101)
6.2.1	猜测法	(101)
6.2.2	查找法	(103)
6.2.3	字典法	(103)
6.2.4	暴力法	(104)
6.2.5	技术法	(104)
6.2.6	Google 桌面法	(104)
6.3	CMOS 密码破解	(104)
6.4	Windows 登录密码破解	(105)
6.5	Office 文件密码破解	(107)
6.6	RAR 压缩文件密码破解	(109)



6.7	PDF 文件密码破解	(112)
6.8	Foxmail 邮箱账户访问密码破解	(113)
6.9	OutLook Express 标识密码破解	(114)
第7章	数据恢复	(117)
7.1	数据恢复典型案例	(117)
7.2	数据恢复的原理	(118)
7.3	删除文件的恢复	(119)
7.4	文件查找	(122)
7.5	磁盘被格式化后的数据恢复	(123)
7.6	计算机不能启动的数据恢复	(125)
7.7	IE 浏览器上网日志删除后的恢复	(130)
7.8	从损坏的分区中恢复文件	(131)
7.9	修复损坏的文件	(132)
7.10	网络恢复	(133)
7.11	数据恢复注意事项	(135)
第8章	电子邮件与即时通信	(136)
8.1	电子邮件	(136)
8.1.1	邮件格式	(136)
8.1.2	邮件保存位置	(137)
8.1.3	邮件阅读标志	(138)
8.1.4	联系人	(139)
8.1.5	邮件的复制	(141)
8.1.6	邮件来源的追踪	(141)
8.1.7	手机与邮件绑定	(145)
8.2	即时通信	(149)
8.2.1	即时通信的使用	(150)
8.2.2	查找特定用户是否在线	(150)
8.2.3	群	(151)
8.2.4	查看 QQ 聊天记录	(152)
8.2.5	IP 地址的获取	(153)
8.2.6	网络语言	(158)
第9章	IP 地址追踪	(161)
9.1	IP 地址分配	(161)
9.2	本机 IP 地址查询	(163)
9.3	本机的外网 IP 地址查询	(163)
9.4	由域名得到网站 IP 地址	(164)
9.5	IP 属地查询	(165)



9.6 通过域名查找拥有者	(168)
9.7 几个值得注意的问题	(170)
第10章 常用调查取证工具介绍	(171)
10.1 常用DOS命令	(171)
10.1.1 DIR	(171)
10.1.2 IPCONFIG	(171)
10.1.3 PING	(173)
10.1.4 NETSTAT	(175)
10.2 Sysinternals 系列工具	(177)
10.2.1 PsTools	(177)
10.2.2 PsInfo	(177)
10.2.3 Pslist	(179)
10.2.4 Psloglist	(180)
10.2.5 String	(181)
10.2.6 AutoRuns	(182)
10.3 数据克隆	(184)
10.4 文件完整性校验	(190)
10.4.1 FCIV	(190)
10.4.2 Md5summer	(192)
10.5 网站下载工具	(194)
10.6 屏幕录像	(199)
10.7 EnCase	(200)
10.7.1 创建新案件	(200)
10.7.2 浏览证据	(201)
10.7.3 添加证据文件	(203)
10.7.4 添加原始映像文件	(205)
10.7.5 证据文件的获取	(207)
10.7.6 恢复文件与文件夹	(208)
10.7.7 书签的制作	(210)
第11章 几类典型网络案件的侦查	(217)
11.1 网上传播淫秽物品	(217)
11.1.1 网上传播淫秽物品的典型案例	(217)
11.1.2 网上传播淫秽物品案件的特点	(218)
11.1.3 网上传播淫秽物品案件的侦查方法(略)	(219)
11.2 网络诈骗	(220)
11.2.1 网络诈骗的典型案例	(220)
11.2.2 网络诈骗案件的特点	(222)



11.2.3 网络诈骗案件的侦查方法 (略)	(222)
11.3 网上盗窃	(223)
11.3.1 网上盗窃的典型案列	(223)
11.3.2 网上盗窃案件的特点	(224)
11.3.3 网上盗窃案件的侦查方法 (略)	(224)
11.4 网上敲诈勒索	(225)
11.4.1 网上敲诈勒索的典型案列	(225)
11.4.2 网上敲诈勒索案件的特点	(226)
11.4.3 网上敲诈勒索案件的侦查方法 (略)	(226)
11.5 破坏计算机信息系统	(226)
11.5.1 破坏计算机信息系统的典型案列	(226)
11.5.2 破坏计算机信息系统案件的特点	(228)
11.5.3 破坏计算机信息系统案件的侦查方法 (略)	(228)
11.6 网上聊天引发的案件	(228)
11.6.1 网上聊天引发的典型案列	(228)
11.6.2 网上聊天引发的案件特点	(229)
11.6.3 网上聊天引发案件的侦查方法 (略)	(229)



第1章 导论

▲ 1.1 网络改变了世界

随着计算机技术的迅猛发展和互联网的快速普及,互联网应用已广泛渗透到社会的政治、经济、文化等各个领域,并发挥着日益巨大的作用。在人类历史上,从来没有一项技术像网络一样如此巨大地影响着世界,改变着人们的生活方式。网络已将世界各个角落连在一起,缩短了世界各地间的距离,把地球变成了一个“地球村”。

通过网络,你可以干什么呢?

- 你可以给你的朋友发送邮件,邮件内容不光是文字,还可以包括图像、声音、视频等。哪怕朋友远在万里,只需几秒钟,他就能收到你的邮件。
- 你可在网上浏览世界各地的最新新闻,真正做到足不出户,能知天下事。你也可以根据自己的爱好订阅新闻,实现与世界同步。
- 你可在网上搜索你所需要的各种信息,旅游信息、医疗信息、股市信息、招工信息、航班信息等。你也可在网上炒股、网上支付、网上预订旅程等。
- 你可在网上获取你所需要的自然、历史、文化、科技等各种知识;通过网络,你可在线学习、在线交流,你可聆听世界著名科学家的讲座,也可参加世界排名前100位的大学的课程学习。网络已成为真正的知识海洋,已把全世界信息共享发挥得淋漓尽致。
- 你可在网上发布商品信息,在网上开店、网上购物、拍卖剩余物品,和世界各地的人们进行商品贸易等。你可在网上发布招聘信息,也可通过网络找到你所满意的工作。
- 你可通过各级政府开设的政务网站,与政府机关打交道,了解机构设置和职责,咨询有关政策,进行税务登记,实现企业执照的年检等。
- 你可在线点播电影,玩各种网络游戏。
- 你可通过博客、播客等方式传播个人信息,发表个人观点,与朋友交流思想情感等。
- 你可在网上与陌生人聊天,结识新朋友,甚至是异国他乡的朋友。

.....

以上只是网络世界的一部分,由于网络功能实在太强大,而且还在不断创新中,在这里我们无法将其一一列出。

我们从上面列举的功能已经知道,网络世界是一个精彩、丰富的世界,以至于人



们将工作、学习、娱乐、交友等全部搬到网上。网络改变了世界，世界需要网络。人类社会发展到今天，已不可能没有网络，对网络的依赖也达到前所未有的地步。因此，出现了有人“可以一天不睡觉、不吃饭，但不能一天不上网”的现象。

没有网络，世界会变成什么样呢？有人说，没有网络，世界可能会一团糟；也有人说，没有网络，世界将回到原始社会；甚至有人说，没有网络，我不想活了。各种各样的观点都有，下面作者将列举几个案例来说明网络是如何影响世界的，至于结论如何，还是让读者自己理解想象吧。

2006年12月26日，台湾地震造成海底光缆断裂，中国大陆地区联系外部的网络发生中断。MSN拒绝登录，微软、yahoo等邮箱不能打开。通过对7万多网民的调查发现：超过90%的网民认为，这次事故影响或严重影响了自己的工作和生活，52.13%的人称断网给自己或自己的公司造成了一些损失，38.82%的人表示损失严重。

2006年10月13日13时28分，北京首都机场电脑离港系统突然“罢工”，导致33个航班延误，致使乘坐飞机出港的旅客难以办理登记手续，机场一度处于混乱状态。

2006年4月20日，中国银联系统通信网络和主机出现故障，造成网上跨行转账业务、银联基金通业务和网上支付业务三个类别交易无法进行。故障期间，银行内人满为患，商场、医院、饭店等场所的人无法进行刷卡消费。

2005年6月18日，万事达、维萨和美国运通卡等主要信用卡服务的一个数据处理中心（这个数据处理中心负责审核商家传来的消费者信用卡号码、有效期等信息，审核后再传送给银行完成付款手续）网络被黑客程序侵入，约4,000万账户的号码和有效期信息被黑客截获。该公司接到了至少6.8万名用户举报，称账户已被人盗用消费。

2001年，尼姆达病毒在全球暴发，互联网因病毒大量传播而发生堵塞，全球损失达26亿美元。在美国，技术专家甚至告诉政府公务员，在病毒没有被查杀的情况下，不要打开自己的计算机。

▲ 1.2 网民的现状

根据internetworldstats (<http://www.internetworldstats.com/>) 统计，截至2007年9月1日，世界网民数已突破11亿(1,173,109,925)，占世界总人口(6,574,666,417)的17.8%。根据中国互联网信息中心(CNNIC)所作的第20次中国互联网络发展状况统计报告显示，中国的互联网普及率已经达到12.3%，比2006年同期(9.4%)提高了近3个百分点。互联网在中国的应用正逐步广泛化，越来越多的人接触互联网，并从互联网中获益。

截至2007年6月底，中国网民总人数达到1.62亿，仅次于美国(2.11亿)，位居世界第二，与2006年末相比，新增网民2,500万。我国目前有网站总数130多万个，但博客、股民、网络银行客户、电子邮箱总量等没有具体的数据，有报道说其分别为3,300万个、超亿人、4,000多万户、3.2亿个，这些数据只能作参考。但从网易发布其旗下有2,600万博客的数据可以看出，这些数据可能是个保守数。上述数据还



在不断增加,预计到2010年,我国网民将达5亿,数量将跃居世界第一。

要了解国民,必须了解网民。目前,各国政府都非常重视和关注网络,通过网络,可以了解民情,接受网上舆论的监督,接受网上投诉,并与网民进行“面对面”的交流。从1997年开始,中国互联网信息中心每年都要进行两次“中国互联网络发展状况统计报告数据调查”,至今已进行了20次,其数据可以说具有较高的权威性。我们从报告数据中可以全面了解网民的数量、年龄结构、学历、爱好等信息。

根据第20次中国互联网络发展状况统计数据显示:

我国网民中,男性网民8,900万,女性网民7,300万。25岁以下网民比例已经超出半数(占51.2%),30岁及以下的网民比例则高达70.6%。

中国网民大专以上学历占43.9%,网民中学历较低的人群正逐步增多,上网已经表现出明显的平民化趋势。

在全国2.16亿学生中,网民数量已有5,945万,互联网普及率达到27.5%,即每4个学生中,就有1个学生是网民。除学生外,企业工作人员是网民的最大的组成部分,数量已超过4,000万。此外,无业和自由职业者网民的数量也非常大,分别都已超过1,600万的规模。

网民在网上主要在干什么?有数据表明:

网络新闻、搜索引擎、即时通信、电子邮件、网络音乐、网络影视和网络游戏已成为大多数网民在网上的主要行为。

生活助手功能进一步延伸了网民的生活,给网民带来了更多的便利。一些代表性功能包括:网上求职、网上教育、网上购物、网上销售、网上旅行预订、网上银行和网上炒股等。各类行为数据见表1-1。

表1-1 网民的上网行为

	使用率		使用率
信息渠道		生活助手	
网络新闻	77.3%	网上求职	15.2%
搜索引擎	74.8%	网上教育	24.0%
写博客	19.1%	网上购物	25.5%
交流工具		网上销售	4.3%
即时通信	69.8%	网上旅行预订	3.9%
电子邮件	55.4%	网上银行	20.9%
娱乐工具		网上炒股	14.1%
网络音乐	68.5%		
网络影视	61.1%		
网络游戏	47.0%		



▲ 1.3 网络与犯罪

网络世界与现实世界一样，既有真情与友谊，也有邪恶与犯罪。网络是如此快捷、方便，又是如此的虚拟，并且与人们经济、生活密不可分，因此一些现实生活中的案件在网络中都出现了，如网络盗窃、网络诈骗、网络敲诈、网络诽谤、网络传销、网络赌博，等等。从某种意义上可以讲，互联网已经成为违法犯罪分子用来作案的重要工具之一。

国外有位专家说，10年之后，几乎全部的犯罪都将有计算机参与其中。国内则有专家称，目前在网络上的犯罪活动，除了需要身体接触外的案件，现实生活中的案件，在网上全能找到。尽管他们的说法可能都有点夸张，但这从一个侧面反映了网络犯罪的多样性和严重性。下面作者列举一些案例，让读者看看网络上到底有哪些犯罪活动。

☞ 案例 1-1

自2006年2月以来，犯罪嫌疑人张某开设“贵族商务网”，组织人员在该网站聊天室内进行淫秽表演，万某、罗某、余某三人负责对聊天室和账目进行管理。网站会员向管理员购买虚拟币后即可通过视频现场观摩淫秽表演。网站一天安排表演至少8场，每天赢利约1万元。同年4月，张某用同样的方法又开设了“BOSS俱乐部”网站。截至案发，两网站共发展会员约4,000人，网上专职表演人员400余人。

张某因传播淫秽物品罪被判处有期徒刑4年。

☞ 案例 1-2

2001年5月11日，中国轻纺城一经营户收到了一封署名“老胡”的电子邮件：“有人想要绑架你的儿子，如果要破财消灾，在指定的账户上存进两万元。”

警方根据“老胡”在网络上留下的蛛丝马迹，在绍兴一农户家中将犯罪嫌疑人钱某抓获。经审讯，钱某承认了他通过电子邮件，利用一张别人遗失的身份证办理的银行账户，向温州、杭州等地的企业老总进行敲诈的事实。

☞ 案例 1-3

2004年全国研究生入学统一考试前的一段时间，互联网上出现了一些兜售考研试题的信息，引起了教育部和公安部的高度重视。在有关省市区教育考试部门密切配合下，北京、天津、山西、辽宁、上海、福建、江西、湖北、湖南、广东、广西、贵州等省、市、区警方分别展开调查，成功查获7名涉案人员。

据已查获的犯罪嫌疑人天津市待业青年杜某、戴某，山西省忻州市待业青年李某等人交代，他们手中并无考题，在网上发布卖考题信息的目的是为诈骗牟利。



案例 1-4

33 岁的张某系浙江温岭市农民, 2004 年四五月份至 11 月 15 日间, 张某为牟取非法利益, 从青岛人李某、黄某处获取台湾新宝盈赌博公司管理网网址、投注网网址以及网络赌博的管理账号, 作为新宝盈赌博公司的代理在台州发展、纠集人员参与网络赌球。

2004 年 11 月 1 日至 13 日短短 13 天时间内, 张某的赌球账号上下注的赌资总额就高达 1,600 余万元, 张某也因此获利上百万元。

这起国内罕见的特大网络赌博案, 涉及浙江、山东等 5 个省市, 涉案人员 400 多人, 赌资高达 10 亿多元。

案例 1-5

一家总部设在美国的网站自称为全球远程教育网, 参加者只需花费人民币 1,360 元, 就可以获得价值 3,000 美元的电子邮包, 并同时取得推荐他人加入的资格。推荐别人购买 2 套 Wodunet 网站软件及“课程”, 就可以赚取 25 美元或 200 元人民币的报酬。如此往复, 就可以根据自己发展的“下线”以及“下线”推荐的人员数量获得报酬。

传销组织者杨某 2003 年加入该网站, 开始发展人员。被其发展的人员, 很多是不懂计算机、不会上网的中老年人。截至案发, 杨某已发展人员 1,800 余人, 涉案金额 250 余万元。

案例 1-6

2006 年 3 月 28 日下午, 徐州张女士来到自动柜员机上查询银行卡里的存款余额时, 发现她所持有的两张工商银行银行卡 (一张存有 15,000 元, 另外一张存有 4,600 元) 的余额分别只剩下 1 元和 2 元。

经银行调查发现, 卡中钱是分 9 次从网上银行被划走的。

调查人员排除了张女士电脑被黑客入侵或中木马病毒的可能, 同时也了解到, 张女士近两万元钱已经通过网上银行直接划到安徽省芜湖市开户的两张银行卡上, 但两张可疑的银行卡都是用假身份证办理的。

警方最后破获此案, 在安徽省芜湖市抓获了 11 名犯罪嫌疑人。据犯罪嫌疑人胡某交代, 他们利用受害者一些疏漏、疏忽, 通过猜测密码的方式, 破译了受害者的密码, 侵入到受害者银行账户当中, 把资金窃取。截至案发, 该犯罪团伙在全国 20 多个省、市盗窃 200 多人的银行存款约 120 多万元。

案例 1-7

2006 年 4 月 29 日, 网民高某在某网站论坛涉及“打击非法营运车辆”的讨论中, 编造“爆炸”的恐怖信息, 引发公众恐慌。高某已被检察机关以涉嫌编造、故意传播



虚假恐怖信息罪批准逮捕。

案例 1-8

2007 年 3 月 3 日, 互联网一博客中出现一条消息: 某县某乡长为担任县土管局副局长, 向有关领导行贿 30 万元。警方经过多日调查走访, 将此案侦破。犯罪嫌疑人孙某是该县土管局一名中层干部, 为阻止他人与自己竞争县土管局副局长的职位, 他唆使好友黎某捏造竞争对手行贿的消息, 并在另一犯罪嫌疑人贾某的帮助下在网上发布。

孙某等人已被检察机关以诽谤罪批准逮捕。

案例 1-9

2006 年年底, “熊猫烧香”病毒在网上暴发。几乎在一夜之间, 数以百万计的电脑纷纷受到一只憨态可掬的“熊猫”的攻击。截至 2006 年 12 月底, 已有超过 50 万台计算机受此病毒感染, 而受害企业用户更是达到上千家。

2007 年 2 月, 湖北省警方侦破了这起制作、传播计算机病毒案件, 李某等主要犯罪嫌疑人被一一抓获。

案例 1-10

黄某是一家网络公司研发部项目经理, 该公司主要为客户提供影片下载服务。2005 年 8 月, 黄某所在公司发现另一家提供影片下载服务的宽娱公司销售业绩较好, 便要求本公司员工设法提高业绩。黄某遂想出用恶意软件攻击宽娱公司的网站, 使其无法提供正常的服务。

2006 年 8 月, 黄某购买了一款攻击软件, 远程操控网吧电脑, 对宽娱公司的网站服务器和影片更新服务器发动拒绝服务攻击, 致使其六台服务器间断性瘫痪, 客户无法登录网站。

黄某的上述行为, 造成宽娱公司大量客户流失, 直接经济损失达 7 万余元。

2007 年, 被告人黄某被法院判处拘役 3 个月, 缓刑 3 个月的处罚。

从以上案例中我们可以知道, 上述专家的说法并不是危言耸听, 网络犯罪已呈现出愈演愈烈之势。

据美国联邦贸易委员会估计, 每年大约有 1,000 万美国人的个人信息被盗窃或滥用, 个人信息失窃以及由此引发的相关欺诈活动, 给消费者造成 50 亿美元的损失, 使商业和金融机构的损失高达 480 亿美元。

日本国家警察厅发布的报告说, 2005 年涉嫌网络犯罪被逮捕人数已超过 2004 年的 2,081 人, 增长了近 52%。

我国自 1986 年发现首例计算机犯罪以来, 利用计算机网络犯罪案件数量迅猛增加。据统计, 1986 年发案仅 9 起, 1999 年立案侦查的就有 400 余起, 2000 年剧增到 2,700 余起, 2001 年则高达 4,500 余起。



根据瑞星发布的《互联网安全报告》披露,目前我国每天有数百个甚至数千个病毒被制造出来,大多是木马和后门病毒。从QQ密码、网游密码到银行账号、信用卡账号等,任何可以直接或间接地转换成金钱的东西,都成为黑客窃取的对象。黑客与病毒制造者已逐渐形成庞大、完整的产业链(黑客侵入个人或企业的计算机,窃取机密资料,然后在网上出售获取金钱)。

有关部门曾进行过统计,网络案件的犯罪嫌疑人多为年轻人,年龄大多在33岁以下。这个年龄段人群,网民数量最多,犯罪率也最高。

表1-2是根据第20次中国互联网络发展状况统计报告数据而获得的,表1-3是根据近万名违法犯罪人员年龄进行统计而获得的。两表数据表明,犯罪年龄分布曲线与网民年龄分布曲线(见图1-1)非常接近,可以说是一致的。

表1-2 网民年龄分布

18岁以下	18~24岁	25~30岁	31~35岁	36~40岁	41~50岁	51~60岁	60岁以上
17.7%	33.5%	19.4%	10.1%	8.4%	7.2%	2.7%	1.0%

表1-3 违法犯罪人员年龄分布

18岁以下	18~24岁	25~30岁	31~35岁	36~40岁	41~50岁	51~60岁	60岁以上
9.4%	38.5%	20.5%	13.1%	8.8%	7.3%	2.0%	0.4%

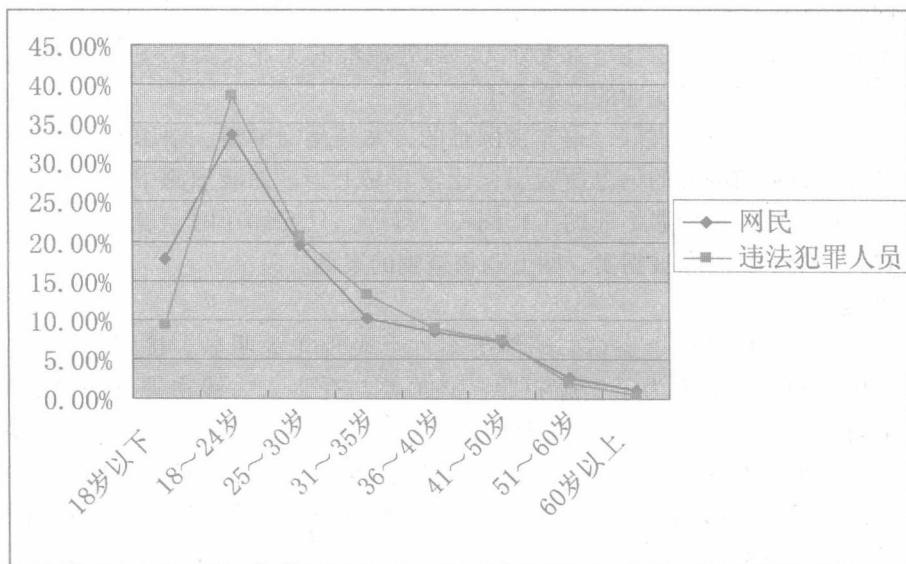


图1-1 网民与违法犯罪人员年龄分布图