

主 编 蒋 平

副主编 陆 娟

计算机犯罪 与电子取证研究

计算机犯罪基本概念
计算机犯罪现状与趋势
中国计算机犯罪状况
计算机犯罪案件侦查
计算机犯罪与电子取证



社会科学文献出版社
SOCIAL SCIENCES ACADEMIC PRESS(CHINA)

主 编 蒋 平

副主编 陆 娟

计算机犯罪 与电子取证研究

图书在版编目(CIP)数据

计算机犯罪与电子取证研究 / 蒋平主编. --北京:
社会科学文献出版社, 2018. 1

ISBN 978 - 7 - 5201 - 1739 - 5

I. ①计… II. ①蒋… III. ①计算机犯罪 - 证据 - 数
据收集 - 研究 IV. ①D918

中国版本图书馆 CIP 数据核字(2017)第 273134 号

计算机犯罪与电子取证研究

主 编 / 蒋 平

副 主 编 / 陆 娟

出 版 人 / 谢寿光

项目统筹 / 许春山

责任编辑 / 王珊珊

出 版 / 社会科学文献出版社·教育分社(010) 59367278

地址: 北京市北三环中路甲 29 号院华龙大厦 邮编: 100029

网址: www.ssap.com.cn

发 行 / 市场营销中心(010) 59367081 59367018

印 装 / 北京季蜂印刷有限公司

规 格 / 开 本: 787mm × 1092mm 1/16

印 张: 14.5 字 数: 182 千字

版 次 / 2018 年 1 月第 1 版 2018 年 1 月第 1 次印刷

书 号 / ISBN 978 - 7 - 5201 - 1739 - 5

定 价 / 42.00 元

本书如有印装质量问题, 请与读者服务中心(010-59367028)联系

▲ 版权所有 翻印必究

序

计算机、信息网络的迅速普及以及我国信息化的快速发展，引领了政治、经济、文化和社会生活各个领域的变革，给我国社会注入了巨大活力。同时，在信息活动领域中，利用计算机信息系统或计算机信息技术作为手段，或者针对计算机信息系统以及网络安全，实施各种破坏甚至犯罪的现象也不容忽视，各类层出不穷的计算机犯罪、网络攻击与破坏、信息窃密等事件，已经成为严重影响国家安全、社会稳定、经济发展的重要因素之一。

研究小组相关作者自 1995 年以来，围绕计算机犯罪与电子取证展开了多方位的研究，相继开展了一系列讲座，并发表了一系列文章，现结集出版，意在向广大研究者和学术界提供一些目录性、连续性和渐进式的资料参考，也从一个侧面反映我国在相关领域的研究缩影。全书包括五部分内容：计算机犯罪基本概念、计算机犯罪现状与趋势、中国计算机犯罪状况、计算机犯罪案件侦查、计算机犯罪与电子取证。其中有些文章由于发表时间较早，观点略显陈旧，资料略显单薄，方法略显单一，但为了保持原貌，本次结集未做较大修改，请专家学者和各界人士批评指正。

编者

2017 年 6 月

计算机犯罪基本概念	/ 001
计算机犯罪概念的演变与理解	/ 003
计算机犯罪初探	/ 012
计算机犯罪的“黑数”及统计差异	/ 022
计算机犯罪的类型探讨	/ 028
计算机犯罪现状与趋势	/ 037
国外计算机犯罪的现状	/ 039
计算机犯罪趋势分析	/ 048
中国计算机犯罪状况	/ 057
我国计算机网络犯罪的基本现状	/ 059
我国计算机犯罪的状况分析	/ 067
中国与世界主要发达国家计算机犯罪的比较研究	/ 077
计算机犯罪案件侦查	/ 105
计算机违法犯罪的立案	/ 107
论计算机犯罪案件的管辖分工	/ 119
计算机犯罪的类型及侦查策略初探	/ 127
利用信息网络实施寻衅滋事犯罪的限制解释	/ 138



网络游戏赌博法律适用问题分析	/ 151
浅析网络违法案件的分类及网络诽谤案件的调查取证	/ 163
计算机犯罪与电子取证	/ 173
电子证据的形式效力及认定	/ 175
电子证据的收集与保全	/ 186
电子证据的发展历程及应用思考	/ 203
后 记	/ 227

计算机犯罪基本概念

这部分内容整理了计算机犯罪基本概念方面的研究成果，共收集了四篇文章：《计算机犯罪概念的演变与理解》《计算机犯罪初探》《计算机犯罪的“黑数”及统计差异》以及《计算机犯罪的类型探讨》。

以上文章介绍了计算机犯罪的概念、类型及特点等，讨论了计算机犯罪“黑数”问题，指出只有有针对性地制定防范和打击计算机犯罪的策略，才能有效地预防犯罪，及时打击犯罪。



计算机犯罪概念的演变与理解

计算机犯罪在国外已有几十年历史了，但在我国却是近年来才出现的一种新的犯罪形式。从1986年深圳市公安机关侦破第一起利用计算机盗窃储户存款案以来，全国各地公安机关立案侦查的计算机违法犯罪案件数量不断增加。因而，国内学术界、司法界以及新闻界围绕计算机犯罪的概念问题进行过激烈的争论，有的从逻辑上判定“计算机犯罪”根本不成立，因为计算机是物，不能成为犯罪主体，何以犯罪；有的从刑法学角度上判定我国没有典型意义上的计算机犯罪，因为《刑法》上没有明确的界定条款（1997年《刑法》修订之前）；有的从犯罪学角度认为计算机犯罪比比皆是，因为随着计算机的普及，各行各业都会涉及计算机，即使没有直接联系，也有间接关系。以上这些观点都有其合理之处，但是他们只看到了计算机犯罪的一面。那么，究竟应当如何全面理解计算机犯罪的概念呢？在此，笔者想发表一管之见。

一 计算机犯罪概念的演变

现代计算机起源于军事应用，因而最早的计算机犯罪发生在军事部门，且与计算机充当什么角色、担负什么作用有关。例如，如果计算机是用来处理军事信息的，那么犯罪的目标就可能是泄密、窃密等。由于军事部门是各国重要的机密机构，即使发生犯罪案件也不会公之于众，所以我们很难找到最早的计算机犯

罪案件记录。同时，从法律的角度来看，计算机在犯罪的实施过程中充其量是工具和对象，不可能是犯罪主体，因而在计算机犯罪的早期阶段，也不可能被当成一类独立的犯罪来看待。

从 20 世纪 50 年代起，计算机应用开始由军事部门向金融、政府、科研等领域辐射。金融领域是金钱和财富最为集中的地方，因而在该领域利用计算机诈骗钱财就成了计算机犯罪分子的首选目标。英国计算机安全专家阿德瑞·诺曼（Adrian R. D. Norman）在《计算机不安全》一书中详细介绍了 1953 至 1982 年世界各地发生的 107 起“计算机不安全事件”，其中被作者划为“犯罪类”的案件共 67 起，而诈骗案件就有 44 起，约占 66%。

截至 1993 年，作为英国最主要的信息发布机构之一的审计委员会（Audit Commission）发布了四份关于计算机犯罪的报告，每一份公布的都是三年内英国的计算机犯罪情况。第一份发表于 1982 年，公布了 1978 至 1981 年英国的计算机犯罪情况；第二份发表于 1985 年，公布了 1981 至 1984 年英国的计算机犯罪情况；第三份发表于 1987 年，公布了 1984 至 1987 年英国的计算机犯罪情况；第四份发表于 1991 年，公布了 1987 至 1990 年英国的计算机犯罪情况。第一、二份报告的标题为“计算机诈骗”，从第三份起标题改为“计算机诈骗和滥用”。因而，英国早期的计算机犯罪概念基本上是指利用计算机进行诈骗活动。英国审计委员会从刑事法律的角度将其界定为“任何试图通过计算机获取钱财的诈骗行为”，并将利用信用卡骗钱也列入其中。英国审计委员会还进一步确定了计算机犯罪可能经历的三个阶段，即输入诈骗、输出诈骗和程序诈骗。

与此同时，欧盟也对计算机犯罪进行了界定，即“输入、修改、删除或隐藏计算机数据或程序，干扰数据处理过程，由此影响数据处理结果，达到为自己或他人谋求非法利益而使别人受到

经济或财产损失的行为”。

20世纪80年代中期以后，随着个人电脑的发明及电脑性能的不断提高，计算机的应用领域不断扩大，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、方式以及手段都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遇到了很多困难。因而，有的学者和执法人员提出了“电脑滥用”的概念，认为“电脑滥用”就是计算机犯罪。

20世纪90年代，互联网飞速发展。计算机网络的发展使计算机犯罪概念逐步演变为网络犯罪或信息犯罪。利用网络窃取国家政治、军事以及商业秘密，销售毒品，传播黄色淫秽物品，侵犯知识产权和个人隐私以及洗黑钱等，都逐渐增多。美国于1996年夏天成立了一个专门委员会，以对付网络上的计算机恐怖分子。德国要求互联网接入服务提供者禁止传播有关性和新纳粹的材料。新加坡政府要求网络接入服务提供者对涉及性、宗教和政治的内容进行审查，以掌握包括对书籍、电影和政治活动等加以限制的社会控制权。此外，在新加坡，一些政党在网上提供的信息内容也需要得到政府的许可，并不得与网络上传播的可能会引发宗教和政治动荡的材料的外来网点接通。中国香港也拟修订原有法律以管制计算机网络传送有害信息。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系统安全保护条例》，明确规定该条例的保护对象是联网运行的计算机。

由此可见，计算机犯罪有两个演变方向：一是由针对钱财的犯罪逐步向针对多领域的犯罪发展；二是由单机犯罪逐步向网络犯罪发展。

二 计算机犯罪术语的理解

计算机犯罪作为一个名词、一个术语，至少可以从三个角度

加以理解，即语法角度、法学角度及技术角度。从语法角度看，计算机犯罪在英语中有两种称谓，即 Computer Crime 和 Computer - Related Crime，我国一些译者将其统译为“计算机犯罪”。事实上，在英语国家中，这两个词所表达的意义基本相同，经常会被研究者和执法部门交叉使用。甚至在《国际犯罪政策概览——联合国关于预防和控制计算机犯罪手册》（*International Criminal Policy Review - United Nations Manual On the Prevention and Control of Computer - Related Crime*）中，这两个词也常被交叉使用。因而，在讨论计算机犯罪时，应尽量克服文字表述理解上的障碍，不要因文字表述不同而产生不必要的争议。例如，根据汉语翻译，可能会出现“计算机犯罪”“与计算机相关的犯罪”“计算机应用产生的犯罪”以及“计算机带来的犯罪”等多种翻译结果，并由此各执一词，自成一派，其实大可不必。至于有人从逻辑上判定“计算机犯罪”这个词用法不妥，认为计算机是物，不可能成为犯罪主体等，更不应该成为争论的热点。事实上，这只是一个约定俗成的问题，也是我国语言的一个特点，例如从前的许多典故后来都转为了另有所指的成语。此外，这个概念用词精练，已为多数国家所接受。

从法学角度看，计算机犯罪还具有法学上的含义。法学是一个覆盖面很广的学科，包括犯罪学、刑法学、刑事侦查学、犯罪侦查学、法医学、预审学等。因而，在研究计算机犯罪时，可以从多学科多角度加以考察。1997年3月14日重新修订的《中华人民共和国刑法》（以下简称《刑法》）在八届人大五次会议上通过后，从刑法意义上理解计算机犯罪已不成问题。但还需要从法学的其他分支和角度理解计算机犯罪，不能仅将研究视线放在《刑法》上，否则既不利于学术研究，也不利于打击和预防计算机犯罪。

从技术角度看，计算机犯罪是当前典型的高科技犯罪，研

究、打击与侦破计算机犯罪也必须使用相应的技术手段，需要高科技知识。尤其是在研究如何控制和预防计算机犯罪时，更需要高深的技术。因而，除了从社会科学角度理解计算机犯罪的概念外，还可以从技术角度对之加以讨论、研究。

三 计算机犯罪概念的表述

研究犯罪的角度很多，相应地对之进行界定的出发点和方法也很多，例如可以从刑法学、犯罪学、社会学、生物学、伦理学、人类学等角度研究和界定犯罪。同样，研究和界定计算机犯罪也是如此。笔者认为，正确区分和界定计算机犯罪在法律和技术层面上的概念，将有助于我们加深对计算机犯罪的认识，以制定预防、控制和打击计算机犯罪的策略。

四 刑法意义上的计算机犯罪概念

我国在1997年《刑法》修订前，实际上并没有刑法意义上的计算机犯罪概念，至于司法部门和学者们所做的界定和表述，只是根据当时的有关法律从学理角度进行的探讨。1997年《刑法》修订后，我国才有了真正刑法意义上的计算机犯罪概念。抽象地看，计算机犯罪就是我国《刑法》规定的应受刑罚处罚的犯罪行为。具体地说，凡触犯了全国人民代表大会于1997年3月14日修订的《刑法》（当年10月1日施行）第285条、286条规定的，就是计算机犯罪。

《刑法》第285条规定：“违反国家规定，侵入国家事务、国防建设、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286条规定：“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，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，影响计算机信息系统正常运行，后果严重的，依照第一款的规定处罚。”第 287 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。”由于第 287 条规定了利用计算机进行传统犯罪的，仍按传统罪名定罪量刑，因而《刑法》中实际用来惩处计算机犯罪的条款只有第 285 条和第 286 条。

最高人民法院在 1998 年发布的《关于确定犯罪罪名的司法解释》中，明确将《刑法》第 285 条和第 286 条的罪名分别概括为“非法侵入计算机信息系统罪”和“破坏计算机信息系统罪”。如果将这两个罪名进行刑法意义上的表述，可概括为：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罚处罚的危害社会的行为。简言之，即“侵入或破坏计算机信息系统的犯罪行为”。犯罪客体是社会管理秩序，直接客体是信息系统安全运行秩序；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；犯罪主体是以“白领”居多的一般主体；犯罪的主观方面是故意。

1998 年 10 月，设在天津港南疆港区的天津壳牌润滑油有限公司经理江某报案，称其所用的一部电脑上网费用由原先的每月 30 元，在半年里逐月猛涨，已达每月 6000 元，怀疑有人盗用其上网密码并无偿使用。经天津港公安机关立案侦查发现：1997 年 4 月，犯罪分子罗某根据网上“电脑黑客俱乐部”所传授的破译密码方法，破译了电脑网络公用区中出现的天津数字通信局的一个“用户目录文件”上显示的大量的用户字头和乱码中的十几个

密码，其中江某的密码上网操作最为简便，于是罗某将此密码告诉胡某，胡某又传给其他网友，如此“传销”式的传播，使江某的密码先后被 13 个人使用，给江某造成约 15 万元的损失。1999 年 7 月 29 日，重庆某大学计算机系本科生杜某编写了一个名为“病毒”的程序，这是第一起在国内编写“黑客”程序的案件。它本身属于“特洛伊木马”程序，再加上病毒，属于较严重的文件型电脑病毒，以邮件形式通过软盘和互联网传播。计算机被感染后往往无征兆即可突然被激活，硬盘中便会出现“火.YAI”文件，这种病毒破坏力和感染力较强。在这个案件中，杜某的行为是典型的故意制作、传播计算机病毒的犯罪行为。

五 犯罪学上的计算机犯罪概念

依据国内外犯罪学对犯罪的定义及我国对犯罪学的研究，参考国内外计算机安全专家对计算机犯罪的界定，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，并要考虑方方面面的因素。犯罪学上的计算机犯罪概念可表示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。

这个概念包括三层含义：①不明确实施犯罪的具体手段，只要是针对或利用计算机信息系统或所处理的信息所实施的犯罪，如擅自中断计算机网络或者信息通信服务等行为，都应划入计算机犯罪的研究范畴。2000 年 5 月，犯罪嫌疑人肖某在家中用黑客程序扫描并攻击某市 3 个网吧的计算机信息系统，致使这些网吧的计算机信息系统速度减慢，甚至死机，不能正常运行。1999 年 6 月 19 日下午，上海某信息网一用户登录到该单位邮件服务器，利用该服务器转发了 4000 封电子邮件，导致服务器严重过载，中断电子邮件服务两天。②对系统的非授权访问、存取及破坏其



功能、应用程序、处理信息、工作环节或网络部件等行为，应列入计算机犯罪研究范畴。比如毁坏计算机硬件、焚烧计算机机房等物理破坏。尽管对物理破坏的犯罪进行处罚可能只将其视为一般的财物破坏，定罪量刑也不考虑计算机因素，但首先它是从刑法角度认定犯罪的，与从犯罪学角度进行研究不矛盾；其次这类外表是毁坏计算机硬件设备的犯罪也可能与真正的计算机犯罪有直接的联系，如破坏现场、逃避打击等。如2000年9月，某市银行储蓄所发生火灾。大火扑灭后发现所内作为服务器用的计算机严重损坏。经查，大火原来是该所储蓄员利用计算机侵吞公款后为销毁证据而为。^③将目前看可能是一种误用或不良品行，但从长远看可能发展为对社会具有危害性的行为，也列入计算机犯罪的研究范畴，以便超前制定对策措施。如青少年上网浏览有害信息，或发布不实消息等轻微违法行为。

实际上，犯罪学上的计算机犯罪概念，不但是犯罪外延的横向扩大，而且是处罚程度的纵向延伸，既包括受刑罚处罚的犯罪行为，也包括受行政处罚的违法行为和受行政处分的违规违纪行为。

六 技术形态上的计算机犯罪概念

从技术角度讨论计算机犯罪，关注的主要是其技术手段。因而，计算机犯罪概念可表述为：凡运用计算机知识和技术实施的危害社会的行为，就是计算机犯罪。在欧洲，许多国家都非常注重技术形态上的计算机犯罪。从目前我国计算机违法犯罪情况来看，计算机犯罪是一种具有代表性的高科技犯罪，因而从技术形态上讨论和研究计算机犯罪，有助于研究计算机犯罪的技术手段，从而采取相应的技术对策。如根据美国学者帕克的“犯罪手段十七种类型”，我们可以有针对性地研究反计算机犯罪的十七

类技术对策。

以计算机安全技术作为参照物，我国已发生的计算机犯罪可分为以下四类：一是突破系统环境技术防范机制的直接或间接犯罪，包括非法进入机房操作计算机、利用技术设备拦截电磁信号、利用技术手段阻挡信息传输等；二是逾越访问控制机制实施各类犯罪，包括偷窃、猜测、绕过、闯过各类口令及防火墙和虚拟专用网（VPN）控制区；三是破译密码实施各类犯罪，包括截取、盗窃、破解各类算法；四是制造、传播或利用非正常程序实施犯罪，包括病毒、定时炸弹、逻辑炸弹以及其他非系统所需程序。

1999年6月17日，丹阳市某派出所接到某酒店报案称，该酒店电脑程序遭人破坏。经警方调查证明，该酒店电脑程序被南京某电脑技术员郑某破坏。6月2日，郑某以对电脑软件版本进行升级为名，进入该酒店微机房，并在电脑服务器上写入了一套破坏性程序。事后，郑某多次打电话给酒店，威逼酒店立即付款2万元，否则其设计的破坏性程序将于6月15日凌晨发作。酒店认为自己与郑某所在的公司无直接合同关系，故拒绝付款。6月15日凌晨，酒店电脑中的破坏性程序发作，导致系统内原始数据丢失，造成了严重的经济损失。

可以看出，如果能根据以上四种情况，有针对性地制定防范和打击计算机犯罪的策略，不但能有效地预防犯罪，也能及时打击犯罪。只有始终注意研究技术形态上的计算机犯罪，我们才能做到“魔高一尺，道高一丈”。

（作者：蒋平，本文原载于《信息安全》2002年第2期）