

信息安全系列丛书

Computer Forensics

计算机取证

杨永川 顾益军 张培晶 等 编著

 高等教育出版社

信息安全系列丛书

Computer Forensics

计算机取证

杨永川 顾益军 张培晶 等 编著



高等教育出版社

内容提要

计算机取证是一个涉及法学、刑事侦查学、计算机科学等学科的交叉学科,在进行计算机取证的相关司法实践过程中,也常常需要对相关问题从相关法律、侦查方法、取证规范、取证技术等多个角度进行思考。本书介绍计算机取证的相关研究与司法实践方法,内容涵盖计算机犯罪、电子证据和计算机取证的基本概念、基本原理和方法,主要内容包括计算机取证程序、计算机取证技术、计算机取证工具、计算机取证法律和规范、对典型对象的调查取证和计算机取证实验等。

本书适合作为信息安全和相关专业研究生的教学参考书,也可作为信息安全、计算机取证、电子证据司法鉴定等领域研究人员、技术人员和管理人员的参考书。

图书在版编目(CIP)数据

计算机取证 / 杨永川等编著. —北京:高等教育出版社,
2008.6

ISBN 978 - 7 - 04 - 024749 - 7

I. 计… II. 杨… III. 计算机犯罪—证据—调查 IV.
D915.13

中国版本图书馆 CIP 数据核字 (2008) 第 079235 号

策划编辑 陈红英 责任编辑 陈红英 封面设计 刘晓翔 责任印制 宋克学

出版发行 高等教育出版社
社 址 北京市西城区德外大街 4 号
邮政编码 100011
总 机 010 - 58581000

经 销 蓝色畅想图书发行有限公司
印 刷 高等教育出版社印刷厂

开 本 787 × 1092 1/16
印 张 17
字 数 340 000

购书热线 010 - 58581118
免费咨询 800 - 810 - 0598
网 址 <http://www.hep.edu.cn>
<http://www.hep.com.cn>
网上订购 <http://www.landaco.com>
<http://www.landaco.com.cn>
畅想教育 <http://www.widedu.com>

版 次 2008 年 6 月第 1 版
印 次 2008 年 6 月第 1 次印刷
定 价 30.00 元

本书如有缺页、倒页、脱页等质量问题,请到所购图书销售部门联系调换。

版权所有 侵权必究

物料号 24749 - 00

信息安全系列丛书编审委员会

主任：卿斯汉

副主任：陈克非 王清贤 王丽娜

委员（按姓氏笔画排列）：

方 勇 吴 向 李凤华 何大可 张宏丽 张焕国
肖德琴 罗 平 杨义先 杨永川 周明全 林柏钢
赵一鸣 钮心忻 胡华平 贾春福 唐韶华 谢冬青
曾贵华 董晓梅

前言

计算机取证(Computer Forensics)的任务是解决各种计算机犯罪案件以及传统的刑事案件、民事案件、行政案件涉及的计算机及相关系统、设备的取证问题。随着计算机及网络普及程度的不断提高,各种利用计算机工具从事的犯罪活动以及涉及计算机取证的各种其他刑事犯罪、民事案件、行政案件越来越多,计算机取证司法实践需求十分迫切,该领域的研究与实践受到越来越广泛的关注。目前,国内许多法律部门,特别是公安机关都拥有了自己的计算机取证实验室,同时还成立了电子证据检定机构,从事相关数字证据的司法鉴定。为适应计算机取证司法实践的需要,国内许多院校和研究机构开展了计算机取证的研究,许多院校的计算机安全专业开设了计算机取证研究生课程,为了适应信息安全的研究和教学需要,我们编写了本书。

计算机取证是一个涉及法学、刑事侦查学和计算机科学等学科的交叉学科,在进行计算机取证的相关司法实践的过程中,也常常需要对相关问题从相关法律、侦查方法、取证规范、取证技术等多个角度进行思考。为了帮助读者对计算机取证的相关研究与司法实践方法有一个全面的了解,本书从计算机犯罪、数字证据、计算机取证概念的界定及涉及的相关法律法规、计算机取证程序、计算机取证技术以及计算机取证工具和取证实实践等多个角度,对于计算机取证相关领域的研究进展和较为常用的取证实实践方法进行了较为全面的介绍。相关内容包括:

第1章计算机犯罪与数字证据,从刑法学表述、犯罪学表述以及相关学术研究等多个方面对计算机犯罪概念进行了分析,结合相关学术观点对计算机犯罪概念进行了界定,并对计算机犯罪的特定和发展趋势进行了分析;从立法角度和学术研究角度对数字证据的概念进行了界定,并从法律视角对数字证据来源及收集、数字证据保全及效力、数字证据认定及出示等计算机取证相关环节进行了分析。

第2章计算机取证概述,对计算机取证研究的发展历程、计算机取证概念、计算机取证的研究内容和发展趋势进行了概要介绍。

第3章计算机取证程序,重点介绍了国内外计算机取证程序、计算机取证原则、计算机取证步骤的相关研究。

第4章计算机取证技术,详细介绍了计算机取证中涉及的相关技术,并对计算机取证过程中所涉及的常用技术进行了深入分析。

第5章计算机取证工具、第6章典型对象的调查对取证实践中涉及的取证工具和取证方法进行了详细介绍,并在第7章计算机取证试验针对计算机取证过程中遇到的一些常见问题设计了取证实验。

本书适合作为信息安全和相关专业研究生的教学参考书,也可作为信息安全、计算机取证、电子证据司法鉴定等领域研究人员、技术人员和管理人员的参考书。

本书由中国人民公安大学杨永川和顾益军张培晶编写,董健、郝文江、杨莉莉、张羽参与了本书的编写工作。

由于编者水平有限,书中难免存在错误、疏漏和欠妥之处,敬请读者批评指正。

作者

2008. 4. 12

目录

34	计算机犯罪与数字证据	1
34	1.1 计算机犯罪概述	1
34	1.1.1 概念的历史来源	1
34	1.1.2 概念的界定方法	2
34	1.1.3 学术界观点评析	3
34	1.1.4 计算机犯罪的界定表述	4
34	1.1.5 计算机犯罪特点	6
34	1.2 计算机犯罪的现状及趋势	7
34	1.2.1 计算机犯罪的现状	7
34	1.2.2 计算机犯罪趋势	10
34	1.3 数字证据概述	13
34	1.3.1 国内数字证据规定	14
34	1.3.2 国外数字证据规定	15
34	1.3.3 学术界观点评析	17
34	1.3.4 数字证据的广义界定	19
34	1.3.5 数字证据的特点	20
34	1.4 数字证据的来源及收集	20
34	1.4.1 数字证据来源	20
34	1.4.2 数字证据收集	21
34	1.5 数字证据的保全及效力	25
34	1.5.1 数字证据保全	26
34	1.5.2 数字证据效力	30
34	1.6 数字证据的认定及出示	32
34	1.6.1 数字证据认定	32
34	1.6.2 数字证据出示	35
34	思考题	38
34	第2章 计算机取证概述	40
34	2.1 计算机取证的起因与现状	40

2.1.1	计算机取证的发展历程	40
2.1.2	我国计算机取证的发展现状	43
2.2	计算机取证概念	45
2.2.1	典型的计算机取证概念	45
2.2.2	计算机取证概念的界定	46
2.3	计算机取证的研究内容	46
2.3.1	计算机取证程序	47
2.3.2	计算机取证技术	47
2.3.3	计算机取证工具	49
2.3.4	计算机取证法律与规范	50
2.4	计算机取证的发展趋势	54
	思考题	55
第3章	计算机取证程序	56
3.1	国外计算机取证程序分析	56
3.1.1	事件响应方法	56
3.1.2	数字犯罪现场调查过程模型	57
3.1.3	取证抽象过程模型	57
3.1.4	集成的数字调查过程模型	58
3.1.5	端到端的数字调查过程模型	58
3.1.6	综合计算机取证模型	59
3.2	国内计算机取证程序分析	60
3.2.1	多维计算机取证模型	60
3.2.2	基于抽象层的取证模型	61
3.3	计算机取证程序原则	62
3.3.1	一般刑事案件取证原则	62
3.3.2	计算机取证原则	63
3.4	计算机取证步骤	65
3.4.1	准备响应阶段	66
3.4.2	调查取证阶段	68
3.4.3	整理阶段	80
	思考题	81
第4章	计算机取证技术	82
4.1	计算机取证技术的研究范围	82
4.1.1	计算机证据收集技术	82
4.1.2	计算机证据分析技术	87
4.1.3	计算机证据呈堂技术	89

4.2 计算机取证中的常用技术分析	89
4.2.1 数据恢复技术	89
4.2.2 基于后门程序的主机信息监控技术	92
4.2.3 基于网络嗅探的网络信息监控技术	96
4.2.4 基于网络搜索的互联网信息监控技术	111
4.2.5 串匹配技术	120
4.3 计算机取证技术的发展趋势	126
思考题	126
第5章 计算机取证工具	128
5.1 计算机取证中的通用工具	128
5.1.1 证据收集类	128
5.1.2 证据分析类	132
5.1.3 证据呈堂类	135
5.2 专用取证工具	136
5.2.1 国外研制的专用取证工具	136
5.2.2 国内研制的专用取证工具	143
5.3 计算机取证工具的发展趋势	146
思考题	146
第6章 典型对象的调查	147
6.1 Windows 系统调查取证	147
6.1.1 Windows 系统联机取证调查	147
6.1.2 Windows 系统取证复制	169
6.1.3 Windows 系统静态取证分析	175
6.2 UNIX 系统调查取证	196
6.2.1 UNIX 系统联机取证调查	197
6.2.2 UNIX 系统取证复制	206
6.2.3 UNIX 系统静态取证分析	214
6.3 网络及关键设备的调查取证	230
6.3.1 IP 地址定位	230
6.3.2 MAC 地址定位	233
6.3.3 路由器的调查取证	234
6.4 获取网络数据流信息	237
6.4.1 UNIX/Linux 系统环境下的网络嗅探	238
6.4.2 Windows 等系统环境下的网络嗅探	239
思考题	240
第7章 计算机取证试验	241

7.1 计算机取证试验室	241
7.1.1 试验室要求	242
7.1.2 试验室功能	242
7.1.3 功能区域划分	243
7.1.4 器材配备	243
7.2 数据恢复试验	244
7.2.1 试验目的	244
7.2.2 试验准备	245
7.2.3 试验步骤	245
7.3 EnCase 分析试验	247
7.3.1 试验目的	247
7.3.2 试验准备	247
7.3.3 试验步骤	248
7.4 易失证据获取试验	249
7.4.1 试验目的	249
7.4.2 试验准备	249
7.4.3 试验步骤	251
7.5 网络协议分析	252
7.5.1 试验目的	252
7.5.2 试验准备	252
7.5.3 试验步骤	253
7.6 系统日志分析试验	253
7.6.1 试验目的	253
7.6.2 试验准备	253
7.6.3 试验步骤	254
思考题	255
参考文献	256
3.1 IP 地址	230
3.2 MAC 地址	233
3.3 路由器	234
4.1 UNIX 系统	237
4.2 Windows 系统	238
4.3 网络	239
4.4 网络	240
4.5 网络	241

第1章 计算机犯罪与数字证据

随着世界科学技术的迅猛发展和信息技术的广泛应用,特别是我国国民经济和社会信息化进程的全面加快,计算机信息系统的基础性、全局性作用日益增强,计算机信息安全已经成为国家安全的重要组成部分。但随着计算机技术的发展,计算机犯罪也呈现出与日俱增的态势。本章通过对计算机犯罪概念的理解,分析了当前我国计算机犯罪的现状与发展趋势,进而提出了数字证据的概念。数字证据是指能够为法庭接受的、足够可靠和有说服性的、存在于计算机和相关外设中的电子数据的确认、保护、提取和归档的过程中产生的证据^[1]。同时,本章还提出了数字证据来源与收集、数字证据保全与效力以及数字证据认定与出示等一系列认知性的概念问题。

1.1 计算机犯罪概述

随着科学技术的不断发展,计算机普及程度不断增加,我国社会已经进入高科技时代。2008年1月18日,中国互联网络信息中心(CNNIC)在北京向全世界发布了我国第21次中国互联网发展与统计报告。其中指出:截至2007年12月,中国网民人数已经达到2.1亿,仅次于美国2.15亿的网民规模,位居世界第二。目前中国的互联网普及率已经达到12.3%,比2006年同期9.4%的互联网普及率提高了接近3个百分点^[2]。与此同时,计算机犯罪案件也与日俱增,并呈现出受害范围广、无时空地域界限、社会危害严重等特点,使得我国刚刚起步的互联网产业受到了严重威胁,阻碍了社会主义建设的和谐有序发展。

人们一般把以计算机为主要工具的犯罪和以计算机资产为对象的犯罪总称为计算机犯罪。计算机犯罪与计算机技术的发展和有着密切的关系。随着科学技术的发展以及计算机应用领域的拓宽,犯罪的方式、手段、领域等将随之发生变化,犯罪概念的内涵和外延也会有所改变。因而在探讨计算机犯罪概念之前,有必要分析计算机犯罪概念含义的发展变化过程。

1.1.1 概念的历史来源

现代计算机起源于军事应用,最早的计算机犯罪也发生在军事部门,且与计算

机充当的角色、担负的作用有关,比如用来处理军事信息的计算机就可能成为被间谍攻击的目标。20世纪80年代中期以后,随着计算机性能的提高和计算机网络的出现,计算机应用领域不断扩大,许多企业和机构对计算机的依赖程度日益增加,计算机犯罪的领域、方式出现了一些与传统犯罪有质的差异的新特点,当时的法律在惩处这类犯罪时也遇到很多困难。因而,有的学者和执法人员提出了“计算机滥用”的概念。所谓“滥用”,即表明除计算机诈骗外,计算机犯罪还有许多其他方式。英国商业学校对1990年3月前的计算机滥用情况进行调查,得出的结果是英国每年因计算机滥用造成的损失是4.07亿英镑,为此1990年英国制定通过了《计算机滥用法》(Computer Misuse Act)^[3]。

20世纪90年代,计算机网络的发展使计算机犯罪概念逐步演变为特指网络空间犯罪或信息犯罪。比如,利用网络窃取政治、军事、经济及商业秘密,销售毒品,传播黄色淫秽物品,侵犯知识产权和公民隐私权等,成为众所周知的犯罪形态。美国于1996年成立对付计算机犯罪的专门委员会,德国禁止网络上传播新纳粹主义,新加坡政府对网络内容信息进行全面审查及登记。我国于1994年2月颁布了第一部计算机安全法规,即《中华人民共和国计算机信息安全保护条例》,联网运行的计算机是其保护对象。1998年公安部成立“公共信息网络安全监察局”,简称网络警察。可见,计算机犯罪已发展为网络空间犯罪,并成为世界各国的共识。

1.1.2 概念的界定方法

目前世界各国有许多不同的观点,归纳起来大致有两大类,即刑法学定义的概念和犯罪学上的概念。刑法学上的概念是以刑事实体法为基准定义的犯罪,即法律上的定义。犯罪学上的概念即犯罪定义虽以刑事实体法为基准,但又不完全局限于刑事实体法的规定,这是犯罪学研究方面的定义。我国犯罪学家康树华认为:“刑法学上的犯罪概念是刑法规定的,作为追究刑事责任的论据,从这种意义上说,它是狭义的犯罪概念。而犯罪学上的犯罪概念,是在刑法学犯罪概念基础上发展起来的。也就是说,犯罪学上的犯罪概念是以刑法作为依据,但它却不局限于刑法的规定,它还包括其他法律文件所规定的违法行为以及有可能发展为违法犯罪的不良行为。从这种意义上说,它是广义的犯罪概念。”

目前,世界各国对计算机犯罪没有统一的界定方法,但总体上可以在以下三个方面形成共识:

(1) 计算机犯罪是隶属于犯罪的一种,计算机犯罪可能类似于传统意义上的犯罪,如盗窃、诈骗、伪造和破坏等,这类犯罪不论在哪个国家或地区都会受到惩处。

(2) 计算机犯罪是高科技犯罪,它的技术性很强。随着计算机技术的发展和计算机应用的普及,其表现形态、犯罪方式、技术手段等都将进一步发展,刑法不可

能超前对其所有的形式进行规定。(3) 与社会的发展和历史文化有着不可割裂的联系。

1.1.3 学术界观点评析

计算机犯罪不是指计算机自身实施的犯罪行为,而是由人所实施的与计算机有关的犯罪行为。这一概念是 20 世纪五六十年代在美国等信息科学比较发达的国家提出并形成的。到目前为止,围绕计算机犯罪概念的讨论仍然相当激烈,归纳起来有以下几种观点,即相关说、滥用说、工具说、工具对象说。

1. 相关说

(1) 欧洲计算机合作与发展组织对计算机犯罪所下的定义为:“在自动数据处理过程中,任何非法的、违反职业道德的、未经授权的行为都是计算机犯罪。”这是一个较广的定义。但是它只是对计算机犯罪的一种可行的分类,并没有精确的界定。在这一定义中,不仅把违法行为当成犯罪来解释,而且把违反数据处理职业道德的问题也提高到了法律范畴的高度,混淆了道德和法律的区分,这显然是不合适的。

(2) 美国司法部的《刑事审判对策》中对计算机犯罪的定义为:“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。”该定义从刑事审判角度出发是比较恰当的,但该概念不能作学术研究上的计算机犯罪定义。因为,成功的起诉包括刑事起诉和民事起诉,该定义混淆了违法与犯罪的界限,而且把计算机犯罪解释为纯技术性的犯罪,并没有包括计算机犯罪的全部含义。

(3) 瑞典数据法中对计算机犯罪的定义为“侵犯个人隐私的行为为计算机犯罪”。如未经允许建立和保存计算机私人文档;侵犯受保护的数据;非法存取电子数据处理记录;非法修改、删除、录入记录或准备侵犯数据等。这个定义并没有包括数据诈骗的全部内容,也没有包括对计算机信息系统的破坏等行为。鉴于数据法的宗旨是保护计算机系统中的个人数据,此种提法是可行的,但不能作为一般的计算机犯罪定义来理解。

(4) 中国政法大学信息技术立法课题组从学术角度对计算机犯罪所下的定义为:“与计算机相关的危害社会并应当处以刑罚的行为。”该定义用“相关”一词来描述各种计算机犯罪,没有把计算机在犯罪中的地位和作用表述出来,显得含糊且不确切。

2. 滥用说

中国台湾学者对计算机犯罪的定义为:“计算机犯罪是指滥用电脑或使用足以破坏电脑系统正常运作之行为,而形成与电脑特质有关之犯罪”。即行为人滥用电脑或破坏电脑之犯罪行为需与电脑之特质有关者,才属于电脑犯罪。反之,行为人以电脑为犯罪工具或犯罪客体,但其行为与电脑之特质无关者,即非电脑犯罪。他们认为,电脑本身不会犯罪,只是被有些人滥用,所以有学者愿意使用“电脑滥

用”或“与电脑有关的犯罪”一词来代替“电脑犯罪”一词。这与“橱柜犯罪”、“刀子犯罪”是一个道理。他们认为电脑犯罪是具备电脑特质的行为,如与电子资料处理有关、具备自动化犯罪过程(与传统的以手动为主不同)的行为。简言之,惟有操作电脑资料的不法行为才可称为电脑犯罪。该定义较为准确地把握了计算机犯罪的根本特征,即“与电脑特质有关”的犯罪,排除了计算机犯罪与传统财产犯罪的混淆,但不足之处在于没有明确界定何为“电脑特质”,对“电脑犯罪”的范围认定也比较宽泛。

3. 工具说

将计算机犯罪定义为:“所谓计算机犯罪就是指那种利用计算机辅助实施的犯罪行为”^[4]。这一定义仅把计算机犯罪解释为行为人利用计算机作为犯罪工具而实施的各种犯罪行为,忽视了计算机犯罪中的其他方面的因素。

4. 工具对象说

中华人民共和国公安部网络监察局对计算机犯罪的定义为:“以计算机为工具或以计算机资产为对象实施的犯罪行为。”这一定义避免了纯技术性、片面性,还对计算机在犯罪中所处的地位和作用进行了简单表述。但该定义也有不妥之处,一是没有对“计算机资产”作限制性解释,而且把“以计算机为工具”和“以计算机资产为对象”割裂开来;二是没有对“以计算机为工具”作特定的解释,比如,用电脑砸死人按此定义应该属于“以计算机为工具”的计算机犯罪,而实际上它属于传统的杀人罪。也有专家把计算机犯罪定义为:“计算机犯罪是指行为人以计算机的技术知识发挥作用为前提,实施的与计算机特性有关的各种犯罪行为的总称”^[4]。该定义指出,必须是利用计算机操作所实施的危害计算机信息系统(包括内存数据和程序)安全的犯罪行为才可以称为计算机犯罪。如果仅仅将计算机、计算机信息系统、计算机的数据和程序作为单纯的物理性存在而利用与计算机技术毫不相干的手段和方法加以侵害的行为只是传统的财产犯罪而不是计算机犯罪,这一定义的优点是:第一,说明了计算机犯罪行为只能通过计算机的非法操作来实施,突出了计算机作为犯罪工具所具有的不可替代性,而在传统型犯罪中计算机作为工具是有替代性的。第二,这一定义符合有关计算机犯罪的立法原意。

1.1.4 计算机犯罪的界定表述

1989年,欧盟犯罪问题委员会为各成员国制定了一系列立法指南,列举了应该予以处罚的计算机犯罪行为,但没有试图确定一个正式的计算机犯罪定义,而将它留给各成员国按照各自的法律体系和历史传统自行解决。本书对于计算机犯罪概念的界定主要从刑法学角度和犯罪学角度进行分析。

1. 刑法学上的表述

我国1997年3月14日修订、同年10月1日施行的刑法在惩治计算机犯罪方面作了三条五款的规定:

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。

第二百八十七条规定: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。

第二百八十七条其实是说明利用计算机进行传统犯罪不能视为刑法上的单独罪名,比如利用计算机进行贪污犯罪仍视为贪污罪,因而也不属于刑法上的计算机犯罪概念范畴。真正的计算机犯罪罪名是第二百八十五条的“非法侵入计算机信息系统罪”和第二百八十六条的“破坏计算机信息系统罪”^①。

综上,刑法学上的计算机犯罪可表述为:非法侵入受国家保护的重要计算机信息系统以及破坏计算机信息系统并造成严重后果的应受刑法处罚的危害社会的行为。简言之,计算机犯罪就是“侵入或破坏计算机信息系统的应处以刑罚的行为”。犯罪客体是我国计算机信息系统安全管理秩序,犯罪的客观方面是对计算机信息系统实施了侵入,对其功能、数据、程序及其运行实施了破坏,犯罪主体是一般主体,犯罪的主观方面是故意。

2. 犯罪学上的表述

当代犯罪学中关于犯罪的概念大致有三种定义,即“法律的定义、社会学的定义和法律与社会学综合的定义”^[5]。犯罪的法律定义即刑法学上的定义,认为“犯罪的决定性因素是对刑事法律的破坏,犯罪是指现行法律所指控为犯罪的行为”,持这种观点的某些犯罪学研究者甚至将犯罪学视为刑法学的补充学科。犯罪的社会学定义有多种解释,其基本含义是“把犯罪行为归结为社会生活的产物,认为犯罪是与现行行为规范相冲突的行为,它包括一切反社会行为”。犯罪的法律与社会学综合定义是试图通过将两者结合起来而获得的一个完善的定义,认为“犯罪既是法律范畴的,也是社会范畴的,犯罪是社会法律现象,是在一定时间和空间范围之内所实施的被法律规定为犯罪的危害社会行为”^[5]。我们赞成法律与社会学综合定义。犯罪学家康树华在其主编的《犯罪学通论》一书中认为,我国犯罪学研究的主要任务有以下三方面:“调查研究我国各时期特别是现阶段犯罪情况及其变化发展,预测未来犯罪的发展趋势,分析产生犯罪的社会因素和犯罪人犯罪的主观因

① 最高人民法院和最高人民检察院对刑法中关于计算机犯罪的罪类定名。

素,为党和国家制定同犯罪作斗争的方针、政策、法律、法令提供可靠的经验素材和理论依据;总结和在新的历史条件下预防犯罪的有效途径、方法和措施,为制定和完善我国犯罪预防的方针、政策、法律以及建立健全社会的犯罪预防体系提供依据;为建立和完善新中国犯罪学而努力”。

依据国内外犯罪学者对犯罪的定义及我国犯罪学的研究任务,参考国内外计算机安全专家对计算机犯罪的界定,我们认为,我国现阶段从犯罪学角度研究计算机犯罪应该有广泛的视野,可以考虑方方面面的因素,视为一种社会法律现象。因而,犯罪学上的计算机犯罪可表述为:针对或利用计算机信息系统及其所处理的信息而实施的违法犯罪或将来可能发展为违法犯罪的具有社会危害性的行为。

1.1.5 计算机犯罪特点

计算机犯罪是一类新型犯罪,花样繁多,具有许多传统犯罪所不具备的特点。从犯罪学的角度来看,计算机犯罪通常具备以下主要的特征。

1. 犯罪形式的隐蔽性

互联网的出现大大拓宽了计算机犯罪的空间,例如有些计算机犯罪可以通过网络远程实现,其来源可来自全球的任何一个终端,随机性很强。而且计算机执行一项犯罪指令常常在瞬间即可完成,有些罪证只涉及几个字节(Byte)的信息。许多犯罪嫌疑人选择将计算机信息系统中销毁或删除,因而留下的数字证据,常常是一些不可直接阅读的电磁纪录。巨大的网络空间和计算机犯罪中反取证技术的使用,大大提高了计算机犯罪的隐蔽性,同时也增加了数字证据的取证难度。根据美国商务部透露,100例计算机犯罪中仅有1例被发现,而发现的犯罪中有70%被披露。

另外,计算机犯罪黑数高。所谓黑数是已经实际存在,但未被列入官方统计的计算机犯罪总和中的那部分犯罪数字。造成计算机犯罪黑数值高的原因主要有两个:一是计算机犯罪往往涉及公民的隐私、公司企业的秘密乃至商业的信誉,受害者为维护自身的信誉并不乐意报案。二是司法机关对计算机犯罪惩治力度不大。由于我国司法机关普遍存在经费不足,无法与金融、国防等部门同步进行计算机管理工作,而司法工作人员缺乏计算机专业知识,对计算机犯罪难以发现,不能适应计算机犯罪的侦查、起诉和审判等司法活动的需要。

2. 犯罪主体及手段的智能性

计算机犯罪的根本特点在于犯罪过程中高技术和高智能的结合。在计算机犯罪的各种手段中,无论是“特洛伊木马术”还是“逻辑炸弹”,无一不是凭借高科技手段实施的,而熟练运用这些并实现犯罪目的的则是具有相当丰富的计算机技术知识和娴熟的计算机操作技能的专业人员。而且犯罪分子在作案前常常会进行周密的预谋和精心的准备,如对计算机信息系统及其工作机制进行全面的考察,选择适当的时机和地点精心策划反侦查对策等,这都要求行为人必须具备较高智能。

3. 犯罪动机的多面性

多数计算机犯罪案件以贪财牟利为目的,但也有其他因素。美国一项研究表明,促使犯罪者实施计算机犯罪的最有影响力的因素是个人财产上的获利,其次是进行犯罪活动的智力挑战。也有一些掌握计算机技术的年轻人并非为了进行恶意破坏或非法侵占他人财产,而只是为了满足好奇心或者炫耀自己的才能而设计计算机病毒,或成为“黑客”浏览访问非授权文件从而导致犯罪。

4. 破坏性极大

在计算机犯罪中,财产犯罪是主要形态,其涉案金额非常惊人。如美国 Equity Funding 保险欺诈案中,犯罪通过利用计算机伪造大量的保险单证骗取保险金额,涉案金额高达 20 亿美元。一些具有较强破坏性的计算机犯罪,如通过制造或传播病毒会造成大规模的数据丢失,系统瘫痪等事件,也会为社会带来巨大损失。

1.2 计算机犯罪的现状及趋势

近年来,随着信息技术的迅猛发展,我国计算机的应用日益广泛和深入,普及程度也越来越高。但是,科学技术是一把双刃剑,在给人类带来巨大便利和进步的同时,也带来一系列的社会问题。正如一位计算机犯罪专家所说:“计算机键盘,作为一种非常有用的工具,加快了人类发展的进程,但它同时也成为了一种危险的武器,不仅会给国家或团体带来巨大的经济损失,还有可能使其分裂或解体;对于个人,它甚至会危及人的生命。”因此,在人类越来越离不开计算机和信息网络的同时,信息网络特有的开放性、隐蔽性、高效性以及快捷性等特点,也给犯罪分子提供了高超的作案技术手段和广阔的作案空间,不仅滋生出许多新的犯罪类型。并且传统的违法犯罪活动在信息环境下也纷纷呈现出新的发展势头,对社会造成了严重的危害。因此,对于我国计算机犯罪及其现状进行分析与对策研究,有助于帮助认识新形势下的计算机犯罪现象,帮助预防、打击和控制计算机犯罪。

1.2.1 计算机犯罪的现状

1. 计算机犯罪案件

随着我国计算机及其技术的日益普及,与计算机有关的各类违法犯罪活动也日益剧增,近年来发案率更是呈直线上升趋势,每年都以 30% 的速度递增。利用计算机制作、复制传播色情、淫秽物品的案件十分突出,网上诈骗、网上敲诈勒索、利用网络非法传销的案件增多,危害计算机信息网络安全案件增幅较大,侵犯公民人身权利和民主权利的案件也在增长,利用互联网危害国家安全的案件持续上升。据统计,1998 年立案侦查的计算机违法犯罪案件仅为百余起,而到 2006 年已上升到 5100 多起,其中 90% 以上的案件牵涉网络,而且犯罪类型和手段日益多样化。2005 年以来,以下五种类型犯罪明显增多:一是利用计算机制作、复制、传播