辽宁省教育厅青年基金项目

计算机取证技术

JISUANJI QUZHENG JISHU

米 佳　刘浩阳　编著

群众出版社

辽宁省教育厅青年基金项目

计算机取证技术

米 佳 刘浩阳 编著

公安机关
内部发行

群众出版社
2007年·北京

图书在版编目(CIP)数据

计算机取证技术/米佳,刘浩阳编著.—北京:群众出版社,2007.4

ISBN 978-7-5014-3990-4

Ⅰ.计… Ⅱ.①米… ②刘… Ⅲ.计算机犯罪—证据—调查—研究 Ⅳ.D915.5.13

中国版本图书馆 CIP 数据核字(2007)第 033127 号

计算机取证技术

编　　著/米　佳　刘浩阳
责任编辑/韩俊雯
封面设计/王　子

出版发行/群众出版社　电话:(010)52173000 转
社　　址/北京市丰台区方庄芳星园三区 15 号楼
网　　址/www.qzcbs.com
信　　箱/qzs@qzcbs.com
经　　销/新华书店
印　　刷/北京市亚通印刷厂

890×1240 毫米　32 开　9.75 印张　270 千字
2007 年 4 月第 1 版　　2007 年 4 月第 1 次印刷
印数:0001-3000 册

ISBN 978-7-5014-3990-4/D·1924　　定价:20.00 元

前　言

在信息技术飞速发展的今天，无论是基于计算机和网络的高科技、高智能犯罪案件还是传统的各类刑事案件、行政案件、民事案件，许多重要证据都留在了计算机和网络中。因此，警察和司法人员从计算机和网络里获取犯罪证据的能力就变得尤为重要。

计算机取证技术就是把计算机看作是犯罪现场，对各种存储介质中保存、恢复的数据进行的一种科学的检查和分析方法。计算机取证技术作为一项特殊的技术，经过十余年的发展，已经成为公安部门发现证据、获取证据的重要技术手段之一，被广泛地用来解决大量的计算机犯罪和事故，包括网络入侵、盗用知识产权、保险诈骗、洗钱、色情活动、赌博和 E－mail 欺骗等。国外很多专业院校和取证研究机构一直在开展计算机取证技术研究，并开设了一系列关于计算机取证的专业课程，为执法机关、调查机构培训专业的计算机取证、数据分析人才。

本书是作者承担辽宁省教育厅青年基金项目“计算机犯罪侦查与取证的研究”的研究成果，主要侧重于从技术角度，对计算机取证技术基础、计算机取证原则和方法、计算机取证技术应用及常用的计算机取证设备等几方面进行全面系统的介绍，适合于公安院校相关专业的师生、网络警察以及计算机犯罪相关执法人员阅读。

本书由辽宁省教育厅和大连市科技局资助出版，全书在编写过程中得到了公安部十一局许建卓博士、辽宁警官高等专科学校、大连市公安局网络警察支队、厦门美亚柏科有限公司的大力支持，在此向上述单位及个人表示衷心的感谢！向全国计算机取证界的朋友和全国广大网络警察战友们表示敬意！

编者

2007 年 3 月

目　录

第一章　计算机犯罪及其侦查机构 …… (1)
1.1　计算机犯罪的定义 …… (1)
1.1.1　国外关于计算机犯罪概念的界定 …… (1)
1.1.2　我国刑法中关于计算机犯罪的定义 …… (3)
1.1.3　计算机犯罪的几种形式 …… (4)
1.2　计算机犯罪的特点 …… (5)
1.3　计算机犯罪的现状 …… (7)
1.4　计算机犯罪的立法 …… (8)
1.4.1　国外计算机犯罪立法状况 …… (8)
1.4.2　我国计算机违法犯罪处罚依据 …… (9)
1.5　计算机犯罪侦查机构的建立 …… (9)
1.5.1　国外计算机犯罪侦查机构 …… (9)
1.5.2　我国计算机犯罪侦查机构的建立 …… (12)
第二章　计算机取证概述 …… (14)
2.1　电子证据及其特点 …… (14)
2.1.1　电子证据的概念 …… (14)
2.1.2　电子证据的特点 …… (16)
2.1.3　常见电子设备中潜在的电子证据 …… (18)
2.2　计算机取证技术概述 …… (20)
2.2.1　计算机取证技术的相关概念 …… (20)
2.2.2　计算机取证的三个重要知识体系 …… (22)
2.2.3　计算机取证的基本原则 …… (22)
2.2.4　计算机取证的相关技术 …… (23)
2.2.5　涉及的案例类型 …… (24)

2.3 国内外计算机取证技术的发展和研究概况 …… (25)
2.3.1 国外计算机取证技术发展概况 …… (26)
2.3.2 我国计算机取证技术发展概况 …… (28)
2.4 计算机取证技术的发展趋势 …… (30)
第三章 计算机取证相关技术基础 …… (35)
3.1 数据存储设备和存储原理 …… (35)
3.1.1 硬盘存储原理 …… (35)
3.1.2 数字移动设备存储原理 …… (53)
3.2 磁盘的文件系统 …… (56)
3.2.1 常用的文件系统 …… (56)
3.2.2 文件存储原理 …… (58)
3.3 数据的删除与恢复原理 …… (59)
3.3.1 硬盘分区方式 …… (59)
3.3.2 数据恢复原理 …… (60)
3.3.3 操作系统的启动 …… (62)
3.4 系统日志文件的查看和记录方式 …… (65)
3.4.1 日志的概念 …… (65)
3.4.2 日志的特点 …… (66)
3.4.3 系统日志文件 …… (67)
3.5 数据加密技术 …… (77)
3.6 CRC 校验和 MD5 哈希 …… (78)
3.7 Internet 基础 …… (80)
3.8 网络数据包的截取和解密技术 …… (82)
3.9 恶意代码 …… (84)
3.9.1 恶意代码的定义及传播特点 …… (84)
3.9.2 恶意代码的类型 …… (84)
3.10 漏洞扫描 …… (85)
3.11 入侵检测 …… (86)
第四章 计算机取证的原则、技术和流程 …… (89)
4.1 计算机取证的原则 …… (89)

4.2　计算机取证的技术 …… (90)
4.2.1　基于单机和设备的计算机取证技术 …… (90)
4.2.2　基于网络的计算机取证技术 …… (94)
4.3　计算机取证的流程 …… (97)
4.3.1　评估阶段 …… (97)
4.3.2　获取阶段 …… (98)
4.3.3　检查和分析阶段 …… (103)
4.3.4　备案和报告阶段 …… (103)
4.4　计算机取证工具介绍 …… (104)
4.4.1　现场获取设备 …… (104)
4.4.2　数据分析工具 …… (110)
第五章　计算机现场勘查与取证 …… (115)
5.1　勘查流程 …… (116)
5.1.1　进入现场之前的准备工作 …… (116)
5.1.2　提取、固定易失性数据 …… (119)
5.1.3　搜查证物 …… (123)
5.1.4　在线分析 …… (125)
5.1.5　提取、固定证物 …… (126)
5.1.6　证物移交 …… (128)
5.2　一个典型的现场勘查流程 …… (129)
第六章　计算机取证技术应用 …… (130)
6.1　IE 访问历史记录的分析与取证 …… (130)
6.1.1　行为记录文件介绍 …… (130)
6.1.2　Index. dat 取证 …… (148)
6.2　注册表分析与取证 …… (150)
6.2.1　注册表概述 …… (151)
6.2.2　注册表的组织结构 …… (152)
6.2.3　注册表的分析 …… (156)
6.2.4　几种常见软件的注册表相关数据 …… (160)
6.2.5　注册表的取证 …… (163)

6.3 电子邮件的调查与取证 …… (165)
6.3.1 电子邮件的诞生与发展 …… (165)
6.3.2 电子邮件的传输原理 …… (166)
6.3.3 电子邮件的编码方式 …… (170)
6.3.4 电子邮件的分析 …… (172)
6.4 即时通信工具的调查与取证(QQ、MSN、UC) …… (184)
6.4.1 QQ …… (184)
6.4.2 MSN …… (187)
6.4.3 雅虎通(Yahoo! Messenger) …… (188)
6.4.4 新浪 UC …… (189)
6.5 网络证据调查取证 …… (194)
6.5.1 网络犯罪的特点 …… (195)
6.5.2 网络证据调查取证要点 …… (197)
6.5.3 Windows 系统篇 …… (198)
6.5.4 Unix/Linux 系统篇 …… (200)
6.5.5 路由器的调查取证 …… (203)
6.6 数字移动设备的取证 …… (215)
6.7 基于数据挖掘的计算机取证技术 …… (218)
6.7.1 计算机取证中的数据挖掘技术 …… (218)
6.7.2 基于计算机犯罪的广义数据恢复与模式重现原则 …… (220)
6.7.3 应用实例 …… (222)
第七章 国内外常用计算机取证硬件和软件介绍 …… (227)
7.1 国外计算机取证硬件 …… (227)
7.1.1 Logicube …… (227)
7.1.2 ICS …… (229)
7.1.3 Tableau …… (231)
7.1.4 VOOM …… (233)
7.2 国外计算机取证软件 …… (234)
7.2.1 New Technologies Incorporated …… (234)

7.2.2　Guidance Software …… (235)
7.2.3　AccessData …… (236)
7.2.4　Ilook …… (238)
7.2.5　Vogon …… (239)
7.2.6　MASTER …… (239)
7.2.7　ProDiscover …… (241)
7.2.8　X－way Forensic …… (241)
7.3　国内取证公司及其产品介绍 …… (242)
7.3.1　厦门美亚柏科公司 …… (242)
7.3.2　北京天宇宏远公司 …… (245)
7.3.3　金诺网络安全技术发展公司 …… (246)
7.4　Unix/Linux 系统下的取证软件 …… (248)
7.4.1　TCT …… (249)
7.4.2　TASK …… (249)
7.4.3　TaFusion MEPIS Forensic System …… (250)
7.4.4　ForensiX …… (250)
7.5　手机和 PDA 取证软件…… (251)
7.5.1　PDA 取证工具软件——PDA Seizure …… (251)
7.5.2　手机取证工具软件——Cell Seizure …… (252)
7.5.3　手机、PDA 取证工具软件——Device Seizure …… (253)
第八章　数据恢复技术 …… (255)
8.1　数据损坏的原因 …… (256)
8.1.1　物理损坏 …… (256)
8.1.2　逻辑损坏 …… (257)
8.2　数据恢复的方式 …… (258)
8.2.1　硬件恢复 …… (258)
8.2.2　软件恢复 …… (260)
8.2.3　数据恢复的常用方法 …… (260)
8.3　数据恢复技术的未来前瞻 …… (266)
第九章　电子证据司法鉴定和相关标准、法律规范 …… (270)

9.1 电子证据司法鉴定 …… (270)
9.1.1 电子证据司法鉴定要解决的主要问题 …… (272)
9.1.2 对电子证据司法鉴定机构取证和鉴定程序的要求 …… (273)
9.1.3 电子证据鉴定的步骤 …… (274)
9.1.4 制作电子证据鉴定报告 …… (275)
9.2 电子证据司法鉴定人员的权利和义务 …… (275)
9.2.1 司法鉴定人的权利 …… (275)
9.2.2 电子证据司法鉴定人员的义务 …… (276)
9.3 计算机取证过程和法律效力 …… (277)
附 录 …… (282)
附录1 几种常见硬盘复制机的比较 …… (282)
附录2 常见设备速度一览 …… (284)
附录3 HASH 算法 …… (286)
附录4 计算机取证的步骤 …… (288)
附录5 常见进程名列表 …… (292)
附录6 残留痕迹常见隐藏位置 …… (294)
参考文献 …… (297)

第一章　计算机犯罪及其侦查机构

近年来，我国信息技术和信息产业迅猛发展，计算机技术特别是因特网对我国政治、经济、军事、科技、文化、教育、卫生及人民群众日常生活的各个领域都产生了广泛而深远的影响，同时也为违法犯罪分子提供了新的犯罪空间和手段。计算机犯罪（Computer Crime）呈现日趋严重的发展态势，从最初的仅是针对钱财的犯罪，发展为针对政治、军事、知识产权等多个领域的犯罪；从单机犯罪，发展到现在的网络犯罪。计算机犯罪给国家安全和社会稳定造成了严重的威胁，严重地危害了我国的政治安全、经济安全和社会安定。

1.1　计算机犯罪的定义

计算机犯罪是刑事犯罪中一种新兴的高科技犯罪，如何界定计算机犯罪，各个国家根据计算机犯罪发展阶段、国家的立法实际及历史文化背景对其从不同的角度提出了不同的定义和解释。

1.1.1　国外关于计算机犯罪概念的界定

综观国外的计算机犯罪概念，归纳起来大致有以下几种：

国际经济合作开发组织（Organization for Economic Cooperation and Development，OECD），将计算机犯罪或与计算机有关的犯罪定义为：关于自动化资料处理与（或）数据传输中任何非法、不道德或越权的行为（any illegal，unethical，or unauthorized behavior involving automatic data－processing and/or transmission of data），以作为 OECD 对各会员国的立法建议。

欧洲经济合作与发展组织的专家认为：在自动数据处理过程中，任何非法的，违反职业道德的，未经批准的行为都是计算机犯罪。

美国司法部从技术角度认为，计算机犯罪是“在导致成功起诉的非法行为中，计算机技术和知识起了基本作用的非法行为”。而美籍华人学者刘江彬认为：“所谓计算机犯罪系指以计算机为工具，采用非法手段使自己获利或使他人遭受损失的犯罪行为。计算机犯罪最基本的要件必须与计算机有关，以它为工具应包括那种以计算机作为犯罪工具和以它作为犯罪对象的情形。”

美国联邦调查局认为，与计算机有关的犯罪（computer – related crime），及凡以计算机为犯罪工具或犯罪目的之所有犯罪皆属计算机犯罪。研究和报告有关计算机犯罪预防、侦查、调查和起诉等情况的美国全国计算机犯罪数据中心认为，涉及使用计算机及破坏计算机或其部件的一切犯罪都是计算机犯罪。

美国斯坦福研究所计算机安全和犯罪高级研究专家唐·B. 帕克根据计算机在犯罪过程中扮演的角色，在他的《计算机犯罪》（Crime by Computer）一书中，提出了计算机犯罪的四种形式：计算机是犯罪对象，计算机构建了实施犯罪的环境，计算机提供了实施犯罪的手段，计算机被用来实施恐吓、欺骗或诈骗受害者。

澳大利亚也有学者把计算机犯罪解释为与计算机有关的盗窃、贪污、诈骗、破坏行为。

德国学者认为，“所谓计算机犯罪，是指利用电子数据处理设备作为作案工具的犯罪行为或者把数据处理设备作为犯罪对象的犯罪行为”。

法国刑法规定，“凡以欺骗手段打入或控制整个或部分数据自动处理系统的行为；有意无视第三者权利，阻碍数据自动处理系统工作或使其发生错误的行为；有意无视第三者权利，直接或间接地将数据植入系统中，或者消除、修改自动处理系统原有数据，或消除、修改自动处理系统数据处理或传播方式的行为”，都是计算机犯罪。

日本警察厅认为，“对非法连接计算机网络系统的通信电缆等附带设备的犯罪，以及所有改换、消除现金卡、信用卡的磁条部分的犯罪都是计算机犯罪”。日本学者板仓宏认为“计算机犯罪是指与计算机相关联的一切反社会行为”。

综上所述，我们可以把广义的计算机犯罪定义为包括利用计算机的犯罪和针对计算机的犯罪两大类。

1.1.2　我国刑法中关于计算机犯罪的定义

根据我国《刑法》第二百八十五条和第二百八十六条分别规定的有关计算机犯罪的内容，以及1997年12月11日最高人民法院发布的《关于执行〈中华人民共和国刑法〉确定罪名的规定》，所谓计算机犯罪，是指借助计算机实施相关犯罪，以计算机资源为对象而实施的犯罪的总称。即计算机犯罪是针对和利用计算机系统，通过非法操作或者其他手段对计算机系统的完整性或正常行为造成危害后果的行为。

本书所指的计算机犯罪是指在法律中有特别定义的犯罪活动。即刑法在妨害社会管理秩序罪一章中规定的扰乱计算机信息系统安全管理秩序的四种犯罪：非法侵入计算机信息系统罪、删除修改增加干扰计算机信息系统功能罪、删除修改增加计算机信息系统中数据和应用程序罪、故意制作传播计算机病毒等破坏性程序罪，具体条款如下：

第二百八十五条，违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

第二百八十六条，违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。

违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。

故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。

第二百八十七条，利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的，依照本法有关规定定罪处罚。

近些年，随着计算机普及应用和网络化的发展，计算机已经渗透

到人们生活的各个方面，因此我们认为，只要与经济利益相关或涉及国家安全等方面的案件，涉案计算机都要纳入视线范围，对计算机系统进行相应勘察分析，防止未能深入挖掘出潜在的计算机犯罪。同时，要注意正确区分一般治安案件与计算机犯罪案件。

1.1.3 计算机犯罪的几种形式

归纳起来目前常见的计算机犯罪形式有以下几种：

1. 信息的窃取和利用

其中最为典型的是计算机窃取和电话网络的盗用。计算机窃取主要表现为通过窃取电子货币账单、银行账目结算单、清单等的相关信息，达到改变公私财产所有权的目的。这类信息窃取犯罪在经济领域十分猖獗。信息盗用犯罪常见的是盗用电话网等通信网络，主要表现为盗码、并机使用不纳费电话号码、买卖外国电话卡号码、盗用共用电话用的电话卡等。这种信息犯罪行为给电信部门和合法用户造成了很大的损失。

2. 信息的欺诈与勒索

其中较为普遍的是通过伪造信用卡、制作假票据、篡改电脑程序等手段来欺骗和诈取财物的犯罪行为。据报道，2003 年我国台湾地区伪造信用卡盗刷造成银行损失金额高达亿千万台币。一个名为“塞巴网络恐怖分子”的国际电脑匪帮通过设置软件逻辑炸弹破坏各网络公司的电脑系统来敲诈勒索，短短三年就作案百余起，共勒索各电脑公司一亿多美元。

3. 信息的攻击和破坏

主要表现为犯罪分子以非法的方式故意对计算机程序或数据资源实施破坏性攻击。例如用电磁铁使磁带或磁盘上的数据或程序丢失、消灭或更改原有的数据资料使系统的操作不能达到设计的目的等，其中最为严重的是通过计算机网络以计算机病毒的方式进行信息攻击和破坏。

4. 信息的污染与利用

主要是一些不法分子出于经济或政治动机，或纯粹出于好奇等目的利用信息网络传播有害数据、发布虚假信息、滥发商业广告、随意

侮辱诽谤他人和滥用信息技术等方面的犯罪行为。如在互联网上散发色情文章以收取费用，散布反动言论破坏社会稳定，用种族主义、恐怖主义的游戏软件挑起种族情绪危害国家安全。

1.2　计算机犯罪的特点

计算机犯罪作为一种刑事犯罪，具有与传统犯罪相同的许多共性特征，但是作为一种与高科技伴生的犯罪，它又有许多与传统犯罪相异的特征，具体表现在：

1. 智能性高

大家知道，无论是简单还是复杂的计算机信息系统，通常都采取多层次、全方位的安全防范机制，因而如果想把计算机作为一种犯罪工具或者想非法侵入计算机信息系统都不是一件容易的事情，只有具有丰富的计算机专业知识和熟练技巧的人才可能做到这一点。正如有的学者所言，单以对于安全系统的破坏而言，犯罪行为人至少必须与安全系统的设计人具有同等的智能才能做到。

犯罪的高技术性决定了作案主体多为白领阶层，其中主要包括和计算机系统的管理、维护和操作相关的程序设计员、系统维护员、设备维修员、计算机操作员和管理人员。这些犯罪主体与传统犯罪的主体相比通常学历更高、专业性更强，给破案侦查、取证、起诉和审判都造成了一定的困难。

2. 隐蔽性强

任何犯罪行为都有隐蔽性的共同特点，计算机犯罪的隐蔽性则表现得更为突出。一方面，是犯罪行为的隐蔽性强。由于计算机软件数据存储的无形性和资料形态的多元化，使得一般人不易察觉到计算机内部软件资料上发生的变化，往往犯罪行为已经发生并已经被记录而计算机本身的运行却丝毫没有被影响，从外表上看也没有什么特别的变化，所以对于被害人而言通常也很难察觉犯罪行为的发生。事实证明，在已经发现的计算机犯罪案件中，多数是偶然被发现的，或者是犯罪人一时大意而暴露了犯罪行为，只有少数犯罪行为是被害人及时

发觉后主动追查犯罪人的。另一方面，是犯罪人的隐蔽性强。从犯罪技术上讲，计算机网络技术的复杂性导致犯罪人可以通过在网络中不断重复登录的手段来隐藏自己。通过重复登录，犯罪人可以从一个国家绕到另一个国家，最终联结到受害人的计算机系统上，每登录一次犯罪者的身份就可以变更一次，而且由于广泛使用匿名服务器，犯罪人可以通过这些匿名服务器来更好地掩盖自己的身份，因此很难确定犯罪人所在地和犯罪人的身份。

此外，由于大部分计算机犯罪发生在金融领域或者机要部门，受害人往往从商业信誉和名声考虑，即使发现了计算机犯罪，也往往隐瞒下来，控制外传，自行处理而不向有关执法机关报案。这种拒不报案的做法使得计算机犯罪更为猖獗，同时也构成了计算机犯罪隐蔽性的另一面。

3. 危害性大

计算机犯罪所造成的损失极其严重，这一点通常是传统型犯罪所无法比拟的。从经济角度讲，计算机犯罪多数为财产性犯罪，其所涉及的金额之大通常是其他犯罪无法望其项背的。几个著名的计算机财产犯罪欺诈案涉及金额均达上亿美元。从社会尺度来衡量，计算机犯罪对于整个社会的政治、经济、文化、军事等方面产生了全方位的冲击，其严重的社会危害性、难以预测的突发性和直接的连锁反应性是其他任何犯罪所不能比拟的。

4. 地域性广

计算机网络的国际化使得计算机犯罪往往是跨地区甚至是跨国界的。对于这种地域性较广的犯罪形式，如何确定犯罪行为地及犯罪结果地是一个值得研究的问题。例如非法侵入计算机信息系统犯罪，当犯罪人在中国领域外实施犯罪行为，而被侵入的计算机信息系统处于中国领域内时，其刑事管辖权方式的选用和诉讼程序的选择都是一个复杂的问题。

5. 诉讼困难

计算机犯罪是一种与时代同步发展的高科技犯罪。目前，一方面，由于计算机犯罪案件的随机性和数据证据问题，导致诉讼困难，

使得一些犯罪案件即使定了罪也往往由于证据问题而从轻处罚。另一方面，大多数司法人员严重缺乏计算机专业知识，不能适应现代计算机犯罪的侦查、起诉和审判等司法活动的需要，甚至对于已经发现的计算机犯罪案件也由于审判人员不懂计算机技术而难以理清案情的脉络，抓不住案情的要害无法定罪。

1.3　计算机犯罪的现状

世界范围的计算机犯罪活动，已经对经济全球化和信息网络化产生了不利影响。世界上第一起有案可查的滥用计算机事件于1958年在美国发生。进入20世纪90年代以来，计算机犯罪日趋猖獗，造成的危害越来越大，国外犯罪学家已经预言，未来信息化社会犯罪的形式将主要是计算机犯罪。发达国家的情况已经证明这一点，计算机犯罪案件已成为十分严重的社会问题。据Warron Research的调查，1997年世界排名前一千的公司几乎都曾被黑客闯入。据统计，近几年美国每年因计算机犯罪造成的损失超过70亿美元，德国约50亿美元，英国约30亿美元。试想如果恐怖组织侵入华尔街的计算机系统实行网络恐怖主义，那对全球的经济造成的危害后果恐怕远比“9·11”恐怖袭击事件大得多。我国自1986年发生第一起计算机犯罪案件以来，发案数连年上升。据公安部公共信息网络安全监察局不完全统计，从1997年到2005年全国公安机关共查处针对计算机信息系统实施的违法犯罪案件达1152起。

纵观国内外计算机犯罪现状，计算机犯罪活动突出表现为：

● 非法侵入重要信息系统，修改或破坏网络功能或数据信息，造成数据信息丢失或网络瘫痪。

● 故意制作、传播计算机病毒等破坏性程序，攻击计算机系统及通信网络，致使计算机系统及通信网络遭受损害，危害计算机信息系统安全。

● 利用计算机信息网络进行侮辱、诽谤他人及进行盗窃、诈骗、敲诈等犯罪活动。