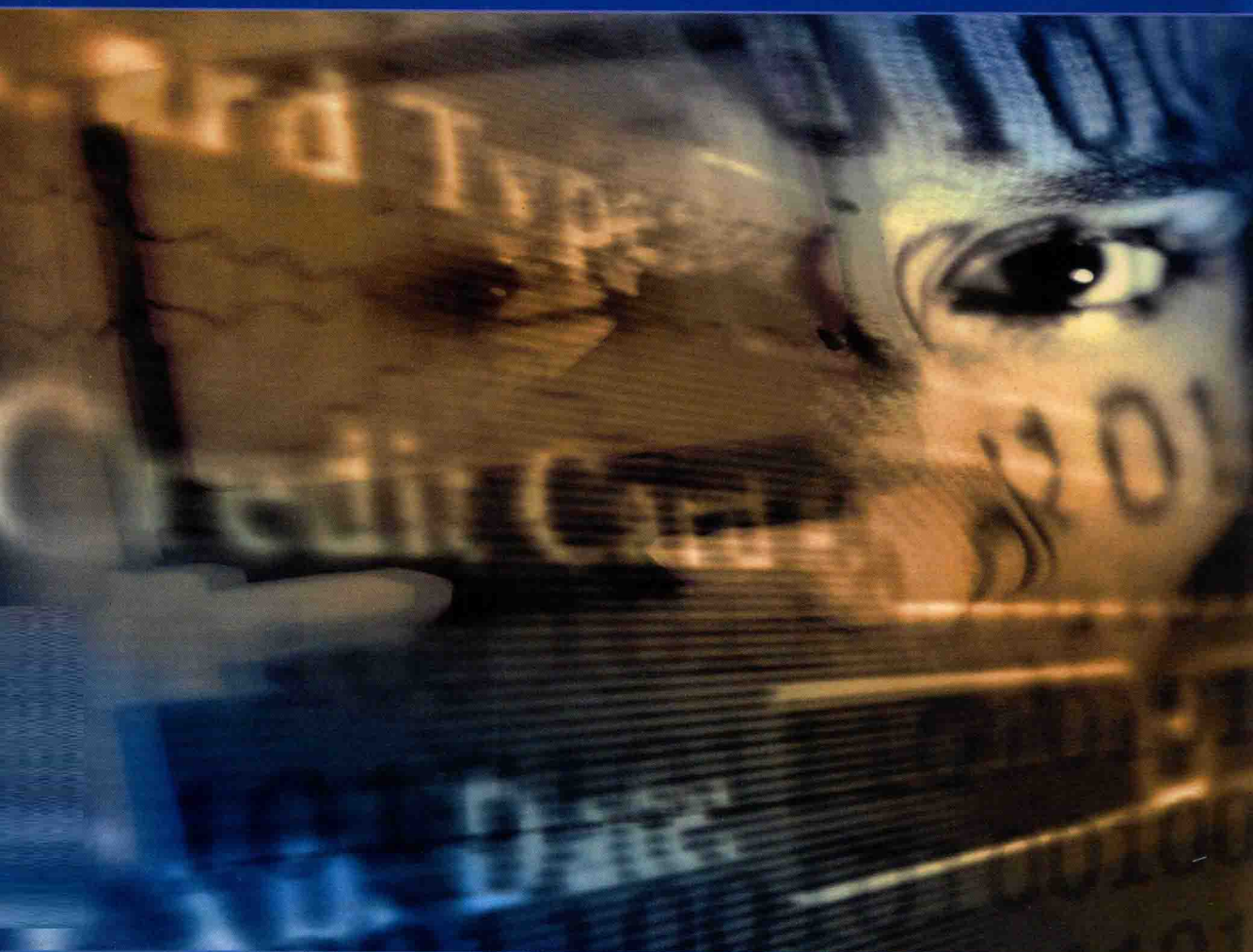
JISUANJI FANZUI YU XIANCHANG KANCHA

郑学功 张明 张晓岩 郑鹏程 编著

计算机犯罪与现场勘查



中国人民公安大学出版社

计算机犯罪与现场勘查

郑学功 张 明 张晓岩 郑鹏程 编著

（· 行）

中国人民公安大学出版社

·北 京·

计算机犯罪与现场勘查

JISUANJI FANZUI YU XIANCHANG KANCHA

郑学功　张　明　张晓岩　郑鹏程　编著

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：涿州市蕴铂印刷有限公司

版　　次：2002 年 9 月第 1 版
印　　次：2004 年 4 月第 2 次
印　　张：10.5
开　　本：787 毫米×1092 毫米　1/16
字　　数：228 千字
印　　数：1501～2500 册

ISBN 7－81087－056－4 / D·053
定　　价：25.00 元（公安机关　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）83905728

E-mail：cpep@public.bta.net.cn

顾问委员会

主任顾问	曲植凡					
副主任顾问	陈吉光	朱有林	张福胜	尹丰文	马兴华	韩良波
	宋卫宁	丁秀华	杨志顺	朱同胜	雷兴华	都建军
	张治平	徐保强	林治鉴	宿　兴	杨卫国	朱金义
	王万威	陈守礼	宋宜斌			
顾　问	李进武	李国峰	王盛林	李卫光	闫光祝	程绍良
	芦新力	曲永广	高振林	赵焕光	宋光明	夏吉恒
	蔡永强	于元魁	季永章	邵爱民	刘建强	李法军
	张力洋	田　力	宋华君	孙为国	贾桂玉	张英珊
	张海涛	武维刚	刘　通	周学军	张维民	蔡　平
	杜晓伟	孙松君	邱兆江	李向东	范景春	赵忠环
	刘书堂	杜福贵	刘志光	王振苏	迟善书	杨秀霞

序

进入 21 世纪，信息技术越来越深刻地影响着人类社会的发展。党的十五届五中全会作出了大力推进国民经济和社会信息化的战略部署，必将大大加快我国现代化建设的历史发展进程。但是信息网络这把“双刃剑”在促进社会、经济和文化发展的同时，不可避免的要带来诸如网上有害信息传播、网络化犯罪、计算机病毒肆虐等负面影响，对社会稳定和国家安全构成新的威胁，这就给新时期公安工作提出了新的严峻挑战。加强公共信息网络安全监察理论研究，对于推进公共信息网络安全监察工作的不断发展，确保公共信息网络安全至关重要。

公共信息网络安全监察是公安机关维护高科技领域安全稳定的新型公安业务工作，具有政策性强、科技含量高的特点。这就更加突出了加强理论研究的重要性。《计算机犯罪与现场勘查》一书是开展公共信息网络安全监察理论研究的成果。作者长期战斗在公安机关公共信息网络安全监察第一线，在打击计算机违法犯罪的实际工作中积累了较为丰富的经验。在本书的写作过程中，作者查阅参考了大量资料，进行了积极有益的探索，付出了辛勤的劳动。这种立足本职、勤于钻研、勇于探索、敢为人先的精神，值得大力提倡和鼓励。

希望本书的出版，能对广大公共信息网络安全监察民警有所裨益。

曲 植 凡

2001 年 11 月 18 日

自　序

谨以此书献给广大的公共信息网络安全管理计算机业界人士。

从1946年世界上第一台电子计算机 ENIAC 的诞生，迄今仅有短短五十多年的历史，但它给整个人类社会历史和科学技术发展带来了革命性的变化。它是人类继蒸汽机和电的使用之后，又一次重大的技术革命。计算机的发展经历了一个从低级到高级，从简单到复杂的过程。其间，计算机活动与其管理，随着信息科学技术的不断发展，亦经历了一个从混乱逐步走向有序，即逐步体制化的过程。特别是近年来世界各国纷纷将计算机技术引入网络管理，借以把网络管理中的网络管理功能、测试仪器和人力资源的重大成功因素集中起来，从而满足现代网络管理的各种要求。

伴随着信息革命浪潮的强大冲击，全球网络热正以不可遏止的势头在世界各国兴起，并广泛应用于政治、经济、文化、军事等各个领域。不仅对人类生产和生活产生了极其深刻的影响，而且为社会的发展与进步带来了前所未有的机遇。然而，网络犹如一把双刃剑，它既可以极大地造福社会，又可以无情地损害人类。尤其是来自网络空间的种种危害，给经济建设和社会稳定构成了现实的威胁，几乎使每个国家和地区都面临着新的更加严峻的挑战。计算机的安全问题日益突出和复杂，计算机犯罪率呈几何级数增长。在信息时代里，犯罪已经转向了高科技的犯罪。以计算机为目标和以计算机为工具的犯罪愈来愈多。随着计算机网络化的飞速发展，特别是国际互联网用户的逐步增加，国外特务机关加强了从互联网上对我国政治、经济、军事机密情报的窃取和政治渗透，加强了对我国某些政治意志薄弱者的勾联、收买和策反活动。敌对分子利用计算机电磁泄漏和信息辐射的弱点，非法从通信线路上截取数据或在机房附近用专用设备接收计算机向外泄漏的电磁波，然后再加以复原；一些高技术犯罪者不断地研究跟踪破译技术，使得各种数据加密标准频频遭受挑战。

目前，国内计算机犯罪的形式已呈多样化，计算机案件已经从最初单纯的病毒破坏，发展到了制造和传播计算机病毒、计算机黑客、利用电磁辐射窃取计算机信息、设置逻辑炸弹、故意对数据或程序实施破坏、利用计算机盗用或非法转移资金以及利用互联网进行计算机犯罪等很多方面。计算机犯罪的表现往往也不再是一种单一的形式，而是几种形式结合在一起，这就给计算机犯罪案件的侦破工作提出了更高的要求。种种事实充分说明，必须加强对计算机犯罪技术的研究，以适应飞速发展的形势的需要。

我国的反计算机犯罪工作主要分为三个阶段：一是反计算机病毒；二是反制作、传播有害信息和制作、传播淫秽、色情软件；三是网络诞生后，对各种综合计算机犯罪问题的处理。

本书分为四章，第一章概述了计算机犯罪的有关内容；第二章详细地介绍了计算机犯罪的攻击步骤与手段；第三章简述了计算机案件现场勘查的基础理论知识和实用技巧；第四章研究了计算机的数据恢复。该书内容丰富、材料翔实、重点突出、可读性强，它可以作为计算机犯罪案件勘查技术人员的教材，又可以作为公共信息网络安全管理人员的通用读本和解决安全问题的实用工具书。

当历史已将世界推向 21 世纪时，《计算机犯罪与现场勘查 》作为刑事侦查学领域中一个新的分支学科而面世，读者不妨将其视为计算机案件侦查学研究中一个新的“热点”。随着时光流逝，如果这个新的“热点”能衍变成几个“热点”、几十个“热点”；这一个个“热点”如果能联成一条条“热线”；这一条条“热线”如果能织成一张张“热网”；而一张张“热网”如果能构成一个硕大的“热体”。那么，我国的《公共信息网络安全案件侦查学》事业定会百尺竿头，更进一步。这也是编著者决心出版这部拙著的动机。

编著者企盼着这一天早日到来……

路漫漫其修远兮，

吾将上下而求索。

本书在编著过程中，引用、参考了一些中外及互联网上的文献与资料，并得到了国内反病毒专家王江民先生的指点，同时为编著者无偿提供了 KV3000 进行数据恢复的全部资料，江民公司的技术专家对全书进行了技术审核。值此书付梓之时，谨向作者、编者深表谢意！由于笔者才识学浅，时间仓促，错误之处在所难免，恳请专家、学者批评斧正。

郑学功 张明 张晓岩 郑鹏程

2001 年 6 月 23 日

前　言

当今社会是信息化社会，电子计算机和通信网络已经广泛地应用到社会的各个领域，利用这些先进技术建立起来的信息系统正改善着人们的生活和工作方式。然而，在我们享受着众多信息系统带来的巨大方便的同时，也时时受到来自各方面对信息系统安全的威胁。据美国 FBI 统计，每年因信息和网络安全原因所造成的损失高达 75 亿美元，法国为 80 亿法郎。此外，计算机病毒也会对计算机信息系统及网络造成严重的破坏，因此计算机信息系统的安全成为了迫切需要解决的问题。

信息安全是社会稳定安全的必要前提条件，随着信息攻击和信息犯罪的增多，社会对信息安全的重视程度显然也达到了空前的高度。信息系统安全无误地运转变得空前重要，并已经引起了我国政府和研究机构的高度重视。

1992 年，我国颁布了《计算机软件保护条例》，1994 年颁布了《中华人民共和国计算机信息系统安全保护条例》，这是我国最早的关于计算机信息系统安全方面的法规。之后，又陆续颁布了《中华人民共和国人民警察法》、《中华人民共和国计算机信息网络国际联网管理暂行规定》、《中国公众多媒体通信管理办法》、《国际联网安全保护管理办法》、《计算机信息系统安全规范》、《关于对国际联网的计算机信息系统进行备案的通知》、《计算机信息系统安全产品分类原则》、《金融机构计算机信息系统安全保护工作暂行规定》、《计算机信息系统国际联网保密管理规定》、全国人民代表大会常务委员会《关于维护互联网安全的决定》、《互联网上网服务营业场所管理办法》，并在《刑法》中增设了关于计算机犯罪的条款。由此可见，上述法规的发布实施，标志着我国计算机信息系统安全保护工作已走上了法制化、规范化的轨道。各级公安机关已责无旁贷地承担起计算机安全保护的历史重任，各级计算机应用部门和单位，应积极配合计算机安全主管部门做好计算机信息系统的安全防范工作，切实维护好国家信息的安全。

计算机犯罪始于 20 世纪 60 年代末，70 年代迅速增长，80 年代形成威胁。随着计算机应用的日趋广泛和社会化，国际上正掀起计算机犯罪的高潮。美国每年计算机犯罪发案率增长 400%，英国每年计算机犯罪增长率为 213%。一些发达国家每年因计算机犯罪造成的直接经济损失，美国超过 100 亿美元，德国约为 50 亿美元，英国为 30 亿美元，法国为 100 亿法郎。

在我国，自 1986 年发现首例计算机犯罪以来，1988 年至 1989 年发生计算机犯罪案件 9 起，1989 年至 1990 年发生计算机犯罪案件上百起，1993 年计算机犯罪案件为 1000 多起，1994 年为 1450 多起，20 世纪 90 年代后期，计算机犯罪的发案率成直线上升趋势。

计算机犯罪的形式分为两大类：暴力和非暴力。

针对计算机本身而实施的暴力形式的犯罪，在刑法上，破坏计算机硬件的犯罪是作为毁坏财物行为或其他行为论处的。

而非暴力形式的计算机犯罪是当今社会上最常见的，可分为：

(一) 以计算机为工具而实施的犯罪

在这种情况下，计算机只是一种作为犯罪的工具，而不是目的，犯罪行为本身仍然是传统意义上的犯罪，如利用计算机贪污、诈骗等，涉及到大部分社会犯罪现象，换言之，除凶杀、强奸、伤害和其他对人的犯罪活动无法通过计算机直接进行外，计算机犯罪几乎包括所有的犯罪形式。在定性上，这种犯罪不是一个独立的罪名，《刑法》第二百八十七条作出了以计算机为手段的犯罪的提示性规定：利用计算机进行金融诈骗、盗窃、贪污、挪用公款、窃取国家机密或者其他犯罪的，依照本法有关规定定罪处罚。

(二) 针对计算机储存的信息、情报、资料、数据而实施的犯罪

当今社会是计算机普及的社会，一些高效率的国防系统、尖端科学领域和商业机构大都将重要的情报和数据存入计算机系统，这已成为各国间谍偷窥的目标。犯罪分子以各种秘密手段非法侵入竞争对手的计算机系统，窃取系统中的重要数据和信息，以达到发展自己，挤垮对手，或倒卖他人有用的信息牟取暴利的目的。

20 世纪 90 年代以来，国际互联网在世界各国得到了迅猛发展。信息网络国际化、社会化、开放化、个人化的特点使国家的“信息边疆”不断延伸，甚至到了每一个上网的个人。全球信息高速公路的开通，计算机技术的飞速发展，将对整个社会的科学技术、经济文化带来巨大的推动与冲击，同时也引发出许多意想不到的问题。国际上围绕信息的获取、使用和控制的斗争愈演愈烈，信息安全成为维护国家安全和社会稳定的一个焦点。

众所周知，我国在计算机犯罪预防方面下了很大的力气，包括制定相应的法令法规；建立健全的管理制度；大力发展安全技术，研制开发和推广使用计算机安全技术产品；加强监督检查，制定行业标准，加强对安全产品市场的管理以及狠抓计算机安全教育，等等。这些举措可能短时期内不会取得什么效果，但这对规范我国的计算机安全制度，降低计算机犯罪带来的危害，有效地打击计算机犯罪活动都有着不可估量的作用。

信息安全的概念在 20 世纪经历了一个漫长的历史阶段，20 世纪 90 年代以来得到深化。从信息的保密性，拓展到信息的完整性、信息的可用性、信息的不可否认性。计算机的安全性历来是人们讨论的主要话题之一，而预防和打击计算机犯罪则是公安机关公共信息网络安全监察部门研究的重要课题之一。预防和打击计算机犯罪需要“攻、防、测、控、管、评”等多方面的基础理论和实施技术。

计算机应用事业方兴未艾，公共信息网络安全监察任重道远！

目　录

第一章　计算机犯罪概论

第一节　计算机犯罪的概念

计算机犯罪是20世纪五六十年代由信息科学技术发达的西方国家最早提出来的，并逐步被世界各国所接受和采用。

计算机犯罪(Computer crime)，作为一个概念是在计算机犯罪不断产生的过程中形成的，是计算机犯罪发展到一定阶段的产物。

所谓计算机犯罪，是指通过计算机非法操作所实施的危害计算机信息系统（包括内存数据及程序）安全以及其他严重危害社会的并应当处以刑罚的行为。

纵观世界各国，有关计算机犯罪的定义，大体分为广义说、狭义说、折衷说。

一、广义说

根据对计算机与计算机之间关系的认识来界定计算机犯罪,所以也称关系说。持广义见解者认为，所谓计算机犯罪，泛指与计算机技术、计算机系统有关，或与计算机数据处理有关的犯罪行为。换句话说，凡是以计算机作为犯罪工具，或以计算机为犯罪目的的所有犯罪行为，都是计算机犯罪。

较典型的有相关说和滥用说。

二、狭义说

持狭义见解者认为，计算机犯罪是指与计算机数据处理有关的故意违法的财产破坏行为。

三、折衷说（或工具对象说）

目前，定义中折衷说占主流。折衷说认为，计算机本身是作为犯罪工具或作为犯罪对象出现。在理论界，折衷说主要形成两大派别，即功能性计算机犯罪定义和法定性计算机犯罪定义。

综上所述，无论是广义的或是狭义的计算机犯罪的定义，都各有其偏颇。广义的计算机犯罪的定义，范围相当广泛，凡是在计算机领域中发生的犯罪行为，均属计算机犯罪。反之，狭义的计算机犯罪的定义，将计算机犯罪仅限于财产破坏，又使计算机犯罪

的范围显得过分狭窄，所以说，狭义的计算机犯罪的定义是无法涵盖全部的计算机犯罪的。

以上是国际上对计算机犯罪定义的不同观点。总之，“计算机犯罪”一词在国际上普遍使用，似乎已经成了一个惯用词，最终会有一个较统一的定义。

第二节 计算机犯罪的起因

计算机犯罪的产生与变迁，有极其复杂的背景，并且与计算机技术的发展紧密相关。一部“计算机犯罪史”，其实就是一部计算机发展的历史。

一、电话网络的发展，诞生了计算机犯罪的先驱

1876年，亚历山大·格雷厄姆·贝尔（Alexander Graham Bell，1847—1922）发明了电话。1904年，电话网络已布满美国全境。1907年，电话作为一种技术应用设备走进了千家万户。然而，自从电话网络开始具有生财能力开始，就有人非法利用各种电子装置，做到不付钱打电话。电话窃贼的鼻祖约翰·德雷普，偶然发现用CaptainCrunch为名的麦片盒中附赠的哨子（这是为了鼓励消费者购买而特设的奖品）能发出2600赫兹频率的音调，把它对着电话听筒吹，哨子的音调会使中心电话线路自动接出一根长途线。多年来他一直四处云游，向人们宣扬制造和使用“蓝匣子”的经验。20世纪60年代~70年代，伍兹和乔布斯在约翰·德雷普发明的基础上，对“蓝匣子”的技术性能做了进一步的改进。电话窃贼常常使用伍兹和乔布斯制造的高性能的“蓝匣子”，盗窃电信服务，欺骗电话公司的记账系统。后来“蓝匣子”有了升级换代的产品，颜色也不再局限于蓝色，并且自成系列。20世纪70年代初期，电话窃贼活动达到顶峰。

诚然，以上的行为称不上什么严格意义上的计算机犯罪。但电话窃贼的出现，我们可以把他们看成是计算机犯罪的先驱。

二、早期计算机技术管理上的桎梏诱发了计算机犯罪现象的出现

纵观计算机的发展历程，正是由于早期计算机技术管理上的桎梏，从而诱发了一群不安分守己的天才——黑客的出现和存在，并促使计算机的制造和应用技术得到了飞速的发展。

自1945年世界上第一台计算机爱尼亚克诞生以来，计算机经历了以电子管、晶体管、中小规模集成电路和超大规模集成电路为特征的四个发展历程。在计算机开发过程和使用的早期，由于计算机的生产企业，将其主要的精力放在开发价格昂贵、体积庞大、使用不便的大型机上，操作中实行严格的等级制度和中央控制，设备只能由受过专门训练的极少数技术人员操作。这种严格的近似无情的管理模式，引起了当时相当一批不安分守己的天才们的不满。他们崇尚技术，反对权威，冲破限制，最大潜力地对计算机系统

进行智力上自由探索，开创了计算机历史上犯罪的先河。

三、20世纪60年代美国社会的现状促进了计算机犯罪群体的诞生

20世纪60年代后期，一场反主流文化浪潮革命席卷美国大地。

布兰德、富勒、麦克卢恩和其他一些人的理论在反主流文化的青年中引起巨大的反响。嬉皮士运动所提倡的自治主义与民主观念奠定了个人计算机革命的基石。黑人争取民权的“自由乘客”运动在美国南部引起骚乱。同时，几乎所有的美国大学都经历了一场洗礼：现存的价值观和制度受到怀疑和挑战，人们反叛一切，寻求着通往新的社会和谐的道路。大学里爆发了大规模的反战运动，越来越多的年轻专业技术人员发誓，工作时不与军方有任何来往。在学生和知识分子中，涌动着一股对公认的各种思想形态的强烈不满。嬉皮士的队伍日益兴盛。摇滚乐和麻醉剂，被当成拯救千疮百孔的救星。并以其特有的魅力征服了一大批追随者。

20世纪60年代的嬉皮士们一度谴责电脑是集权控制的象征，然而他们中的一小部分人很快就意识到电脑更深层的潜能：它将是飞向自由的魔毯。在计算机上，他们找到了通向未来的道路。在此，他们惊讶地发现：个人计算机所将要造就的境界，与摇滚乐、迷幻剂一样，使人们不再受到工业社会清规戒律的羁绊。“这一代人一口吞下了计算机，就像他们一口吞下了迷幻剂一样。”一批新的计算机黑客开始崭露头角，在他们手里，信息技术最大限度地成为民主的工具。他们定期聚会，交流各自的攻击心得体会和经验，并印发自己的刊物，形成了一个藐视社会、藐视法律，向社会、向法律挑战的群体。

四、因特网技术的飞速发展加速了计算机犯罪群体的扩大

最初，因特网仅用在美国致力于防御研究的院校和机构的少数工作人员，主要用于文书传送。而今，它的用途非常广泛。成千上万的公司为那些快速增长的拥有个人电脑和调制解调器(Modem)的家庭用户提供联接，通过与因特网服务商(ISP)，如计算机服务、德蒙网及与许多别的公司达成的协议，个人电脑用户可阅读内部电子公告栏或公共的因特网信息(最流行的是万维网)。

因特网，不但吸引了许多家庭用户，同时也吸引了许多商业机构，据估计现有可达3亿多用户使用因特网。在用户增加的同时，因特网的内容也在变化，从完全由字符组成的电子邮件或信息公告栏的文章，又变成由图表、声音和图像组成的新形式。因特网许多有趣而且有价值的方面，吸引了越来越多的人。其中，计算机攻击技术也越来越多的在因特网上出现，从而为计算机犯罪群体的发展提供了及时、迅速的技术支持。

第三节 计算机犯罪的特征

计算机犯罪有许多与传统形态犯罪不同的特征，其中最重要的有专业性与业务性、

复杂性与隐秘性、作用时间长、毁灭证据容易、侦查与取证的困难性、运用智力作案，等等。下面分别介绍计算机犯罪的特征：

一、专业性与业务性

计算机犯罪中的主要犯罪行为，如：程序操纵、窃用计算机、计算机间谍等。行为人必须具备与计算机有关的专业知识，尤其是突破安全系统的防护，需要有相当的计划、耐心和能够破解防护机制的智力，才能实施其犯罪行为，所以说计算机犯罪具有专业性。

计算机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、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。

二、复杂性与隐秘性

计算机犯罪的复杂性主要表现为：第一，犯罪主体的复杂性。任何犯罪分子只要通过一台联网的计算机便可以在电脑的终端与整个网络合成一体，调阅、上传、下载、发布各种信息，实施犯罪行为。而且由于网络的跨国性，犯罪分子完全可来自各个不同的国家、地区、民族，网络的“时空压缩性”的特点为犯罪集团或共同犯罪提供了极大的便利。第二，犯罪对象的复杂性。计算机犯罪就是行为人利用网络所实施的侵害计算机信息系统和其他严重危害社会的行为。其犯罪对象也是越来越复杂和多样。

计算机犯罪的另一特征是隐秘性，不易被人觉察。由于计算机系统有安全系统的防护，及软件工程上资料形态的多元化，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。往往有这种情况，犯罪行为已经发生并记录于软件的资料中，但对计算机的运行却毫无影响，从外表看也没有什么变化，这就使得受害人很难觉察犯罪行为的发生。

三、行为人的持续性

计算机犯罪具有相当高的重复犯罪的可能性，行为人第一次得逞后，很少立即被人发现，通常会重复犯罪一直到被发现为止。

四、行为时与结果时的分离性

有些计算机犯罪，犯罪行为实施的时间与行为发生作用而造成结果的时间，具有相当的时间差。比如，逻辑炸弹，行为人可设计犯罪程序在数月甚至数年之后才发生破坏作用。所以说，有的计算机犯罪，具有行为时与结果时的分离性。

五、侦查与取证的困难性

计算机犯罪由于计算机处理的数据量大、毁灭犯罪证据容易、涉及个人隐私资料或商业秘密等原因，从而增加了侦查与取证的困难性。由于网络的开放性、不确定性、虚拟性和超越时空性等特点，使得计算机犯罪具有极高的隐蔽性，增加了计算机犯罪案件

的侦破难度。据调查，已经发现的利用计算机或计算机犯罪的仅占实施的计算机犯罪或计算机犯罪总数的5%~10%，而且往往很多犯罪行为的发现是出于偶然。

六、社会危害性大，损失严重

计算机犯罪的社会危害性大小，取决于计算机信息系统的社会作用的大小，取决于社会资产计算机化的程度和计算机应用普及的广度。计算机信息系统的社会作用越大，社会资产计算机化的程度越高，计算机应用普及的范围越广，发生计算机犯罪案件的概率就越高，计算机犯罪的社会危害性也就越大，这一点是国际计算机安全专家们一致的观点。

计算机犯罪始于20世纪60年代，80年代形成威胁。计算机犯罪的危害性远非一般传统犯罪所能比拟，不仅会造成财产损失，而且可能危及公共安全和国家安全。据美国联邦调查局统计测算，一起刑事案件的平均损失仅为2000美元，而一起计算机犯罪案件的平均损失高达50万美元。据计算机安全专家估算，近年因计算机犯罪给总部在美国的公司带来的损失为2500亿美元。另外，计算机犯罪与社会经济管理活动关系最密切，而且大多数犯罪属财产犯罪，牵涉的金额的数目都相当大。计算机高精功能和使用的重要场合，决定了一旦被非法利用则常导致巨大经济损失. 也会给社会管理和各项制度以及社会安定带来威胁。

正是由于计算机犯罪的社会危害性如此之大，许多国家的领导人和计算机安全专家担心，对计算机犯罪问题处理不当，会对国家和整个社会造成大规模的破坏。从近年来，一些国家计算机病毒大肆蔓延的事实来看，已经充分证明了这种担心完全不是多余的，而是各国所面临的现实问题。这正如帕克所指出的："计算机犯罪是一个世界性问题，因为凡是有计算机的地方都会发生计算机犯罪。"因此，我们必须对计算机犯罪进行分析与研究，从而找出预防计算机犯罪的策略和根治计算机犯罪的方法。

第四节 计算机犯罪的类型

综观计算机犯罪，其类型大致有计算机侵入、信息盗用和窃取、信息攻击和破坏、信息污染和滥用、信息欺诈和勒索几种。

一、计算机侵入、信息盗用和窃取

（一）计算机侵入

侵入计算机系统，目的不在于盗用、破坏或间谍活动，而只是为了寻求攻破技术安全措施的乐趣。实际上，这类犯罪活动经常发生，就损害而言，必须进行具体分析。在大多数情况下，受到侵犯的计算机用户实际没有受到损害，只是遭遇到危险。在任何情况下，有关的计算机系统的完整性和秘密性总是遭到破坏。我国也发生过若干起侵入重

要计算机信息系统的案件，虽未造成任何损害，但对计算机系统的安全性带来了影响。并且电话、电信技术的新发展使得当今“侵入”不仅影响到计算机系统，还越来越涉及到通信系统。

（二）信息盗用

最初出现的与计算机有关的经济犯罪可称为信息盗用，主要指业内人员利用其工作的方便条件盗用用户的账号密码以及系统管理员的特权密码，从而改变公、私财产所有权的违法或犯罪行为。在典型的盗窃案中，主要表现为盗窃可用以支付的电子货币、账单、银行账目结算单、清单等。

（三）信息窃取

在计算机系统中，大量的数据存储在狭窄的空间，使用现代技术和数据通信可以既快又方便地拷贝下来，这就使得信息窃取成为一种危险的犯罪。窃取的主要对象针对计算机程序、研究或实验数据、商业活动数据、客户地址，甚至是国家或军事的机密数据。作案方式一般是突破系统的安全防线后，作简单的拷贝，但偷窃数据载体、分析“剩余数据”、截收电磁辐射、窃听通信线路等也是信息窃取的内容。由于数据处理和电信的结合，电信网络数字化，在电话窃听中，普遍采用通过数据线侵入交换机，或者无线电微波通信，甚至卫星线路，故若不使用加密通信，这些都可以成为信息窃取的作案场所。

二、信息攻击和破坏

在这类犯罪行为中，绝大多数是属于非暴力性手段，即其攻击和破坏的主要对象是计算机程序或数据。

随着计算机网络的不断发展，以计算机病毒的方式进行信息攻击和破坏的现象十分严重，已成为当今的一大社会公害。据不完全统计，目前，全世界已发现的计算机病毒近 4000 种，著名的如“黑色星期五”、“米开朗基罗”等，都曾造成过世界性的恐慌，其所造成的损失根本无法估量。我国也于 1989 年首次发现计算机病毒感染，并出现了国产病毒，如“中国病毒一号”、“中国炸弹”等。

以黑客手段，非法侵入或攻击计算机网络。目前，在我国负责提供国际互联网接入服务的单位，绝大部分都受到过黑客的攻击或侵入。1996 年，由于黑客的“造访”，全球范围内，主要的银行和大公司损失了大约 8 亿美元。如世界上第一个将黑手伸向军用计算机系统的美国 15 岁少年米尼克，运用破译电脑密码的特殊才能，成功地打入了“北美防空指挥中心电脑系统”，并将美国瞄准前苏联的核弹头绝密资料一览无遗。在中国，由于黑客的“光顾”，给国家和集体也造成了巨大的财产损失。

三、信息污染和滥用

计算机犯罪中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、滥用信息技术等方面的犯罪行为已越来越突出，成为一种全球性的威胁。这些信息污染和滥用现象，有的出自于政治目的，如境外敌对组织和敌对分子利用国际互联网向境内散布政治谣言，进行非法宗教宣传等危害国家安全的活动等；有的是出于