武汉大学刑法学博士文库

电子商务领域犯罪研究

皮　勇　著

武 汉 大 学 出 版 社

前　言

20 世纪 90 年代以来，以计算机及网络技术为核心的信息科学技术迅猛发展，并被广泛应用于社会各领域，给人类社会以深远影响。电子商务是信息科学技术应用于经济领域的创造，是 21 世纪的新经济模式，由于它具有传统商务所不能比拟的优越性，引起世界各国的高度重视，各国把它作为本国经济发展战略的重要组成部分。电子商务在全球特别是在欧亚美洲国家迅速发展，对所在国乃至世界经济的稳定、持续增长产生重要影响。与此同时，计算机信息技术这把“双刃剑”也为一种新的犯罪——电子商务领域犯罪创造了条件，在不长的时间内，电子商务领域犯罪迅速发展起来，严重威胁着电子商务的安全。必须说明的是，在我国刑法分则中没有电子商务领域犯罪这样一类犯罪或者个罪，电子商务领域犯罪不是刑法规范意义上的类罪名或者个罪名，而是在信息时代电子商务应用中出现的、具有某些共同特性的诸多犯罪的集合。由于它对电子商务这种重要的经济活动构成严重威胁，因此，有必要作为一类犯罪进行专门研究，探索遏制这类犯罪的对策，为我国电子商务的发展提供安全保障。

近十余年来，计算机犯罪越来越严重，引起了各国刑事立法、司法及理论研究工作者的高度重视，已有相关论文、专著发表和出版，而专门讨论电子商务安全与犯罪的论文非常少，论著至今未见面世。作者认为，电子商务领域犯罪是发生在电子商务领域的一类特殊的计算机犯罪，它既具有计算机犯罪的一般特征，同时具有自身的特殊之处，把电子商务领域犯罪从计算机犯

罪中剥离出来，进行专门研究，既有利于计算机犯罪研究的具体化和深入发展，又能配合正在进行中的我国电子商务立法，解决电子商务安全与犯罪的立法问题。

基于以上考虑，本书首先从犯罪学的角度，研究目前国内外电子商务领域犯罪的发展态势，了解电子商务领域犯罪的整体特征，然后分析这类犯罪的犯罪人组成结构、犯罪心态、犯罪客观表现和犯罪被害人等方面的特征，并试图从犯罪学、社会学的角度分析其产生的原因和条件。另外，电子商务领域犯罪是一类高科技犯罪，其行为方式、犯罪方法与传统犯罪有很大差别，是目前司法界、理论界希望了解而缺乏了解的问题，这也是本书研究分析的重点。

仅靠刑法手段不能根除犯罪，但它是惩治预防犯罪的重要手段，刑法控制体系是否有力、有效，直接影响着遏制犯罪的效果。本书比较了英美德日等国关于电子商务领域犯罪的刑事立法，希望从中找到国外相关立法的成功经验，以为我国立法借鉴。电子商务领域犯罪给我国刑事审判工作带来的大量新法律问题，是本书研究的重点，其中，涉及电子商务领域的信用卡诈骗罪、侵犯著作权罪、侵犯商业秘密罪、诈骗罪、非法行医罪、盗窃罪、制作、贩卖、传播淫秽物品罪的刑事法律问题较多，较有代表性，而且，这些犯罪在电子商务领域犯罪中经常发生，表现得更突出。作者本着“学以致用”的思想，着重对以上犯罪在适用刑法时遇到的疑难问题进行研究，并提出相关立法建议。此外，本书还研究了危害计算机信息系统安全犯罪的司法及立法上的问题。

关于电子商务领域犯罪的对策，作者认为，电子商务是全球性的宏伟工程，要有效防治电子商务领域犯罪，制定对策时必须充分考虑电子商务领域犯罪的特点、我国电子商务发展及立法现状，从多个方面同时入手，多管齐下，相互协调配合，构建电子商务领域犯罪综合控制体系，包括技术控制、健全管理、完善立

法，以及加强公民网络道德和法制教育。本书着重研究我国电子商务在社会规范管理、刑事实体和程序立法以及司法实践等方面的状况，并提出相应的对策建议。

电子商务、电子商务领域犯罪是近几年发展起来的新鲜事物，它们带来的问题随着电子商务的发展不断增加和变化，这些问题对每一位研究者都是一个崭新的课题。作者试图在电子商务领域犯罪问题上作粗浅探讨，但受限于学识疏浅，在分析研究中一定会有不当之处，敬候读者指教。希望本书的出版能对刑法学界研究电子商务领域犯罪问题起到抛砖引玉的作用，对司法实践中处理这类犯罪有一定的参考价值，果能如此，我就十分欣慰了！

作　者

2001 年 11 月于珞珈山

目　录

第一章　电子商务及其发展中的问题

20 世纪 90 年代，计算机、网络技术等信息科学技术迅速发展，并得到广泛应用，社会生活各个领域的信息被大量发掘和应用起来，信息对人类社会产生了前所未有的影响，推动人类文明进入信息时代。电子商务是信息时代传统商务变革创生的一种新经济模式，必然对 21 世纪的人类社会产生深远影响。同时，由于电子商务安全及相关犯罪问题的时代性、特殊性，故研究它们不能脱离信息技术革命、信息社会这一特定的社会背景，只有了解信息技术的发展应用及其社会影响，了解电子商务这一新经济模式，才能正确认识电子商务安全和该领域的犯罪问题，进而寻找有效遏制的对策，保障电子商务正常发展。

第一节　计算机与信息时代

一、信息、信息交流及计算机信息技术的发展

从人类产生伊始，信息的生产、消费一直伴随着人类文明进步而发展，但是，人类对信息这一概念的认识却是一个漫长的过程，直到 1948 年信息论的创始人 C.E. 申农才提出信息论的科学范畴。然而，关于信息的概念，至今仍然没有一个统一的定义，不同领域的人有不同的定义，C.E. 申农认为，信息是两个不确定性之差，是信宿对信源的统计不确定性的消除或者减少的

量度；[①]，韦弗、维纳等其他信息论的奠基人也都把信息看做一种抽象的数学量。随着信息的广泛应用，信息这一概念的范畴也逐渐由自然科学领域扩展到社会生活和人类认识活动领域中。一般认为，信息反映的是处于不均匀状态的事物发展变化的运动形式，信息的内容能够揭示事物的属性和特征，如气象信息、市场行情信息、国家政局信息等等。

信息是事物运动状态的反映，具有客观性、普遍性、无限性、传播性、依附性、可计量性和共享性等主要特征，其中需要特别关注的是信息特殊的传播性、依附性和共享性。

信息特殊的传播性表现在，传播与信息密不可分，有信息就有传播，信息传播的速度决定于信息载体的传播速度和信息分享的程度，分享程度越高，载体传输速度越快，信息传播的速度就越快。反之，信息就会死亡。

信息特殊的依附性表现在，信息没有体积和重量，其生产、处理、将所有“存储”、传播、利用都依赖于信息处理、传输技术；信息必须依附于某种物质载体而存在，无法独立用于交流；信息的依附性是绝对的，同时也是相对的，同一信息可以有多种载体。

信息特殊的共享性表现在，同一内容的信息可以在同一时间和地点被两个或者两个以上的使用者利用，这是信息区别于实物和能量的主要标志。信息的共享得益于信息对载体依附的相对性和转换的便利性。

信息是客观世界的三大要素之一，对人类社会的生存和发展至关重要。信息可以消除认识的不确定性，增强人类认识和改造世界的能力，同时，人类在认识和改造世界的过程中，又在不断地生产信息和交流信息，信息生产的数量和质量以及信息交流的速度，在一定程度上反映了人类文明发展的程度。科学技术对信

① 周安伯等著《信息科学论纲》，江苏教育出版社1990年版，第11页。

息的生产和交流具有巨大的推动作用。按照信息交流方式的产生顺序以及所依赖的科学技术，可以把信息交流分为语言信息交流、文字信息交流、大众信息交流（以报刊为主导工具的大众媒体）和电子信息交流，与此相对应的分别是狩猎及采集经济时代、农业经济时代、工业经济时代和信息时代。信息时代是信息生产前所未有的丰富的时代，故被称做“知识爆炸”的时代，信息时代是信息交流前所未有的便利的时代，偌大的地球变成了“地球村”，信息时代还是信息载体前所未有的多样化的时代，文、图、声、影像、触觉等各种信息载体被应用起来。这一切都建立在以计算机、网络技术等信息技术的基础上。

20 世纪 40 年代微电子技术及其工业得到迅速发展，为电子计算机的诞生奠定了物质基础，当时正在进行中的第二次世界大战也急需高速、准确的计算工具，用以解决大量的弹道计算问题，军事上的紧迫压力加速了电子计算机的诞生。1945 年世界上第一台电子计算机 ENIAC 在美国研制成功，标志着电子信息处理工具的产生，从此计算机替代了一部分脑力劳动，人类社会活动开始摆脱人类脑力的限度而更加有效地运作起来。在不到半个世纪的时间里，微电子技术特别是集成电路技术和计算机软件技术发展极为迅速，电子计算机的体积越来越小，处理能力越来越强，操作越来越便利。这时计算机除了应用于科学计算领域外，还逐渐推广到社会生活各个领域，其中用于信息处理的计算机占半数以上，计算机已经脱离了早期“计算”的范畴。1977 年 IBM 公司宣布将跨入消费电子领域，着手开发个人电脑 IBM PC（Personal Computer）①，这是计算机应用的重大突破，从此计算机不再只是大机构所特有，而像彩电、冰箱一样进入普通家庭，用于人们日常工作、教育、生活、娱乐等活动相关信息的处理和存

① 尼葛洛庞帝著，胡泳译：《数字化生存》，海南出版社 1997 年版，第 136 页。

储。

计算机的发明、发展和广泛应用使信息大量产生，但是，在这一阶段信息交流仍然主要借助实物传输的渠道进行，这就不可避免地影响了社会信息交流的速度。信息交流的飞跃是人类文明迈进信息时代的最后一步台阶，这一步通过计算机网络技术的发展和应用来完成。由于军事上的需要，1963 年拉里·罗伯茨（Larry Roberts）设计了互联网络，并在美国军方的资助下建成 ARPA 网（ARPA net），其目的是为了在核战争爆发时，作战命令通过各种传输途径仍然可以传递到目的地。后来，ARPA 网转为民用，计算机网络技术在社会生活各个领域逐渐推广应用。计算机网络技术发展的时间不长，而发展却极为迅速，在不长的时间内国际互联网络延伸到世界各地，通过互联网络，信息在全球范围内以极快的速度传播开来。

在以上两项主要信息技术的推动下，信息社会逐渐呈现在人们面前。

二、信息社会及其特征

计算机、网络技术的结合不只是两项技术的简单相加，而是引发了一场伟大的信息技术革命，揭开了信息时代的序幕，奠定了信息社会的基础。1993 年 9 月美国克林顿政府推出举世瞩目的《国家信息基本设施》计划（National Information Infrastructure，简称 NII），它被形象地比喻为信息高速公路（Information Superhighway），随后，欧盟、日本、加拿大以及新加坡、韩国等国提出了本国的信息高速公路计划，巴西、阿根廷、乌拉圭等一些发展中国家也在加紧实施光缆传输网的铺设工程，我国于 1993 年 12 月成立了国家发展信息产业的决策机构——国民经济信息化联席会议，制定了《中国国家信息化基础结构发展纲要要点》。1994 年 9 月美国提出建立《全球信息基础设施》（Global Information Infrastructure，简称 GII）的倡议，1995 年 2 月西方

七国集团在布鲁塞尔举行“七国集团信息社会部长级会议”，会议提出建立《全球信息基础设施》的宏伟目标。第二次信息革命的浪潮以不可抗拒之势席卷全球，促使全球信息社会形成，推动人类文明逐渐进入信息时代。

人类社会何时迈入信息时代尚存在争论，但是人类文明已经进入信息时代，并且信息化程度不断提高则是人们的共识。借助于国内国际信息基础设施，信息社会组成极大地扩展，它不局限于国家疆域，而是在全球范围内构建。另一方面，信息社会组成对人类社会的影响不断加深，有力地影响着政治、经济、文化和科学等各项社会活动。

在政治领域，政治家利用互联网络向人们宣传自己的政治主张，争取选民支持，政府利用互联网络收集公民对政府的意见，公告政府的施政方针等。

在军事领域，军用计算机网络覆盖全球各地，甚至在大气层、太空都设立了计算机网络站点，一个全球警戒、反应迅速的军事指挥网络正在形成，它能够在第一时间内将战争信息传到战场各处，从而赢得战争主动权。

在经济领域，全球电子商务蓬勃发展，现代企业纷纷提出自己的网络经营战略，与网络相关的高技术股票为广大股民青睐。美国联邦储备委员会主席格林斯潘说，“美国企业在 IT 方面的投资导致了美国经济 9 年来的强劲增长”①。

参与网络生活的人数越来越多，并且增长迅速。据《电脑产业年鉴》报告《1990～2005 年互联网络用户展望》统计，互联网络用户从 1996 年的 6 100 万激增至 1998 年 1.47 亿，这一数字预计在 2000 年接近 3.2 亿，2005 年达到 7.2 亿②，我国的互联网络用户在 1998 年约 220 万，1999 年约 400 万，2000 年底则

① 《格林斯潘一锤定音》，《计算机世界报》，1999 年 5 月 31 日。

② 《全球上网人数增至 1.47 亿》，《深圳特区报》，1999 年 3 月 1 日。

突破 2 200 万人，上网计算机数约 892 万台。

计算机信息科技继续保持着迅猛发展的态势。计算机性能不断提高，计算机、网络技术时有突破，多媒体技术、虚拟现实技术等新技术层出不穷。同时，这些信息技术与其他领域科学技术结合，推动各领域科学的发展。在信息社会里不与信息技术结合的部门、行业是不可想象的，人们已经融入浩瀚的信息“海洋”。

信息社会具有三个主要特征：(1) 信息交流的广泛性。通过覆盖全球的互联网络，信息的交流不再受国家疆域和距离的限制。(2) 信息应用的深入性。随着社会信息化的深入，对各行各业而言，信息都是不可或缺的“空气”，影响着它们的生存与发展。(3) 信息形式的综合性。计算机技术使各种形式的媒体如图片、文字、声音、影像等，都可以转换为电子数据，并在互联网中同时传送，给用户以完整、全面的信息表现。

第二节 电子商务概述

一、电子商务的含义

什么是电子商务？国内外至今没有统一的定义，不同领域的专家从不同的角度界定电子商务的内涵和外延，这些定义大致可以划分为广义定义和狭义定义两种：

全球信息基础设施委员会电子商务工作委员会的报告草案对电子商务作了广义定义：电子商务是运用电子通信作为手段的经济活动，通过这种方式人们可以对带有经济价值的产品和服务进行宣传、购买和结算。电子商务的广义定义也可称为商业电子化，是指电信工具（包括电报、电话、传真以及互联网络等）在商务活动中的应用，依照这种定义，不仅包括 20 世纪 60 年代就已经产生的企业间电子数据交换，而且包括使用电报、电话、电传等电信手段进行的商贸活动，如电话购物、电视购物等等。

联合国经济合作和发展组织在有关电子商务的报告中对电子商务作了狭义定义：电子商务是发生在开放网络上的包括企业间、企业和消费者之间的商业交易，如通过互联网络进行的商品和服务买卖以及资金转账、公司间和公司内利用电子邮件（E-mail）、电子数据交换（EDI）、文件传输、传真、电视会议、远程计算机联网所能够实现的全部功能（如市场营销、金融结算、销售以及商务谈判）等。

笔者认为，电子商务是在信息基础设施上建立起来的一种新经济模式，不仅仅是少数企业营运的科技革新，而是对整个经济活动的一次变革，具有极广泛的参与者或者具有这一趋势。而具有这种广泛参与者的“电子商务”，是伴随国际互联网络的产生和广泛应用才逐渐形成，因此开放性数字信息网络在商务领域的应用是电子商务的基本特征，或者说，电子商务是建立在开放性数字信息网络上的经济活动，不具有这种特征的、利用电子工具从事的商务活动，只能列入电子工具辅助的传统商务一类，是传统商务向电子商务过渡的中间阶段。因此，笔者认为，狭义定义更加符合电子商务的现代特征，更具有现实意义。本书讨论的电子商务都是指狭义的电子商务。

需要指出的是，电子商务不仅包括在互联网络上进行购买业务和资金汇兑等直接带来利润的事务，而且包括支持利润产生的事务，如产生对产品和服务的需求、提供销售支持和客户服务、促进业务伙伴之间通信等，具体而言，电子商务涵盖的范围包括：商务信息交换、售前售后服务（提供产品和服务的细节、产品使用技术指南、回答顾客意见）、广告、销售、电子支付（电子资金转账、信用卡、电子支票、电子现金）、运输（包括有形商品的发送管理和运输跟踪以及计算机数据类产品的发送）、组建虚拟企业（如网络银行）等。电子商务交易的对象包括有形商品（如生产资料、生活消费品、专用医疗器械等）、无形商品（如计算机软件和数据库等计算机数据类产品）以及服务（如市

场需求调查、金融法律业务咨询、医疗保健、远程教育等)。

根据不同的标准，可以将电子商务进行以下分类：

1. 根据电子商务是否完全通过数字信息网络完成，可分为完全电子商务和不完全电子商务

所谓完全电子商务，是指整个商务交易活动都通过数字信息网络完成的一类电子商务。这类电子商务交易的内容一般是无形商品和服务，如计算机软件、音乐、音像节目等计算机数据类商品。另外，电子资金的划拨、专业信息服务等也可以完全通过数字信息网络完成。在完全电子商务中，交易信息和商品或服务完全通过网络传输，突破了传输距离带来的障碍，极大地扩展了商务交易的范围。

所谓不完全电子商务，是指商务交易的部分活动通过数字信息网络完成，而其余活动仍然需要通过传统商务方式完成。如在互联网上购买实物商品，如 CD 唱盘、书籍、机器设备等，除交货外的所有活动可以通过互联网完成，如为购买商品而进行的商品广告、商务洽谈、用户意见反馈、售后服务等。

2. 根据参与电子商务交易方的不同，可以分为商家与客户间的电子商务、商家间的电子商务

商家与客户间的电子商务是指电子商务交易方分别是商家和个人客户的电子商务。商家间的电子商务是指电子商务交易双方都是商家的电子商务。20 世纪 90 年代以来商家间电子商务迅速发展，占整个电子商务交易额的大多数。1999 年商家之间业务的“交易额达到了 1 450 亿美元，大大高于 200 亿美元的‘企业对消费者’的网上销售额。据马萨诸塞州福里斯特研究机构的保守估计，到 2004 年，企业对企业的电子交易额将上升到 2.7 万亿美元，而加特纳集团的相关预测比这更高，达 7.3 万亿美元”①。

① 唐永新：《迅速崛起的美国电子商务》，《科技日报》，2000 年 3 月 15 日。

二、电子商务的基本特征

电子商务建立在信息技术及信息基础设施基础上，与传统的商务形式相比，电子商务具有以下基本特征：

(1) 商务资料传递速度快。计算机数据在互联网络上能够在一瞬间传送到世界各地，极大地加快了商务信息的交流。如果利用互联网络传送计算机数据类产品或者专业服务信息，交易的商品能够即时传递给消费者。

(2) 联系范围广泛。电子商务是在互联网络上进行的商务交易，互联网络的覆盖范围也就是电子商务的覆盖范围。国际互联网络经过几十年的发展，已经覆盖全球绝大多数地方，而且仍在迅速扩展。广泛的互联网络把亿万企业和消费者直接联系在一起，为电子商务企业开拓出全球市场。

(3) 成本低廉。利用互联网络进行商务信息的交换和商品的传输，其营运成本要比利用邮政、普通电信服务、货物运输等传统商务手段低廉得多，降低了交易成本，增强了企业竞争的优势。

(4) 商务信息表现形式丰富。互联网络应用融合了计算机技术、网络技术、多媒体技术等多种信息技术，互联网络上的商务信息可以是文字、图片、动画、声音、影像等多种形式，使客户可以直观地浏览和选择商品。此外，在互联网络上还能够实现双向互动交流，商家能够在网上展示商品，提供有关商品信息的查询，和顾客做互动双向沟通，为消费者提供个性化需求服务。

(5) 科技含量高、自动化程度高。电子商务系统是一种分布式的信息自动处理传输系统，系统的功能通过管理程序事先设定，具体业务由计算机信息系统自动完成，一般无需人为干预或者很少干预，节约了大量人力、物力，提高了企业的生产经营效率。

三、电子商务的运作机制

(一) 电子商务活动的主体

电子商务种类很多，各类电子商务活动主体不完全相同，有

的电子商务参与主体较多，如网上销售，包括交易方、金融电子化结算机构、认证机构、网络通信服务商、交通运输商、政府机构等，有的主体较少，如电子资金划拨，参与主体只有金融机构、资金划拨客户、网络服务商、政府机构等。在这些电子商务活动中，有些机构是电子商务活动不可缺少的重要主体，如网络通信服务商、金融电子化结算机构、政府机构、交易方，有些是电子商务活动中具有代表性的主体，如认证机构、电子商务商户等，以下分别予以介绍：

1. 网络通信服务商

互联网络是电子商务的运作平台和活动空间，大量的商务信息和商品要通过互联网络来传输，网络通信服务商提供的网络通信服务是电子商务活动的基础。

2. 金融电子化结算机构

支付是电子商务不可或缺的部分。金融机构利用金融电子化结算系统处理业务和传输资金转账信息，实现了即时资金过户，非常适合电子商务应用的需要。我国网上银行业务发展迅速，目前国内各大金融企业都在发展金融电子化结算系统。

3. 政府机构

互联网络不是无国界的空间，电子商务仍要受本国工商、税务、海关等政府机关的管理，政府部门应该对电子商务提供正确的指导和服务，维护正常的电子商务秩序，保障电子商务顺利进行。同时，由于电子商务的特殊性，这些政府机构的相关业务要适用电子商务的特点进行调整。

4. 认证机构

电子商务认证是电子商务的关键。由于电子商务交易活动的虚拟性，交易双方不能直接了解对方的资信状况，不利于建立交易双方的信心，而电子商务认证机构（Certification Authority，CA，以下简称认证机构）就是为交易各方提供验证的机构，解决电子商务活动中交易方身份、资信的认定，维护交易活动的安

全，保障电子商务交易活动顺利进行。世界各国对电子商务认证机构的建设非常重视，我国认证机构建设也十分迅速，中国人民银行支付科技司组织工行、农行、建行等 12 家商业银行联合共建的中国金融认证中心（CFCA），于 2000 年 6 月正式开始运行，第一阶段将发放 SET 和非 SET 证书共 25 万张。

5. 电子商务交易方

电子商务交易方是电子商务活动的核心。他们大致可以分为电子商务交易企业和网上消费者两类，参与电子商务的企业一般必须向有关认证机构申请电子商务身份证，在网络金融结算机构开设用于电子商务交易的资金账户，有完备的从事电子商务交易的技术设备等。在我国电子商务发展比较快的城市，利用互联网从事经营活动的电子商务企业和个人，还要到工商行政机构申请电子商务营业执照①。

电子商务主体之间的关系如图 1-1 所示：

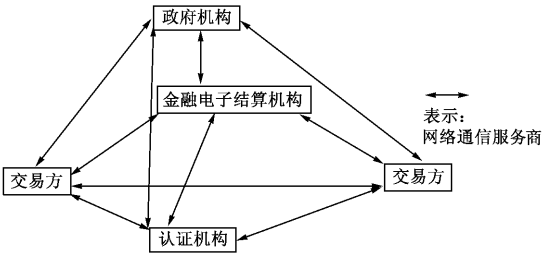

图 1-1

① 《上海：欲做网上生意　先亮网上执照》，《科技日报》，2000 年 8 月 31 日。

电子商务主体之间的关系体系宛如一个圆球壳体包围下的三角棱形。政府机构就是这个圆球壳体，如同包围在地球表面的空气层，它是电子商务领域的宏观调控者，负责制定电子商务发展政策和法律法规，从宏观上指导电子商务发展，并且通过各行政管理部门的管理和服务，实现对电子商务发展的调控，维护电子商务的正常运作。其他四个主体是电子商务活动的具体操作者，其相互之间的关系应该是独立民事主体之间的关系，其中交易双方的关系是这个关系体系的主体，一般表现为商品或服务的购销关系以及相关的其他关系。电子商务认证机构和金融电子结算机构为完成交易方提供认证和结算服务，它们与交易方的关系，依附于交易方之间已经存在或者预计要发生的民事关系。同时，电子商务认证机构和金融电子结算机构也保持着密切的联系，在业务处理上相互配合，如电子商务认证机构要向交易方的开户行咨询其资信状况，金融电子结算机构要等待认证机构确认交易方的资信，才能资金转账。

（二）电子商务的运作机制

电子商务包括多种经济活动，主要有网上销售业、互联网络广告业、网上服务业、网络金融证券业等，不同活动内容的电子商务涉及的主体不同，运作机制也有较大差异，以下简要介绍网上销售的运作机制。

网上销售是目前电子商务的热点之一，这种经营形式是把销售的全部或者部分环节通过互联网络来完成。网上销售的主体是销售商、客户、网络通信服务商、认证中心、金融结算机构和政府有关部门。进行网上销售，首先由网上销售商在网上建立销售网站，并通过一定的广告方式招揽顾客访问，网站提供销售商品的品质特性、价格等方面的信息，告知用户可以使用的支付方式，如信用卡或者其他网上支付工具。客户在网上浏览并确定要购买的商品、服务，然后填写电子订购表格，在支付表单中填入

网上支付的账户信息，所有这些数据加密后传输给电子商务认证机构和金融电子结算机构。认证机构完成电子商户的身份认证，并把确认信息返回给客户，客户根据这一信息决定是否进行支付。客户点击支付按键后，账户信息被传输到金融电子化结算机构。结算机构确认客户账户资金余额是否可以进行交易，如果判断为肯定，则向商户的计算机系统传送肯定信息，商户的计算机信息系统收到肯定信息后，向客户的计算机传送交易接受信息。如果以上有任何项目未获通过，则客户和商户的计算机将收到交易被拒绝的信息。最后，商户向客户提交货物，金融电子化结算机构将客户账户上交易的资金划拨到商户账户上，从而完成整个商品或服务交易。政府各部门根据自己的职责管理监督以上主体，如向商户和客户征税、接受客户投诉等。

四、电子商务的发展状况及其趋势

电子商务在全球范围内蓬勃发展，1999 年 5 月 17 日是“世界电信日”，主题是电子商务，1999 年因此被称为“电子商务年”。我国电子商务发展迅速，2000 年被国务院定为“电子商务管理年”。2001 年各国电子商务企业经历了一次淘汰，大批电子商务网站陷入经济困境甚至倒闭，电子商务经济一度萎缩。但这不能否定电子商务作为新经济模式的优越性，电子商务经过“网络泡沫经济”的洗礼后将更加成熟，必将重新获得迅速发展，成为新世纪经济浪潮的主导。这符合新生事物发展的螺旋式上升规律。纵观电子商务的发展，它表现出以下主要特点：

1. 发展速度极为迅速

电子商务发展时间不长，发展却极为迅速。有信息表明，1996 年全球电子商务市场的规模已达 1 500 亿美元，到 2001 年全球 10% 的商务将实现电子化，涉及到的商品与服务将达到 6 000亿美元。亚洲的电子商务到 2001 年将以 100 倍的速度增

长，营业额在各种销售渠道销售总额中将占有 42% 的份额①。我国电子商务虽然起步晚，但发展势头强劲，将成为上网人数最多的国家之一，上网用户每半年增加一倍，1998 年 12 月 31 日超过 210 万，1999 年 12 月 31 日超过 890 万，2000 年 12 月 31 日超过 2 200 万。虽然我国 1999 年电子商务交易额仅人民币 2 亿元，但后续成长力度及幅度将相当惊人，信息产业部表示，1999～2000 年是我国电子商务的起飞期，从 2002 年开始将步入快速增长期，估计到 2002 年将急速增至 100 亿元②。

2. 对经济发展有巨大的推动作用

由于电子商务具有传统商务不可比拟的优越性，对全球经济的发展具有巨大的推动作用。预计到 2002 年，全球因电子商务应用而节约成本将达 12 500 亿美元。在我国，与网络相关的信息产业成为增长最快的产业，1999 年全国通信业务收入完成 2 803亿元，比上年增长 24.6%，电子信息产品制造业实现销售收入 4 300 亿元，增长 22.7%，国内网上中文站点超过 1.5 万个。据互联网实验室（ChinaLabs.Com）的最新研究报告，1999 年国内互联网公司价值评估超过 1 亿元的网站已经超过 20 家，2000 年市场价值达 10 亿元以上的网站将超过 40 家——这表明电子商务惊人的发展速度和巨大的商业潜力。③

3. 发展分布不平衡

电子商务是一个全球性的系统工程，目前由于电子商务体系发展尚未完善，加之各国信息基础设施建设程度不同，全球电子

---

① 谭朴珍：《知识经济电子商务：一种全新的贸易形式》，《外向经济》，1998 年第 12 期。

② 《大陆电子商务市场潜力惊人》，《南方都市报》，2000 年 1 月 28 日。

③ 廖蔚蓉：《网络经济：国有企业直面挑战》，《科技日报》，2000 年 3 月 17 日。

商务发展很不平衡。根据美国一家市场研究公司的预测，2000年北美、欧洲和亚太三大地区的电子商务交易额将占全球电子商务总额的94%，这种局面近年内不会有大的改变。在公司间的电子商务方面，虽然欧美和亚太以外的地区也会有所发展，但电子商务比较普遍地扩展到全球的各个地区也许还要10年时间。

4. 对传统企业经营方式构成严重的威胁

在传统的生产经营模式中，生产商、中间商或批发商、零售商是传统经济流通的三个不可缺少的环节。随着网络的发展，全球成了网上的“地球村”，供求双方在网上直接交易，网上看样品、谈价格、签合同、支付货款，分布在全世界的网络神经系统能够超越中间环节获得正确的信息，电子商务不仅使传统的中间商、批发商的财路日益萧条，也给传统企业带来巨大的压力。根据Forrester Research的预测，到2004年，在2.7万亿美元的企业对企业商务中，电子商务市场将占53%的份额①。电子商务的迅速崛起，使越来越多的美国公司感到缺了它不行，并产生了一种紧迫感。据调查，约有60%的公司认为电子商务重要，而42%的公司甚至说，如果不搞电子商务，公司生存将会面临威胁②。英特尔公司总裁贝瑞特甚至认为，将来不上网的企业只能等死。

当今国家间竞争实质上是国家综合国力的竞争，其核心是经济实力。电子商务作为信息时代的新经济模式，是信息技术革命创生的新生产力，对经济的发展具有巨大的推动作用，是21世纪各国经济的发展趋势。发展电子商务对我国具有战略意义，它既是一次良机，也是一次挑战，我国应该克服信息基础设施落后等方面的困难，大力推进电子商务的发展，特别是要优先发展企

① 《电子商务侵蚀制造业利润》，《南方都市报》，2000年3月9日。

② 唐永兴：《迅速崛起的美国电子商务》，《科技日报》，2000年3月15日。

业间电子商务，推动我国企业经营向电子商务模式的转变，为增强综合国力构筑坚实的经济基础。发展电子商务是信息时代的一个崭新的课题，各国都没有可供参照的成熟范例，我国发展电子商务时间晚，技术、管理、法制基础较薄，但绝不能因此而延缓我国电子商务健康发展的进程，否则将留下历史性的遗憾，正如全国人大代表、北京大学教授、两院院士王选所说，任何产品、技术都要考虑到因特网，错过一段时间可以原谅，但最可怕的是错过一个时代①。

第三节　电子商务发展中的问题

和任何新事物一样，电子商务的发展会遭遇许多问题，主要有：一是安全保障问题，即保障电子商务系统稳定正常运作，不因自然力、事故和恶意破坏而严重影响系统的持续正常工作；二是法律规范问题，即制定法律法规、规章制度，规范电子商务活动秩序，规范什么是合法行为，什么是违法行为和犯罪行为，进而利用社会力量对违法行为进行谴责，对犯罪行为进行严厉打击，以保护电子商务活动的正常进行。由于电子商务发展时间短，各方面的配套措施还很不完善，电子商务尚在荆棘中探索前进。这里只讨论电子商务在法律规范方面的问题。

电子商务在法律规范方面的问题主要体现在以下方面：

1. 税收立法

电子商务不同于传统经济模式，对其是否征税、如何征税，是各国税收立法必须面对的问题。各国关于电子商务税收的政策各不相同，美国等国家希望电子商务免税，而其他国家则坚持对电子商务必须征税。在坚持对电子商务征税的国家，现行税法针

① 杨谷：《最可怕的是错过一个时代》，《光明日报》，2000 年 3 月 6 日。

对的是有形产品，并以属地原则为基础，而电子商务具有虚拟化、超国界和数字化等特点，互联网络的开放性、使用者的流动性和隐匿性带来的纳税人身份判定问题，交易过程的可追溯性问题，税务部门的税务稽查问题，使传统的税收法律制度难以适应。目前，世界各国对电子商务税收立法都十分谨慎，立法进程缓慢，我国电子商务税收立法还处于找问题，探讨解决办法的阶段，成熟的电子商务税法尚未出台。

2. 电子商务合同立法

电子合同是电子商务发展带来的新法律问题，我国修改后的《合同法》注意到这一问题，并在相应条款上进行调整，如电子合同书面形式、签名以及要约和承诺等都纳入了合同调整的范围。但是，我国现行有关电子合同的法律仍然很不完备，需要进一步完善。

3. 电子商务安全立法

电子商务安全是电子商务发展的基础，法律保护是维护电子商务安全的重要手段。我国在 20 世纪 90 年代制定了若干相关行政处罚法规，1997 年新刑法也增补了三条法条惩治计算机犯罪行为，这些法律规定是维护电子商务安全的有力法律武器。但是，侵犯电子商务安全的违法犯罪发展很快，现有的法律法规已经不能有效维护电子商务安全，急需电子商务安全立法的完善。

4. 知识产权立法

全球电子商务的迅速发展，使现行知识产权保护制度面临新的挑战，如知识产权的专有性和地域性，面临网上信息的公用性、网络空间的无国界性的挑战。此外，还有作品的数字化、网络传播和抢注域名等新问题。现有的知识产权法律体系滞后于电子商务发展现状，急需立法完善。

5. 网上个人数据及其隐私保护立法

个人数据是指任何与一个确定的或可确定的个人相关的信息。电子商务的开展，必然要建立和使用许多有关顾客的信息数

据库，这些数据库可能包含了敏感程度各异的隐私内容。由于对数据库信息采集和使用没有严格的立法，网上个人隐私数据得不到充分的保护，许多人担心网上个人隐私数据的安全，而不愿意上网消费。美国商业周刊 1998 年 3 月的一次调查结果显示，目前还没有使用互联网的消费者，将对个人信息和通信隐私的顾虑列为其远离互联网的首要原因。我国没有制定保护隐私权的单行法律，保护个人隐私的法条散见于民事、刑事等法律法规中，尚未形成完备的法律体系，这种法律保障状况不利于消除人们参与电子商务的担忧。因此，保护网上个人隐私数据应成为我国电子商务立法的重要组成。

6. 电子支付立法

电子支付是电子商务的重要环节，指通过计算机及其网络，将传统支付方式电子化，以某种形式的电子信息取代传统支付工具的支付方式。现行支付法以票据法为核心，其完善经历了上百年时间，而电子支付是近 20 年才出现的，它与传统的票据支付有较大差异，现行票据法不能很好地适用于电子支付，这使得电子支付参与者的权利义务不明确，参与者对交易的法律后果无法充分预期，进而影响了电子商务正常发展。我国支付法建立较晚，直到 1995 年票据法才出台，刚刚跟上传统支付法的发展，对电子支付的立法还处于探索阶段。

由于存在以上问题，电子商务在现阶段是比较脆弱的，容易遭受不利因素的影响。在阻碍电子商务发展的诸多因素中，电子商务领域犯罪的危害最大。2000 年 1 月 18 日发布的《中国互联网络发展状况统计报告》的调查显示，安全可靠性是网络用户最关心的问题。一旦因为电子商务领域犯罪动摇了投资者、消费者对电子商务的信心，必然动摇电子商务发展的社会基础，严重影响我国电子商务的发展。因此，关注电子商务发展中的问题，特别是电子商务领域的犯罪问题，对保障我国电子商务迅速发展具有重要意义。

第二章　电子商务领域犯罪的基本情况

第一节　电子商务领域犯罪概述

一、电子商务领域犯罪的含义

研究电子商务领域犯罪首先要弄清它的含义，确定其内涵和外延。我国刑法分则和 1997 年“两高”公布的《刑法》罪名表中，不存在电子商务领域犯罪这样的类罪或者个罪，它是在信息时代电子商务活动中出现的，具有某些共同特性的诸多犯罪的集合，同时它又严重侵害电子商务这一重要的经济活动，因而有必要作为一类犯罪进行研究。

犯罪是属于一定历史范畴的社会现象，有些犯罪在各社会时期都存在，如暴力犯罪、性犯罪，有些犯罪只在特定的社会环境下产生，电子商务领域犯罪只在电子商务应用环境中产生，并随着电子商务发展不断变化。电子商务领域犯罪包含多种具体犯罪，具有以下基本特征：

（一）严重危害电子商务秩序是电子商务领域犯罪的内容和范围。被侵犯的电子商务秩序不是某一种社会关系，而是发生在电子商务活动中的若干社会关系的集合。在这一社会关系的集合中，既有国家利益，如国家对电子商务的管理控制权，也有社会利益，如网络通信服务安全关系每一个网络用户的利益，还有个人利益。电子商务领域犯罪与电子商务领域违法违规行为的区

别，在于其具有严重的社会危害性，阻碍着正处于发展关键阶段的电子商务。

（二）电子商务领域犯罪在行为方式上表现为利用电子商务计算机信息系统的特性。电子商务信息系统主要指用于电子商务活动的计算机系统，包括企业、个人和其他社会组织使用的计算机信息系统以及相关的网络通信设备。利用电子商务信息系统特性有两层含义：一是利用其技术特性，包括计算机系统特性、网络通信系统特性、计算机数据的技术特性等等；二是利用电子商务信息系统应用功能，如销售网站推销商品、广告宣传、竞价拍卖、售后服务功能，电子商务认证系统身份认证功能等。对以上两种特性，犯罪行为人至少会利用其中之一，不利用两者中任何一种特性的，如炸毁电子商务认证中心、砸毁电子商务网站计算机信息系统设备等行为，不是电子商务应用环境下特有的行为，不属于电子商务领域犯罪行为。但是，行为人利用电子商务信息系统的技术特性，使用物理方法破坏电子商务信息系统某部分，如抽拔系统元器件、截断网络通信线路，破坏电子商务信息系统功能的，应当属于电子商务领域犯罪。

除以上两个基本特征外，电子商务领域犯罪还具有空间时间上的大跨度性。即这类犯罪的行为与犯罪的结果（包括中间结果）经常不是同时发生，而是有一个相当长的时间间隔，在空间上大多不在同一地方，有时远隔千里。

根据以上分析，作者认为，电子商务领域犯罪是电子商务时代产生的，具有若干共性的一类犯罪，这类犯罪中各具体犯罪的特性可能不同，但是都应具有利用电子商务信息系统特性和严重危害电子商务发展两个基本特征，或者说，电子商务领域犯罪是指利用电子商务信息系统特性危害电子商务正常秩序，具有严重社会危害性的行为。需要说明的是，这里对电子商务领域犯罪所下的定义不是刑法学意义上的定义，刑法学意义上的犯罪应该具

有严重的社会危害性和刑事违法性两个基本特征①，而电子商务领域犯罪是短时间内发展起来的一类犯罪，其中有的行为有刑法条文规定，如故意传播计算机病毒危害电子商务计算机信息系统的行为，有的则没有，如以破解他人软件产品反侵权措施为常业的行为等，虽然后者具有严重的社会危害性，由于刑事立法的滞后，却不构成犯罪，不能进行刑罚处罚。因此，本书定义的电子商务领域犯罪是犯罪学意义上的定义。研究电子商务领域犯罪，不仅要研究刑法已有规定的犯罪，还要研究刑法没有规定的犯罪，以推动电子商务领域刑事立法的完善。

电子商务领域犯罪与计算机犯罪有密切联系，但不是同一个概念。何为计算机犯罪，尚无统一的看法。作者认为，计算机犯罪是指利用计算机信息系统特性严重危害社会的行为②。伴随计算机、网络等技术的推广应用，计算机犯罪不断发展变化，先后经历了与单个计算机相关的计算机犯罪、计算机局域网中的计算机犯罪和国际互联网络中的计算机犯罪三个阶段，其影响范围由最初的科学计算领域，扩展到社会生活各领域，目前越来越集中在经济生活领域，特别是在电子商务领域，而且，目前的计算机犯罪在行为形态上更多地表现为利用国际互联网、电子商务计算机信息系统功能特性。因此，可以说，电子商务领域犯罪是计算机犯罪的最新发展，是一类特殊的计算机犯罪，它具有计算机犯罪的基本特征，同时具有自身的特点。关于计算机犯罪的新发展，有学者提出“网络犯罪”、“信息犯罪”等概念，作者认为，这些概念只反映了计算机犯罪的部分技术特征，不能全面、准确地概括计算机犯罪的最新发展。电子商务领域犯罪是计算机犯罪发展的主要趋势，应当作为研究的重点。

---

① 马克昌主编《犯罪通论》，武汉大学出版社 1999 年版，第 12～28 页。

② 赵廷光、皮勇：《论我国刑法中的计算机犯罪》，《现代法学》，1999 年第 4 期，第 101～104 页。

有学者提出电子商务犯罪的概念，认为电子商务犯罪是指在电子商务活动的各个环节涉及的犯罪①。作者认为，用“电子商务活动各个环节涉及的犯罪”来界定电子商务犯罪，其外延过于宽泛，可能超出电子商务犯罪的界限，比如行为人在电子商务网站上，散布煽动分裂国家、破坏国家统一的信息的，可能构成煽动分裂国家罪，而这种行为难以被理解为电子商务犯罪。

二、电子商务领域犯罪的分类

根据不同的标准,可以把电子商务领域犯罪分为不同的种类。

（一）根据犯罪主要侵害的社会关系分类

根据电子商务领域犯罪主要侵害的社会关系，可以分为电子商务犯罪和电子商务关联犯罪、危害电子商务计算机信息系统安全的犯罪三类。

电子商务犯罪的特点是发生在正常电子商务活动过程中，利用电子商务系统特性侵害各种社会关系，如电子商务领域的信用卡诈骗犯罪、侵犯著作权犯罪、盗窃商业秘密犯罪和诈骗犯罪等。电子商务犯罪随着电子商务的发展不断扩展其范围，新形式的犯罪不断增加，新的法律问题不断产生，给传统刑法体系予以全面冲击，电子商务犯罪问题是电子商务刑事立法和理论研究的重点。

电子商务关联犯罪的特点是，虽然不发生在正常电子商务活动过程中，但与电子商务活动有着紧密联系。与电子商务犯罪相似，电子商务关联犯罪在行为方式上表现为利用电子商务系统的特性。电子商务关联犯罪带来了大量新的法律问题，也是电子商务刑事立法和理论研究的重点。

危害电子商务计算机信息系统安全的犯罪，主要侵犯的是电

---

① 赵秉志主编：《新千年刑法热点问题研究与适用》，中国检察出版社 2001 年版，第 489～497 页。

子商务计算机信息系统安全管理秩序。电子商务计算机信息系统是电子商务运作的物质技术基础，是电子商务正常运作的基本保障。电子商务计算机信息系统安全主要包括有效性、保密性和完整性，根据这类犯罪侵犯电子商务计算机信息系统安全性的不同方面，可以进一步分为破坏计算机信息系统功能的犯罪、非法侵入计算机信息系统的犯罪、破坏计算机信息系统中数据的犯罪。危害电子商务计算机信息系统安全的犯罪发案较多，影响较大，通常具有高智能性和高技术性，是一类重要犯罪。

（二）根据犯罪主体进行分类

根据电子商务领域犯罪的主体特征，可以分为自然人进行的又可犯罪、单位形式的犯罪。

1. 自然人进行的犯罪可分为两种：一是单个自然人进行的犯罪。其特点是单个行为人不与其他人或组织合谋，仅凭自己的技术和设备危害电子商务的行为。由于受个人技术水平、犯罪工具等条件所限，这类犯罪的社会危害性并不十分严重。但是，也有另外，如 2000 年 2 月，行为人使用“拒绝服务”计算机程序造成若干大商业网站瘫痪，经济损失严重。多个犯罪人事先没有结成一定组织，而合谋进行具体犯罪的，属于若干自然人进行的共同犯罪。二是有组织犯罪。其特点是若干行为人组成具有一定形式的组织，合谋、协作进行电子商务领域犯罪。这类犯罪中，各犯罪人事先经过合谋、演练，在具体犯罪中分工协作，破坏能力超过单个犯罪人破坏力的简单相加。近年来，互联网络上的犯罪组织越来越多，例如 1993 年以来，被称为“赛巴网络恐怖分子”的犯罪组织活跃在美、英等国家的计算机网络上，专干设置“逻辑炸弹”的勾当，破坏各网络公司的计算机信息系统，借以进行敲诈勒索。据统计，“赛巴网络恐怖分子”先后作案四十余起，共勒索各计算机公司 6 亿多美元①。

① 刘广三：《计算机犯罪论》，中国人民大学出版社 1999 年版，第 77 页。

2. 单位形式的犯罪是指犯罪人不是某个自然人、犯罪组织，而是公司、企业、社会团体等单位。现代企业大多使用计算机系统进行经营管理，在日益激烈的企业竞争中，有些企业使用不正当手段进行竞争，利用技术手段攻击竞争对手的计算机信息系统，干扰正常工作或侵入他人计算机信息系统窃取商业秘密。

需要指出的是，虽然不存在一个国家对另一个国家的犯罪，但是，在实际生活中存在以国家形式进行的危害他国电子商务的行为。冷战结束后，全球间谍战的主战场转移到广阔的计算机网络空间，主要目标是各国商业领域，如 1995 年春在美国与日本进行的关于豪华轿车进口问题的激烈谈判中，美国的中央情报局和国家安全局曾窃听日本汽车业高级主管和贸易官员的谈话，向美国谈判代表提供了情报①。2000 年欧盟议会 3 月 30 日证实，美国在全球有一个名为“梯队”的监听网，大肆对欧洲盟国进行窃听活动，欧盟轮值主席国的葡萄牙内政部长费尔南德·葛麦斯在一份发言中强烈批评美国对欧盟国家进行窃听活动。葛麦斯说，问题的关键不是存不存在这个监听系统，而是已危及到欧洲企业的利益②。

第二节　电子商务领域犯罪的态势和特征

一、电子商务领域犯罪的现状和发展趋势

现代科学技术是一把双刃剑，在为人类造福的同时，也为高科技犯罪提供了新的有效手段。计算机犯罪伴随计算机及通信科技发展和应用而产生，半个世纪以来愈演愈烈，被称为“飘过世

① 黄学彬：《接近零点——全球反计算机犯罪透视》，四川人民出版社 1997 年版，第 28 页。

② 《欧盟强烈反对美监听活动》，《科技日报》，2000 年 4 月 4 日。

纪的乌云”，自 20 世纪 90 年代以来，越来越多地发生在电子商务领域，成为各国电子商务发展的巨大阻碍。

综观国内外电子商务领域犯罪的态势，其具有发案数量迅速增加、社会危害性日趋严重、新形式犯罪日益增多等特点。

20 世纪 90 年代中期以来，电子商务领域犯罪发案数量迅猛增加。英国工业贸易部、国家计算中心、LCL 以及英国信息产业安全评估与认证委员会主持了英国企业遭受计算机犯罪危害的调查，1995 年发生的与计算机相关的盗窃比 1994 年增长了 60%，由于计算机信息安全性遭到破坏给被害公司造成的损失比 1994 年也几乎翻了一番；在加拿大，互联网上发生的非法侵入公司系统的案件由 1997 年的 4% 增加到 1998 年的 8%，300 家加拿大企业中有 70% 报告其计算机安全性遭到破坏；根据澳大利亚维多利亚警察局计算机犯罪小队和 Deloitte Toche Tohmatsu 所主持的对计算机犯罪的调查报告，至少 1/3 的澳大利亚公司已经成为计算机犯罪的目标；1997 年、1998 年美国计算机安全研究所与 FBI 国际计算机犯罪中心旧金山分部合作对 500 余家美国公司、政府机构、金融机构以及大学作了计算机犯罪与安全调查，发现虽然美国公司和政府机构花费增加了，但是发生在这些单位的计算机犯罪以及其他信息安全违法事件仍呈上升势头，报告显示计算机安全受到侵害的事件 1998 年比 1997 年增加了 16%，被害单位所遭受的经济损失比前一年增加了 36%，由于与国际互联网络连接而频繁遭受攻击的机构数目，从 1996 年的 47% 上升到 1997 年的 54%，比 1995 年的 37% 增加了 17%。

在数量迅速增加的同时，电子商务领域犯罪的社会危害性程度也越来越严重。一名法国电脑高手从 1994 年 8 月起的 4 个月中，侵入美国联邦调查局的通讯网络线路，利用联邦调查局账号，拨打国际长途电话以及在电脑网络上和全球各地的电脑迷聊天，使美国联邦调查局蒙受了高达 25 万美元的经济损失。英国

的公司每年要花费 5.3 亿英镑对付计算机伪造和侵入犯罪①。我国最严重的一起金融计算机犯罪案件造成经济损失高达 2 100 万元，1998 年在我国大规模爆发的 CIH 病毒造成约 36 万台计算机损坏，直接、间接经济损失超过 10 亿元②。

根据电子商务领域犯罪目前的发案特征，电子商务领域犯罪在以下领域将更严重：（1）金融领域的犯罪，特别是信用卡伪造、诈骗、盗用犯罪；（2）电子商务欺诈犯罪；（3）电子商务领域的侵犯知识产权的犯罪；（4）盗窃商业秘密的犯罪；（5）侵犯消费者网上个人数据及其隐私的犯罪；（6）网上兜售、传播色情物品、信息的犯罪；（7）电子商务认证欺诈犯罪。

二、电子商务领域犯罪的特征

犯罪问题是一个复杂的社会现象，要深入研究某种犯罪，应该从各个角度充分认识其特征。电子商务领域犯罪是信息时代特有的一类犯罪，研究这类犯罪必须研究犯罪人特征、犯罪的客观表现。同时，电子商务领域犯罪的犯罪对象和被害者也是信息时代的产物，没有这些特定的犯罪对象和被害者，就不可能有电子商务领域犯罪的发生。以下将从犯罪人组成结构特征、犯罪心态特征、犯罪客观表现和犯罪被害人特征四个方面进行分析：

（一）犯罪人组成结构特征

电子商务领域犯罪的基本特征之一是利用电子商务信息系统特性，虽然可能存在不懂计算机技术和应用的共同犯罪人，但是实行犯必须具有计算机和网络技术知识或电子商务信息系统应用知识。

这类犯罪人的组成特征可以通过分析上网用户群体特征来认

---

① 胡泳：《信息安全恐慌症》，《生活周刊》，1997 年第 6 期。

② 顾洪洪：《CIH 病毒在中国造成严重危害 经济损失 10 亿元》，《电脑日报》，1999 年 5 月 7 日。

识。从世界范围来看，电子商务用户群集中在经济发达、教育程度高、计算机知识普及程度高的国家和地区，北美占不到5%的世界人口，其计算机数量却超过了世界其他地区的总和，并占全球互联网用户的50%以上。南亚居住着世界23%的人口，但该地区的互联网用户仅占全球用户的1%还不到。由于没有受过教育和缺少基本的计算机技能，发展中国家的人民中几乎没有多少人使用电子商务。例如，在非洲的贝宁，60%以上的人口是文盲，因此要在该国扩大互联网接入、增加上网人数便受到限制。此外，社会文化传统也影响了互联网用户的组成结构，妇女在上网用户中所占的比例在全球很不平均，美国占38%，巴西为25%，南非为17%，俄罗斯为16%，中国互联网用户中仅有7%是妇女，而阿拉伯国家Internet女用户更只占4%①。我国的互联网用户分布也具有类似的特征。我国互联网用户发展迅速，几乎是每半年增加一倍，并且在今后3～5年内将成为上网绝对人数占世界第三的国家，这些网民有1/5在北京，1/10在中国南部沿海城市的广东、上海，最少的为西藏、青海、宁夏回族自治区，多数网民是中产阶层，大部分在城市，24岁以下的占一半，男性比例占79%，女性比例占21%，每周上网平均时间为7小时，使用自己的电脑自己支付网费②。

除了以上特征外，电子商务领域犯罪的犯罪人组成还具有以下特性：(1)从所受文化教育程度来看，许多犯罪人受过较好的计算机技术、电子商务专业知识的教育或者培训，一部分人具有大学本科以上学历，他们在犯罪过程中能熟练运用所学的计算机技术和行业知识，表现出一定程度上的高智能性和专业性。(2)

① 《因特网用户分布不均，北美占到50%以上》，《电脑日报》，1999年7月16日。

② 《中国将成为上网人数最多的国家之一》，《参考消息》，2000年3月1日。

从犯罪人社会地位来看，许多犯罪人具有较高的社会经济地位，但不全是“白领犯罪”人，相当一部分犯罪人是单位内部具有一定管理职权的系统管理人员或者某部门主管，也有一部分内部人员勾结单位外部人员，利用职务便利实施犯罪，因而也表现出职务犯罪和共同犯罪的特征，这些人实现犯罪隐蔽性强，难以防范。(3) 青少年黑客数量不小。目前上网用户中不少是青少年学生，由于他们好奇心强、喜好模仿和追求刺激，对黑客技术十分感兴趣，许多人从互联网上获取黑客工具肆意进行试验，并把自己非法侵入安全性强或重要的网站，作为在“同行”中炫耀的资本。

(二) 犯罪心态特征

犯罪的心态有多种，主要有牟利、破坏、窃密、泄愤报复、炫耀技能的“黑客”动机等五种。从目前发现的案件来看，以牟利为犯罪目的的比例最大，具体形式有多种，有的利用计算机盗窃金融机构资产，有的是意图盗用通信服务，还有出于避免预期的经济损失的目的，如操纵证券计算机信息系统解套自己或者他人的股票。以盗窃商业秘密为犯罪目的的案件也占有较大比例，其间接目的往往是为了出卖牟利，如广州李建新盗卖“好又多”公司商业秘密案①。还有一部分犯罪人出于所谓“黑客”动机，即为了试验自己的计算机技能或者向他人炫耀侵入他人计算机信息系统，一般没有破坏、窃密等其他目的。

(三) 犯罪客观表现特征

电子商务领域犯罪在客观方面表现为极强的隐蔽性和严重的社会危害性。其隐蔽性的原因主要有四：

1. 计算机信息系统的技术性能使这类犯罪具有隐蔽性。电子商务领域犯罪的犯罪对象一般是系统的功能、应用程序、计算

① 邹高翔：《侵犯电脑信息案宣判，2 万元换来两年刑》，《电脑日报》，1997 年 10 月 20 日。

机数据等无形的对象，犯罪不造成物理性有形的损坏，难以引起人们的警觉。加之，电子商务信息系统联系范围广泛、处理的信息量极其庞大，处理速度极快，要在浩如烟海的信息海洋中发现犯罪的踪迹，有如大海捞针，困难很大，有时即使发觉了犯罪事实，由于犯罪技术多样和目前侦破技术的滞后，发现犯罪人的可能性很小。

2．互联网用户身份虚拟性使犯罪人很难被发觉。现有的技术和现行的管理还不能做到用户的网上身份和真实身份一致。加之，一些商业网站为扩大影响，提供各种匿名网络服务，许多人不经身份登记就可以进入网络空间，或使用虚拟身份参与网络空间的各种活动，即使其犯罪行为被发觉，也无法确定行为人的真实身份。

3．内部人员作案使犯罪难以被发觉。在电子商务领域犯罪中，有相当一部分是单位内部人员所为，这些人熟悉业务知识，知道内部管理的漏洞，特别是有作案的有利条件，他们能够在正常工作过程中隐蔽地、逐步地实施犯罪，并掩盖犯罪事实。

4．被害人不举报掩盖了一部分犯罪。被害单位考虑到破案率低、犯罪难以有效追究、担心企业信誉受损、受到犯罪人的继续报复等原因往往不报案，也使相当一部分犯罪得不到暴露。

其社会危害性的原因主要有三：

1．处于发展关键时期的电子商务容易遭受电子商务领域犯罪的沉重打击。电子商务正处于发展的脆弱时期，企业和消费者对电子商务的信心容易被挫伤，电子商务领域犯罪不仅会给直接受害者带来损失，而且会严重影响人们参与发展电子商务的积极性，迟缓甚至扼杀电子商务的发展。

2．电子商务系统中的巨额社会财富可能成为犯罪的直接侵害对象。通过电子商务信息系统，犯罪人能够方便地控制巨量的社会财富，造成巨大的经济损失。而且，电子商务紧密联系着社会的方方面面，一旦遭到破坏，将波及社会生活的各行各业，造

成损害极其严重。

3. 犯罪极强的隐蔽性也使犯罪行为得以多次、连续进行，其累计危害后果可能达到十分严重的程度。

（四）犯罪被害人特征

没有被害者，就没有犯罪，犯罪人和被害人是刑事上的对立者，被害人被害的诱发性是犯罪发生的条件和诱因。所谓被害的诱发性，是指被害方存在的引起犯罪人实施犯罪行为加害被害人的因素。按照被害人对犯罪发生所负责任的大小，主要可以分为两类：一类是对犯罪没有责任或者所负责任很小的被害人。如单位协调员工关系无失误，计算机安全管理规章齐备并执行落实，计算机安全设施完备，犯罪的发生完全是由于犯罪人精心策划，运用较强的科技能力突破安全措施所致。第二类是对犯罪发生负一定责任的被害人。如单位内部管理存在漏洞，安全防护设施落后，员工关系紧张，发生案件不报案，草率处理，个人安全保护意识不强，对关键数据如账户密码信息管理不善。该类被害人的这些特征容易诱发犯罪人对其实施犯罪行为，同时也是犯罪得逞的条件。

第三节　电子商务领域犯罪的常用方法

犯罪方法是危害行为实施的方式、手段、途径和步骤，任何危害行为的实施都不能离开一定的方法，犯罪不同，其方法也不相同，如暴力犯罪的方法是使用暴力或进行威胁，盗窃犯罪的方法是秘密窃取。电子商务领域犯罪的方法与其特性紧密相关，利用电子商务信息系统特性是这类犯罪的共性，而具体的犯罪方法则多种多样，而且随着电子商务领域犯罪的发展，新的犯罪手段、方法会不断产生。目前常用的方法主要有以下几种：

一、施放计算机病毒

病毒是生物学领域的术语，是指能够使生物机体致病的一种微生物。在计算机科学领域，有一种侵害计算机信息系统安全的方法与生物领域病毒的行为特征十分相似，是一种人为编制的计算机程序且能够自动在计算机信息系统中运行，具有一定的破坏性、隐蔽性、可触发性、自我复制性和类似生物病毒的可传染性，人们把病毒这一概念借用过来，把它称之为计算机病毒。计算机病毒通过磁盘或网络通讯等途径传播，感染其他计算机信息系统并隐藏起来，当计算机信息系统的运作满足一定的触发条件时，就破坏计算机信息系统功能、应用程序或者计算机数据。在短短二十多年时间里，计算机病毒发展极为迅速，数量已经超过2万种，并且种类繁多，反侦查能力和破坏能力越来越强。虽然反计算机病毒的技术发展很快，也取得了一定的效果，但由于新形式的病毒不断产生，反计算机病毒总处于被动防御的地位。利用计算机病毒攻击计算机信息系统，是电子商务领域犯罪中的一种极具威胁的犯罪方法。

二、活动天窗

所谓活动天窗（Trapdoors），是指编程人员为了对程序进行调试和维护的方便，故意设置在计算机程序中的入口，通过这些入口可以绕过计算机程序的正常安全检查进入软件系统。一般而言，活动天窗只有编程人员才知道，其他人难以发现，并且在软件调试成功后，往往被要求关闭活动天窗。有些编程人员为达到不可告人的目的，特意留下一些活动天窗，为以后秘密侵入系统，非法操作系统资源准备条件。利用活动天窗窃密不是某个公司偶然发生的事件，而是经常出现在大大小小的计算机软硬件制造商的产品中。美国微软公司是世界上最大的软件制造公司，它生产的操作系统在世界市场上占有绝对优势。1998年微软公司

推出 Windows98 操作系统风行一时，不久人们发觉 Windows98 中有会泄露用户个人资料的“后门”，Windows98 会根据用户的计算机硬件配置情况生成一串与用户名字、地址相关的代码——全球惟一的识别码，这个识别码会通过 Windows98 的电子注册程序，在用户不知情的情况下传送到微软的网站上去①。世界最大的 CPU 制造商 INTER 公司也有此“佳绩”，1999 年 1 月英特尔公司宣布为了增强网上电子商务的安全，将在奔腾Ⅲ处理器中设置用以识别用户身份的序列码。反对序列码的人们指出，在使用了以奔腾Ⅲ为中央处理器的电脑后，员工在互联网络上的一举一动，很可能处在“有心人”的监视之下。虽然后来英特尔公司向计算机制造商分发了一个用来关闭序列码功能的修补程序，但是序列码继续威胁着个人隐私。有些电脑黑客已经开发出了专门窃取别人序列码的程序。

三、特洛伊木马术

特洛伊木马与古希腊特洛伊城战争相关，当时希腊军队为攻下特洛伊城，假装撤军而把腹中藏有士兵的木马留在撤退的战场上，特洛伊守军把这些木马当做战利品搬回城内，晚上希腊军队悄悄返回，木马中的士兵跳出来，里应外合打开城门，攻陷了特洛伊城。特洛伊木马术是指以软件程序为基础进行欺骗和破坏的方法。这种方法是指，在一个计算机程序中隐藏作案所需的计算机指令，用户在执行该程序的同时执行了犯罪人预谋的计算机操作。在互联网络上经常有一些不知名的免费工具程序，如看图程序 See.exe，用户在下载并执行这些程序时，常常发现这些程序执行的是破坏计算机系统的指令，或者秘密执行了一些其他有害系统安全的指令。例如，1988 年日本最大的个人计算机通信网

① 杨谷：《Windows98、奔腾Ⅲ是——埋在我们身边的“定时炸弹”》，《光明日报》，1999 年 5 月 12 日。

络 PC－VAN 的网络成员都可以在屏幕上看到意义不明的文章，为弄清其含义，用户往往输入自己的密码以寻求系统帮助。而实际上，这些意义不明的文章是一种暗号，是“罪犯”用以盗窃用户口令的手段。行为人通过电子邮件把带有这种“机关”的程序发送给用户，用户只要一启动计算机，该程序就立即执行并在屏幕上显示意义不明的文章，继而获得用户的密码并传送给行为人。在这一事件中，行为人使用的正是特洛伊木马术。

四、意大利香肠术

所谓意大利香肠术，是指每次秘密窃取少量的财产而日积月累达到很大数目的一种犯罪方法。在计算机程序中使用意大利香肠术窃取财产，让计算机程序每次只盗窃数量非常小的资金，日积月累也可以积聚到一笔数目不菲的财富。1987 年加拿大一家银行的软件工程师霍克，发现银行的计算机在计算利息的方法上有机可乘，于是他在该银行设立了个人账户，在为这家银行设计利息计算程序时，在程序的末尾加上这样的指令：把计付利息时四舍五入舍去的小数部分自动加到他的账户上。由于银行每季度汇计一次利息，因此每三个月他都可以获得几千甚至上万美元①。

五、数据欺骗

所谓数据欺骗，是指非法篡改输入输出数据，或者输入假数据。使用这种方法简便易行，在目前电子商务领域犯罪中较多见。美国太平洋电话公司和它为数众多的分公司间，是以数据专线经由电话系统与总公司的电脑中心进行联络的。某电子技术员经过精心研究，发现了该公司的电脑订货作业程序和订货密码，

① 黄学彬：《接近零点——全球反计算机犯罪透视》，四川人民出版社 1997 年版，第 33 页。

于是他擅自设置电脑终端，输入各分公司的订货号码，冒用分公司向总公司订货，总公司据此电脑资料把订货在夜间运送到各分公司，次日早上该技术员使用一辆印有公司字号的货车，到各分公司把订货取走，各分公司本无订货，认为是总公司运送错误而回运货物，就让这名技术员运走货物，这名技术员共骗得价值约100万美元的货物。

六、逻辑炸弹

所谓“逻辑炸弹”，是指人为编制的一种危害计算机系统的计算机程序，这种程序只在满足一定的逻辑条件时才发作，损害计算机系统的安全，这些逻辑条件可能是某一个日期，或是系统执行了某一个操作。隐蔽性强的“逻辑炸弹”多为单位内部计算机工作人员所为，例如1997年9月大连市空军华鹰寻呼台的计算机网络系统忽然发生故障，后多次发生同样的情况，给单位造成严重损失，经查发现该台原计算机管理员张某在寻呼台计算机网络系统中设置了“逻辑炸弹”，在被解雇后修改了“逻辑炸弹”程序，以致于频繁发生系统故障。

七、截听信息

计算机信息系统之间要通过通信线路交换信息，行为人可以使用诸如协议分析器之类的工具程序，截听计算机信息系统交换的信息。由于计算机信息系统本身都有一定程度的辐射，行为人还可以使用灵敏的信号接受还原设备，再现远处计算机信息系统屏幕上的信息。国外曾屡次报道，有商业间谍使用装有灵敏的电磁波接收还原设备的汽车，故意停靠在被侦查公司的计算机机房周围，窃取商业机密。

八、建立色情网站

利用网站兜售、传播色情信息是目前电子商务领域色情犯罪

的一种重要方法。行为人在允许经营色情网站的国家或者地区建立网站，在网站中放入大量的各种色情图片、音像，或者兜售淫秽器具，介绍卖淫信息等。目前互联网已经成为色情服务行业最重要的“行销”平台之一，而且这股潮流只会愈演愈烈。由于我国法律禁止经营色情网站，在我国该类犯罪多为设立含色情内容的个人主页，赚取广告资助费，如河南商丘杨柯、何肃黄涉嫌传播淫秽物品案。

九、盗窃信用卡账号密码

随着电子化金融工具的发展，出现了可用于网上支付的信用卡，客户使用这种信用卡，可直接进行电子商务交易。一些犯罪人通过各种方式窃取他人信用卡信息，进而在网上大肆消费，给被害人造成较大的经济损失。2000 年 3 月 4 日意大利警方宣布，两名非法进入美国银行电脑系统并冒用他人信用卡作案的电脑黑客被逮捕，这两名黑客通过破译口令，不断“潜入”美国花旗银行的信用卡电脑系统库，盗窃用户的个人资料，并用于网上博彩。警方已查获这对夫妇盗用他人金额 100 万美元，赌博所赢 80 万美元全被转入他们自己的账户①。

十、电子商务诈骗

电子商务使远隔千里、素未谋面的人们能便利地进行交易，有些人则借电子商务之名进行诈骗。如行为人建立交易网站，提供商品的广告信息，而客户订购商品支付货款后，将收不到订购的商品，或只收到质量很差的商品。如 1999 年 5 月一个以基金投资为名诈骗客户资金的案件被侦破，诈骗分子在瑞士、格恩西、伯利兹、奥地利、马耳他及西印度开设银行账户和办事处，然后向潜在投资者寄送手册，要求他们以“特别”低的价格购买

① 阎涛：《意破获一起电脑黑客案》，《检察日报》，2000 年 3 月 6 日。

基金的股份，并使投资者关注虚构基金每日增长情况的互联网网站。但在投资者希望退出时，他们被建议转换另一家“有希望的投资计划”，并被要求寄出更多的资金。这桩全球投资诈骗活动已骗取香港人数百万港币的投资，在全球的诈骗金额可能已达数十亿港币①。

十一、网上非法传播、贩卖他人版权作品

计算机、网络技术使作品得以更广泛地传播，也为侵犯版权犯罪提供了一种新方法。这类犯罪的行为人利用计算机技术把他人的版权作品数字化，形成计算机数据文件，然后在网络上传播或者销售。目前互联网络中非法传播、贩卖他人版权作品的方式多种多样，有的是直接低价销售，有的是向互联网用户免费提供，借以提升网站的影响。

第四节 电子商务领域犯罪的原因和条件

马克思主义哲学认为，世界万物之间存在普遍的联系，任何事物有其产生、存在、发展的原因和条件。电子商务领域犯罪是信息时代一种特殊的社会现象，电子商务发展中诸多不完善方面，既是电子商务领域犯罪产生的原因，也是犯罪实施的条件。研究电子商务领域犯罪产生的原因和条件，有利于发现犯罪的规律，予以有效地预防和治理。除了电子商务领域犯罪的隐蔽性特征外，这类犯罪产生并迅速发展的主要原因和条件有以下几个方面。

① 《利用互联网进行诈骗，骗取资金数十亿港币》，《电脑日报》，1999 年 5 月 26 日。

一、网络空间反主流亚文化思想的消极影响

“亚文化指的是一种社会性的行为和价值体系，它独立于社会上主导的行为和价值体系而存在，但仍然是这一主要体系的一部分。生活在亚文化中的群体分享主导文明的因素，但也保持某些独特的行为榜样和价值观念”①。伴随计算机和互联网络的应用，相关的亚文化逐渐形成，研究这种亚文化的特点，有必要从其起源谈起。

20 世纪六七十年代，计算机成为军事、科研领域的有力工具，但是，当时计算机设备极为稀少和昂贵，青年人必须在管理人员的控制下，非常有限地使用那些庞大、笨重而功能极为有限的大型机，而且计算机的应用范围也极受限制，被军事工业集团所垄断，“计算机基本上是被用来反对人民而不是去帮助人民，被用来控制人民而不是去解放人民”②。为反抗这种社会状况，争取自由地使用计算机，当时一些年轻人自己手工制造个人计算机，并利用他人捐献的计算机设备组成公众信息网络，这样的努力在当时没有取得最后的成功，却影响了希望能够自由使用计算机，实现个人自由发展的一代青年人。这些人一部分成为计算机领域的杰出人才，如比尔·盖茨等，更多的成为网络空间的黑客。突破现有规章控制，实现个人充分发展是这一群体的共同特征，这一群体有独特的兴趣爱好，并通过网络相互交流、帮助，有的还建立了俱乐部等形式的组织，在长期的交流中形成了某些较稳定的看法和观点，成为一个独立于社会主流文化的亚文化群。

20 世纪 90 年代计算机软件和设备制造技术取得突破性发

---

① ［德］汉斯·约阿希姆·施奈德：《犯罪学》，中国人民公安大学出版社 1990 年版，第 466 页。

② 胡泳、范海燕：《黑客——电脑时代的牛仔》，中国人民大学出版社 1997 年版，第 95 页。

展，人机交流技术、网络技术、多媒体技术等计算机信息科学技术逐渐完善。借助于这些技术成果，即使不是计算机专业人员也能很快学会使用计算机，使用计算机的社会群体越来越大，增长速度越来越快，同时，亚文化群的成员也在迅速增加，其主要成员是 20 世纪七八十年代出生的一代年轻人，计算机、网络技术成为他们挑战限制、伸张个人主张的有力工具。这时的亚文化群组成更加复杂，一部分是良性的亚文化群体，他们希望通过计算机、网络发展个人能力，增加社会交往，充分自由表达个人见解；另一部分是恶性的亚文化群体或称反主流亚文化，他们把网络空间视做绝对自由的天国，凭借锐利的技术工具，就可以藐视他人的正当权利和法律的威严。反主流亚文化群体中，有的人宣称网络空间的任何信息应该是公开的，把非法侵入他人系统窃取信息当做正当行为；有的人认为软件应当免费公用，大肆侵犯他人的版权，甚至以盗版为常业；有的人认为网络空间言论行为绝对自由，一时间网络空间充斥着各种违背社会公德、法律法规的言论和行为，如在网络上传播淫秽信息和物品、犯罪方法、种族歧视和纳粹主义言论；有的人则专门在网络上进行诈骗。反主流亚文化群体成员分布广泛而分散，数量庞大，遍布全球，他们借助互联网络联系和交流，形成一个个各有特征的子群体。以黑客为例，在西方社会“黑客”已成为一个成员广泛的社会群体，存在合法的“黑客”组织、“黑客”学会，1997 年 11 月在纽约召开的世界“黑客”大会就有四千多人参加。在互联网上，“黑客”组织有公开的网址、信道，提供免费的“黑客”软件，介绍“黑客”手法，出版“黑客”杂志（如《2600》杂志）和“黑客”书籍（如《Hacker Proof》介绍攻击手法长达 700 页）。反主流亚文化在交流过程中得以发展，反过来进一步影响更多的人，在更大的范围内传播。

凭借技术在网络空间获取不受限制的绝对自由，这种思想极具蛊惑力，特别是对 20 岁左右的年轻网民具有极大的影响。全

球头号电脑黑客凯文·米特尼克入狱五年间，一直受到很多网民的关注，甚至有人设立了“释放米特尼克”网站，为其出狱进行倒计时①。21 世纪社会信息化网络化程度将进一步提高，计算机信息技术对社会更具影响力，上网用户将越来越多，反主流亚文化影响不但不会消亡，反而会在更庞大的网民群体中存在和发展。如果网络空间亚文化得不到恰当的引导和治理，反主流亚文化将成为一股不可轻视的网域潜流，成为一部分人根深蒂固的信仰和观念，误导那些年少无知、初涉网域的年轻人，成为这些人违法犯罪的内因。

二、电子商务安全管理落后

电子商务安全管理是遏制电子商务领域犯罪最直接的力量，同时，电子商务安全管理的缺陷是犯罪发生的直接原因和条件。电子商务发展的时间不长，其安全防范体系远未完备，主要存在以下几方面缺陷：

（一）技术设备存在安全隐患

电子商务的物质技术基础是互联网，设计互联网的初衷是方便信息交流，而不是保护信息安全，即当信息在互联网上传输时，中间要经过多个网络设备，从这些网络设备上都能截获信息。互联网本身的松散结构，使互联网上的信息安全管理存在难以克服的困难。此外，互联网是一个软件与硬件的结合体，在目前的网络应用中，每个网络上都有一些自行开发的应用软件在运行，这些软件的技术缺陷可能导致网络运作不正常或瘫痪。

电子商务系统建立在信息设备基础上，这些由软硬件系统组成的信息设备是否安全可靠，将直接影响电子商务系统的安全。在目前电子商务应用中，技术设备的安全隐患主要表现在以下两

① 力霜：《网络安全专家留神：全球头号黑客出狱》，《深圳特区报》，2000 年 1 月 23 日第 4 版。

方面：(1) 设备的选型购置考虑不够，没有从质量、功能、性能以及厂商能提供的售后服务等多方面综合考虑，选用的设备型号不统一，或者设备兼容性不好，都会导致安全体系的漏洞。(2) 目前广泛应用的某些关键软硬件设备，如操作系统、中央处理芯片、网络设备如路由器等，被几家大公司、企业垄断，由于这些设备的技术保密，人们难以觉察出技术上的安全漏洞。一旦这些技术缺陷为犯罪人发觉，将在人们没有防备的情况下造成严重的损失。例如美国微软公司出品的 Windows98、Windows95、IE5.0 中都存在安全漏洞；世界最大的 CPU 制造商英特尔公司在奔腾Ⅲ处理器中，设置了用以识别用户身份的序列码，网络用户如果使用奔腾Ⅲ为中央处理器，那么他在互联网络上的一举一动都可能被他人监视。路由器是网络安全的关键设备，是防止黑客破坏的基础，由于技术等方面的原因，我国电子商务企业大量应用的还是国外的路由器，这增大了电子商务系统的不安全系数。

(二) 安全技术保护效果的相对性

保护电子商务信息系统的基本屏障是安全技术。目前主要有防火墙技术、加密技术等，这些措施在一定程度上能够维护系统安全，但是，由于电子商务领域犯罪的方法多种多样，既有来自外部的非法侵入者，也存在内部人员作案的可能性，以上安全技术对于“家贼”就无能为力了。目前发生在金融系统的刑事案件中，有相当一部分是内部人员绕过安全防范措施实施的。并且，技术上的保护具有相对性，例如防火墙是内部网络和外部网络之间的安全防范系统，可以防止非法用户的访问，但是不能防止不经防火墙的攻击；加密技术能够很好地保障网络上传输信息的机密性，高位公私密钥加密算法能使解密的可能性几乎为零，但是，由于解密的数学研究日新月异，计算机性能发展十分迅速，网络协作运算成倍地提高了破密运算能力，曾经被认为是“固若金汤”的加密算法在一定时间后也会失去保护作用。比如，长度

为 40 比特和 48 比特的 RC5 算法、56 位的 DES 算法以及 512 位 RSA 公钥因子已经被攻破①。

（三）电子商务安全管理的疏漏

安全技术措施对外有效，对内却难以成功。安全管理的疏漏是内部人员成功作案的重要原因和条件。电子商务安全管理疏漏表现在多方面，主要有：(1) 操作口令管理不善。不同职务的工作人员使用的口令权限不配套，一般操作人员具有超过工作需要权限的口令；口令设置长度过短，过于简单，容易被猜出；口令没有定期更换等等。(2) 人事权限分配不当。一人同时兼任相互监督的两个或者两个以上的职位，给犯罪人作案并销毁罪证创造了条件，如计算机编程人员同时担任操作员，计算机终端操作员同时兼任账目稽核员等。(3) 电子商务系统缺乏有效的安全监测。系统安全监测不仅要利用计算机程序自动监测、记录电子商务信息系统中用户的各种操作，还要有专门安全人员，监视操作人员工作时的非正常行为。如使用他人的身份和权限操作系统，将系统的保密数据备份带出工作场所等。(4) 事后报案追查不积极。有些经营单位对避免犯罪抱有侥幸心理，或者担心案件公开导致企业信誉下降和对手企业抢走客户，发案后不积极报案侦查，客观上纵容了犯罪行为人继续作案，同时，对日常经营过程中的违法违规行为处理不善，也给内部人员以管理松散的感觉，诱使某些不稳定分子利用管理的疏漏铤而走险。

（四）经营人员对安全和效用选择的失衡

电子商务应用能节约生产投入，提高经营效益，但同时也面临电子商务领域犯罪的威胁，而建设高层次的安全保护措施投资巨大。有些电子商务信息经营人员认为，采用电子商务信息系统而可能遭受犯罪侵害带来损失，是企业经营的正常风险，实际发

① 《512 位 RSA 公钥因子被破解》，http：//www.chinaeb.com.cn/security/security.html，2000 年 4 月 28 日。

生犯罪的可能性并不大，造成的损失也有限，与电子商务带来的效益和节约的巨额投资相比，损失要小于盈利，因此，往往不愿意投入足够的资金完善电子商务安全体系。实际上，薄弱的安全保护措施是犯罪的诱因，加之，电子商务领域犯罪具有隐蔽性、继续性的特点，可能导致犯罪多次发生，造成严重后果。

（五）经营单位内部人事关系、劳资关系恶化

许多电子商务领域犯罪的行为人曾是单位内部人员，或者与经营单位有合作关系。由于内部人事关系恶化，离职人员出于报复的心理对原单位进行破坏，或者意图从原单位获取非法利益来求得“补偿”。此外，单位的内部技术人员或者与单位有合作开发协定的人员，由于担心单位不履行应付义务，或者事先被迫接受了经营单位的歧视性合同，试图通过技术要挟的手段迫使经营单位就范，而在产品中设置破坏性程序或者进行其他破坏、威胁，导致劳资纠纷或者民事纠纷转化为犯罪行为。

三、反常的公众心理因素

电子商务领域犯罪和其他犯罪一样具有严重的社会危害性，但它具有区别于传统犯罪的特点，人们往往难以把它同暴力、欺诈等犯罪等同对待，甚至有些人不仅不把它视做犯罪行为，而认为是一种超人的英雄行为，这种反常的公众心理状况减轻了犯罪分子的罪恶感，甚至激励了一部分人“锲而不舍”地去体验这类犯罪的感觉，在客观上成为电子商务领域犯罪的诱因。导致反常社会公众心理的原因主要有：

（一）犯罪人形象使人难以把他们与罪犯等同

首先，电子商务领域犯罪的犯罪人多是 20 岁左右的青少年，具有较高文化程度，多为内部技术人员，从他们年轻而文质彬彬的脸孔上难以想象出罪犯的形象。其次，这类犯罪行为方式隐蔽，很少使用物理破坏手段损坏设备，行为对象多是那些封闭机箱中的计算机数据和应用程序，造成的损害难以为公众直接了

解。而且，受损害的多为大中型企业，公众难以见到个人直接受害的凄楚场面。电子商务领域犯罪客观方面的这些特点，使公众难以将他们与明火执仗、欺贫凌弱的犯罪分子归为一类。再次，犯罪行为人落案后，往往声称行为的目的只是为了游戏，或者测试自己的计算机技能，而且，这类犯罪人大多经济条件较好、受教育程度较高，公众往往倾向于接受犯罪人开脱罪行的解释，不把他们当做犯罪人看待。

（二）电子商务领域犯罪的特点给犯罪人和公众造成错觉

电子商务领域犯罪直接作用的一般是计算机信息系统，这给犯罪人一种心理错觉，认为“作案人充分利用自己的知识和能力以及接触计算机的机会（他们的受信任地位），想要‘打败机器’的动机常常起一定作用。他们在进行犯罪活动之前设法从心理上自我安慰，他们想象：被害人是匿名的，万一造成损失也会落到许多人头上，不会给企业造成重大损失……公众舆论并不把计算机犯罪视为‘真实的、日常的、一般的’犯罪”①。电子商务领域犯罪往往是个人或者较少人攻击安全设备林立、专业人士如云的大单位，力量对比悬殊，结果却出人意料，这使那些苦于学习计算机技能的人们十分钦佩，正如日本学者西田修评价的，“不少人觉得，利用计算机实施犯罪是一种智慧的表现……因为它是钻进采取了周密的安全措施的电子计算机里把钱偷出来的。不！或许连偷都谈不上，只不过躲过了银行的安全系统，使计算机为自己工作，然后理所当然地得到了银行的报酬而已。要说犯罪感，恐怕拾起他人掉在路上的一万日元钞票塞进自己的腰包，要比通过计算机搞到一亿日元现金其犯罪感还要来得强烈些。对于不附加任何暴力、稳稳当当实施的计算机犯罪，不少人都怀着羡慕的心情赞叹道：‘干得真漂亮！’甚至可能有人会这样想：这计

① ［德］汉斯·约阿希姆·施奈德：《犯罪学》，中国人民公安大学出版社 1990 年版，第 72 页。

算机我拼命学还搞不大懂，可他竟能用它来干‘坏事’，这家伙定非等闲之辈！倘若我也有干这一手的本事……”① 这种反常的公众心理不仅没有给犯罪人以应有的谴责，反而给犯罪人以心理上的奖赏，诱使一部分人加入犯罪的行列。

四、法律控制体系不完善

互联网是从20世纪60年代美国国防部的ARPA网演变发展而成的，它的大发展始于80年代末90年代初。从全球范围看，互联网的发展几乎是在无组织的自由状态下进行的，到目前为止，世界范围内还没有一部完善的法律来规范和引导互联网的发展。由于没有健全法律的约束，缺少强有力机构的管理，互联网自然成为一些犯罪人“大显身手”的理想空间。

法律是遏制电子商务领域犯罪的重要力量，法律控制力量强，犯罪危害程度就会降到较低的水平，反之，如果法律控制不力，这类犯罪的发案率必然上升，社会危害也将增大，同时导致犯罪分子藐视法律，胆敢以身试法。目前控制电子商务刑事立法体系的缺陷，主要表现在以下方面：

（一）缺乏强制报案制度

利用法律手段打击电子商务领域犯罪，首先必须发现并举报犯罪事实，然后才可能有侦查机关的侦查、起诉机关的起诉、审判机关的审判活动。由于电子商务领域犯罪具有很强的隐蔽性，有相当一部分犯罪事实并没有为被害人发觉。在电子商务企业觉察到自己受到侵害的案件中，又有相当一部分被害人担心自己的声誉受到影响，除非影响巨大，否则都不愿意承认自己的网络被侵害，有时即便通过技术手段查出了黑客的踪迹，甚至有人承认对此事负责，被害单位也遮遮掩掩，不肯承认，宁可自己“消

① ［日］西田修：《浅谈电子计算机犯罪》，群众出版社1986年版，第1～2页。

化”损失，也不向有关部门报案，导致大量的案件停滞在被害人报案阶段，犯罪人得不到法律追究，逍遥法外并一再作案。电子商务企业不报案的原因有很多，如发生在企业的电子商务领域犯罪不明显，而且损失往往可以转嫁给消费者；对这类犯罪的侦查、起诉、审判往往需要与司法机关协作，占用了单位有限的资源和时间；案件处理难度大，往往不了了之；侦查可能导致公司内幕的泄露；担心经济信誉受损并被竞争对手抢走客户等等。

电子商务领域犯罪不仅仅是被害人个人遭受损害的问题，犯罪是否受国家法律的追究，不能由电子商务企业决定。国家应规定企业强制报案制度，否则，相当一部分犯罪能够借助这一法律漏洞逃脱制裁。

（二）国内相关法律体系不完善

法律是司法工作的依据，完备的法律体系是有效打击电子商务领域犯罪的重要保证，反之，将使司法工作的开展处于无法可依的境地，更谈不上打击犯罪。由于电子商务领域犯罪是新发展起来的一类犯罪，相关刑事立法极为有限，法律的滞后使这类案件的侦查、起诉、审判遇到很多问题。相关刑事立法的缺憾，主要表现在两个方面：

1. 缺乏相关的程序法：(1) 缺乏相关证据法律。电子商务领域犯罪留下的作案痕迹大多是计算机数据文件或者记录，有的案件中只有这类证据，因此，计算机数据的证据效力直接关系到能否成功侦查、起诉和审判。各国对计算机数据证据效力的规定各不相同，有的国家不承认它们是有效证据，有的国家把它作为警察侦查证据，如英国 1984 年《警察刑事证据法》第 19 条第 4 款规定“警察可以根据计算机中的情报作为证据”。我国现行的《刑事诉讼法》第 42 条把视听资料作为证据，经过查证属实后作为定案根据，但是计算机数据是否属于视听资料，法律尚未明确规定。(2) 缺乏有关管辖权问题的法律。电子商务领域犯罪的重要特点是犯罪过程跨度大，犯罪行为地、犯罪结果地（含中间结

果地）往往不在一个司法管辖区内，有的涉及几个国家或者地区。如某黑客案件中，加拿大黑客非法侵入德国某高校计算机网络，并以该网络中的计算机为工具，攻击美国大型商业网站，造成严重后果，这类犯罪的犯罪行为地、中间结果地和犯罪最后结果地不在同一国家，如何协调这些国家的管辖权，目前尚无法律和条约规定，而司法管辖权的不确定必然阻碍对犯罪的侦查、起诉和审判。

2. 缺乏相关的实体法：（1）许多危害行为没有犯罪化。法律总是滞后犯罪的发展，对于有些电子商务领域的危害行为，缺乏可以适用的刑法条文，致使案件在成功侦查、起诉后仍被判无罪。如 1986 年 6 月瑞士报告了一起利用计算机诈骗案，行为人利用篡改磁带上的记录，把磁带上的记录转移到同案犯的账户下。案发后，地方法院根据行为人非法修改计算机数据文件的犯罪事实，判其有罪，但是上诉法院认为，修改磁带不能算作完全犯罪，行为人并未从中获得赃物，未构成犯罪事实，从而认定地方法院判决无效①。诸如此类法律没有明文规定的、具有严重社会危害性的行为还有很多，刑事法律的缺乏客观上纵容了电子商务领域犯罪。（2）刑事责任年龄的法律缺陷。由于计算机教育的普及，许多青少年都能够熟练使用计算机，相当一部分电子商务领域犯罪行为是青少年所为，特别在黑客犯罪案件中，青少年占有很大比例，法律对这些行为人如何处置？刑事责任年龄是影响行为人承担刑事责任的法定年龄，我国把 14 周岁规定为承担刑事责任的法定最低年龄，因此，对于未满刑事责任年龄的青少年实施电子商务领域犯罪的，即使造成社会危害特别巨大，也不能追究刑事责任，而只能作行政处罚和教育。实施电子商务领域犯罪不一定需要成年人的力量，而且，互联网络上充斥着各种犯罪

① 杨博：《计算机犯罪问题的若干法律思考》，《法商研究》，1995 年第 2 期。

方法信息和工具程序，这些方法信息和工具程序能被青少年轻易获得并用于犯罪。在网络应用道德与法制教育尚未健全的情况下，过于宽松的法律环境不利于威慑犯罪，阻止青少年实施严重危害社会的行为。(3) 刑罚设置的缺陷。对电子商务领域犯罪适用的刑罚多为自由刑，不适合于不需长期监禁的犯罪人和不适合判处自由刑的青少年犯罪人，不能在行为人实施较轻的犯罪时，及时予以矫正。

(三) 司法人员专业素质有待提高

侦查、起诉和审判等司法机关是与电子商务领域犯罪作直接斗争的部门，司法机关工作人员专业素质的高低直接影响了打击犯罪的效果。目前由于缺乏足够的兼有计算机、网络技术和电子商务专业知识的工作人员，司法机关难以有效打击电子商务领域犯罪。1991 年 7 月美国德州警察局在一次缉毒中，发现了一套正在工作中的计算机系统和存储贩毒成员名单和活动网络的磁盘，由于在场的警察不懂计算机技术，无法提取犯罪证据，只好把计算机和磁盘全部运往警察局。但由于计算机和磁盘被同车运送的其他通信设备电磁干扰，磁盘和计算机系统中数据大多丢失，痛失破案良机①。美国某法院在审理一个黑客案件中，由于法官不懂计算机知识，在法庭调查中被迫要求犯罪嫌疑人向他们解释有关技术问题。现在世界各国已经开始重视打击电子商务领域犯罪，并逐步建立专门机构和对司法工作人员进行培训，但是仍不能适应与电子商务领域犯罪作斗争的需要，因此司法人员基本素质有待进一步提高。

(四) 国际司法协助尚未建立

电子商务从其诞生开始就是国际性的商务活动，同样，电子商务领域犯罪也是跨国性的犯罪，犯罪人所在地、犯罪行为地和

① 刘广三：《计算机犯罪论》，中国人民大学出版社 1999 年版，第 134 页。

犯罪结果地往往不在一个国家。一国为调查犯罪事实，往往需要跟踪行为人，未经授权进入其他国家的计算机信息系统获取证据，而这是对他国主权的侵犯，必然遭到他国的反对，因此，为有效惩治这类犯罪，必须建立有效的国际司法协助，否则国际互联网络可能成为这类犯罪的“避难所”。例如 1997 年克罗地亚的三名中学生通过国际互联网络侵入美国军事计算机系统，美国发觉后向克罗地亚要求引渡这三名学生，被该国拒绝，理由是克罗地亚不承认非法侵入计算机信息系统是犯罪①。虽然近年来某些发达国家也正在组建打击网络刑事犯罪的区域性司法协助，如西方 8 国部长于 2000 年 5 月举行网络刑事犯罪的专门会议，以通过一项联合对策，对付网络犯罪行为②。但是，目前国际范围内的司法协助尚未形成，涉及他国司法管辖权的电子商务领域犯罪难以得到有效的惩治。

① 陈兴实、付东阳：《计算机、计算机犯罪、计算机犯罪的对策》，中国检察出版社 1998 年版，第 27 页。

② 《西方重组八国联军，一致对付黑客》，http://www.ccidnet.com.cn/ 2000 年 2 月 17 日。

第三章　黑客和有害计算机程序问题

电子商务诞生伊始，安全问题就一直是人们十分关注的问题，但是谁也没有认识到，目前电子商务信息系统竟如此脆弱！2000 年 2 月 7 日开始，美国接连发生攻击大商业网站的事件，雅虎、微软、美国 CNN 新闻网站、全球经济组织网站等世界规模最大、安全性能最强的八大商业网站，先后遭到黑客攻击而陷入瘫痪，几天内造成的损失超过 10 亿美元①，而后，世界其他国家也相继发生了黑客大规模攻击网站造成重大损失的事件。2000 年 5 月一种叫做“我爱你”的电脑病毒在全球各地迅速传播，4 500 万台电脑受到攻击，造成的经济损失达 100 亿美元②。这两次事件暴露了电子商务物质技术基础的脆弱，使人们清醒地认识到，即使是被认为安全性能最强的大商业网站也不安全，更何况安全性能较差的中小商业网站。电子商务系统安全是电子商务安全的基础保障，电子商务系统脆弱是电子商务安全的根本大患，也是电子商务领域犯罪屡屡发生的诱因。电子商务领域犯罪中犯罪种类繁多，造成的危害影响程度各异，其中对电子商务影响最大的是黑客犯罪和有害计算机程序犯罪，它们比电子商务领域中的其他犯罪现象有更复杂的社会文化背景。因此，有必要将这两个问题专门抽出来，从犯罪学和刑事政策学的角度予以分析、研究。

---

① 《损失惨重影响深远》，《深圳晚报》，2000 年 2 月 14 日。

② 《“爱虫”让你没商量》，《金融早报》，2000 年 5 月 9 日。

第一节 黑客问题

黑客攻击事件并非21世纪才有的事情，早在20世纪60年代，黑客和黑客攻击就已经存在，但是，引起人们对黑客关注的是2000年的若干次黑客攻击大型商业网站的事件。这些严重事件引起了世界各国的震惊，克林顿总统召开网络安全高级会议，与网络公司和政府专家共商反黑客袭击的对策，美国司法部等联邦机构发誓要缉拿真凶。掀起“惊涛骇浪”的黑客是些什么人，做了些什么事情，对社会信息化和电子商务发展起了怎样的作用，对这些问题的认识，直接影响到对黑客问题所采取的对策，因此，深入分析研究黑客及其行为具有重要意义。

一、黑客的概念与分类

（一）黑客的概念

黑客是英文单词Hacker的中文译音，从字面上理解，Hack的意义是“劈砍、乱砍”，其引申意义是“干了一件十分漂亮的工作”。Hacker是指“劈砍、乱砍的人”，目前Hacker很少被理解成这一意义，而是计算机科技应用领域的一个专用术语。黑客一词没有严格的定义，其含义随计算机应用的发展而有所变化。由于近年来发生了多次严重的黑客攻击事件，加之中华文化对“黑”赋予了传统的贬义思维，在中国老百姓的心目中，黑客成了网络犯罪人的代名词。“黑客”究竟指代为何？有必要追根溯源。

黑客成为与计算机及网络相关的名词，起源于20世纪50年代美国麻省理工学院的实验室里，当时黑客是形容独立思考、喜欢钻研计算机技术奥秘并从中增长个人才干的奉公守法的计算机迷。他们崇尚技术，反抗权威，从事黑客活动的目的是希望对计算机系统的最大潜力进行智力上的自由探索，尽可能地使计算机

的使用和信息的获得成为免费和公开的。1969 年 ARPA 网建立起来，为 ARPA 网工作的、由计算机程序设计专家和网络名人组成的高技术人才群体，赋予了 Hacker 新的含义，他们不断地挑战技术的极限，为推动计算机网络技术及应用的发展作出了巨大贡献。可以说在 20 世纪 60～70 年代，黑客是指那些具有高尚的品格、渊博的知识和创新的精神，以其卓越的技术成就推动计算机及网络应用发展的计算机技术人才。

随着计算机应用的发展，社会对计算机信息系统的依赖性越来越强，控制了计算机信息系统就意味着控制了现实的社会，这种不受制约的能力一旦失去方向，必然引起令人恐怖的结果。黑客技术既可以推动社会信息化的发展，也可以用于犯罪，是信息社会里一把锋利的“双刃剑”。

20 世纪 80 年代以来，黑客队伍也迅速壮大，目前已成为一个广泛而特殊的社会群体，在欧美等国有黑客组织或黑客学会，黑客们经常召开黑客技术交流会，1997 年 11 月在纽约召开了世界黑客大会，参加人数达四五千人，其中大多是十几岁到三十几岁的年轻人。同时，黑客团体也出现分化和演变，黑客中的很多人具有反社会色彩，甚至有些黑客专门打涉及商业秘密和国家秘密的计算机信息系统的主意，“黑客”的含义也有了新的演绎。

在这一转变过程中，有两件黑客事件证明了黑客团体的这一演变。其一是 1986～1989 年原联邦德国黑客团伙“汉诺威”集团在克格勃的指使下，试图侵入美国军事计算机网络刺探机密情报，这一事件在原联邦德国电视上曝光后，在公众中引起巨大反应。其二是 1988 年 11 月发生的莫里斯蠕虫案，美国康奈尔大学学生罗伯特·泰潘·莫里斯，将自己编写的网络蠕虫病毒安放在麻省理工学院的网络上，病毒在 ARPA 网上迅速传播，导致成千上万台计算机陷入瘫痪。从此，黑客团体泥沙俱下，鱼龙混杂，其成员组成及动机日益复杂起来，不仅包括那些奉公守法的计算机迷，还有相当一部分利用计算机、网络危害社会的人。后者使

黑客“名声大振”，也玷污了黑客的名声，使人们误认为黑客就是指那些利用计算机、网络技术实施违法犯罪活动的人。

关于黑客的定义，不同的人有不同的理解。有人将黑客定义为，“一个计算机狂热者，他特别精通计算机技术”或者“试图获取计算机系统非法授权访问的计算机用户”；也有人将黑客定义为，“一个未获得计算机系统访问的、非法或滥用计算机访问权（使用权）的人，他热衷于研究计算机操作系统”；还有人将黑客定义为“网络恐怖主义分子”。从上可以看出，黑客具有以下特点：(1) 利用计算机或者网络技术；(2) 未被授权进入并使用他人计算机信息系统，有些还有后续行为，如窃密、破坏等等。作者认为，黑客的概念是一个历史范畴，它是特定时期的产物，同时，随着社会发展其内涵和外延不断变化。现在黑客团体已嬗变为一个组成十分复杂的特殊社会群体，为准确描述这一群体，取其共性对黑客作以下定义：黑客是指利用计算机、网络等信息技术，未经授权侵入计算机信息系统，并可能有其他后续行为如干扰、破坏、窃密的人。同时还需要说明的是，利用计算机病毒程序、“逻辑炸弹”程序等有害计算机程序实施黑客攻击的人，当然也属于黑客。但是，由于这类行为具有不同的特性，人们一般不把它们归入黑客攻击的行列，而将它们看做另外一类危害行为。本书也采纳这种观点，对利用计算机病毒等有害计算机程序危害计算机信息系统安全的在其他章节分析。

（二）黑客的分类

黑客团体人数众多，组成复杂，如果不加区别，容易导致错误打击。因此，必须对他们进行分类，以利于制定区别对待的对策。目前对黑客的分类有多种，如我国有学者将黑客分为这样三类：(1)“为了证实自己的能力，不断挑战计算机网络极限”的黑客；(2)“凭借自己掌握的高超技术手段，以在网上骚扰他人为乐”的黑客；(3)“由于从小遭受家庭变异，心情受到严重创

伤，产生一种渴望报复社会的心理态度”的黑客①。有人把黑客分为七类：(1) 恶作剧型。喜欢进入他人网址，以删除某些文字或图像，篡改网址主页信息来显示自己高超的网络侵略技巧。(2) 隐蔽攻击型。躲在暗处以匿名身份对网络发动攻击性行为。(3) 定时炸弹型。网络内部人员故意在网络上布下陷阱，或在软件内安插逻辑炸弹，在特定的时间或特定条件下引发一系列破坏行动。(4) 制造矛盾型。秘密侵入网络修改他人商业信息或者政府公告，以扰乱市场交易秩序或者社会秩序。(5) 职业杀手型。这类黑客专门实施破坏行为。(6) 窃密高手型。出于某些集团利益的需要或者个人的私利，利用高技术手段窃取商业秘密或者国家秘密。(7) 业余爱好型。这类黑客出于好奇心寻找他人系统上的漏洞，并帮助修补漏洞和防止损失扩大②。

对黑客团体的分类，是为了更好地认识其基本特征。以上两种分类都在不同程度上揭示了黑客团体的特征，对认识黑客的复杂性大有帮助，其缺陷在于分类参照的依据不明确，不利于科学地揭示黑客团体的组成和各类黑客特征。作者认为，从犯罪学和刑法学研究的角度，以黑客主观方面的目的动机和对社会的影响为依据，可以将黑客分为技术挑战性黑客、戏谑取趣性黑客和捣乱破坏性黑客三种类型：

1. 技术挑战性黑客。简称挑战性黑客，也被称为“白帽子黑客”，是指对于计算机、网络技术奥秘有强烈兴趣的人。他们大多数深谙计算机、网络技术，为了提高自己的技术水平，不断挑战计算机技术的极限。这些人出于猎奇好胜的心理侵入他人计算机信息系统，试图从中发现系统技术上的漏洞及其原因，并公开他们的发现与其他人分享，在主观上并无反社会的色彩。例

① 毛惠辉：《黑客——惟我独尊的“网络骑士”》，《科技日报》，1999年6月23日。

② 林皓：《黑客的类型》，《光明日报》，1999年3月10日。

如，2000 年 5 月美国阿帕奇软件基金会网站被黑客侵入，Apache软件基金会的董事会成员 Rasmus Lerdorf 指出，黑客的动作还算有所保留，其实网站的服务器已经完全被黑客控制，他们可以把整个网页恶搞一阵，却只在首页的下方挂上这个微软的假广告，黑客还将入侵的方法也告诉了 Apache，似乎提醒 Apache 要改进安全防护措施①。这类黑客大多人格正直，技术能力较强，有些还是网络安全专家，他们虽然擅自侵入他人的计算机信息系统，但并不实施破坏行为，有些还帮助单位发现并堵塞系统漏洞，甚至还帮助修正系统。他们的行为在一定程度上推动了计算机网络安全的进步，但是，他们未经他人允许擅自侵入他人计算机信息系统，是对他人权利的侵犯，其实质是法律禁止的违法行为。

2. 捣乱破坏性黑客。简称捣乱性黑客，有人还称之为“黑帽子黑客”，或称之为 Cracker（骇客），以与第一类黑客相区别，目前媒体和大众眼中的黑客多半是这类黑客。捣乱性黑客主观上具有牟取非法利益、窃取秘密、破坏、干扰等目的。捣乱破坏性黑客组成十分复杂，依据不同标准可以进行以下分类。

按照黑客是否具有政治目的，可以分为有政治目的的捣乱性黑客和无政治目的的捣乱性黑客。有政治目的的黑客事件有：1998 年印尼排华事件后，有些华裔黑客对印尼政府各部门的电脑系统进行了攻击；2000 年日本右翼团体公开否认日本在第二次世界大战中的侵略罪行，随后，日本首脑机关的计算机信息系统连续遭受黑客的攻击②。2000 年 3 月祖国大陆的黑客被陈水扁的台独行径激怒，大举攻击台湾的商业网站。

按照捣乱性黑客行为人技术水平的高低，可以分为技术水平

① 《Apache 网站被黑客换掉首页》，http：//www.sina.com.cn／2000 年 5 月 9 日。

② 《黑客大闹霞关街》，《科技日报》，2000 年 1 月 29 日。

较高的黑客和技术水平较低的黑客。前者深谙计算机、网络安全技术，具有较高的编程能力，能够开发用于黑客攻击的工具软件，往往攻击影响大、安全性能高的重要网站，如 2000 年 2 月发生的黑客攻击美国八大商业网站就是这类人所为。后者一般不能开发攻击工具软件，但是能熟练使用网上提供的黑客程序，攻击安全性能不高的中小网站和政府网站，如对美国大型商业网站的攻击结束后，持续发生的针对较小网站的攻击，就是这类人所为。

3. 戏谑取趣性黑客。简称戏谑性黑客、恶作剧黑客。这类黑客通常凭借高技术手段，以在网上搞恶作剧或骚扰他人为乐，例如 1996 年 9 月美国中央情报局的网页篡改成“中央愚蠢局”；美国司法部网站主页上的“司法部”被改成了“非法部”；2000 年 2～3 月间墨西哥总统塞迪略成了网络黑客骚扰、偷袭的热门对象，他先后三次被匿名黑客冒名顶替、移花接木，闹得总统府上下不安①。这类黑客徘徊于违法与犯罪之间，随时都可能跌入犯罪的深渊，也被称为“灰帽子黑客”。

二、黑客犯罪的基本特征

（一）黑客结构特征

1. 从年龄结构来看，黑客年轻化倾向越来越突出，十几岁到三十几岁年龄段的黑客占据很大比例。1998～2000 年发生的黑客案件反映了这一特点。如 1998 年 2 月，美国五角大楼计算机信息系统被三名黑客侵入，并在被发现的情况下还进行了将近一周的骚扰，美国国防部费尽九牛二虎之力后将三名黑客擒获，令人吃惊的是他们中最大的一位年仅 18 岁；3 月，两名 16 岁的少年入侵德国最大的因特网服务商 T-Online，窃走了几百个银行

① 张宇清：《墨总统屡遭黑客袭击》，《检察日报》，2000 年 3 月 22 日。

账号资料；6 月，三个十几岁的国际黑客组成的 Milworm 黑客小组成功侵入印度原子研究中心，导致印度原子能研究所的主页页面瘫痪，并下载了 5MB 的数据及电子邮件信息，以此抗议该国当时进行的一系列核试验；7 月，Milworm 黑客小组中一个自称 JF 的 18 岁黑客，在网上一手导演了一场声势浩大的反核试验抗议行动，一举闯入了包括世界杯和沙特皇家站点在内的三百多个网站，并将蘑菇云图像和反核试验宣言张贴到了这些站点的主页上。在我国，青少年黑客也占很大比例，1998 年 4 月，年轻的章某为帮助炒股的朋友解套，偷袭一证券公司，窃取客户股票信息；7 月，江西多媒体通信网遭受 19 岁的黑客的攻击，被迫停用两天；7 月，上海某高校计算机系保送研究生杨某攻击了上海最大的公用信息平台；9 月，原中银奥力威集团教育行业部职员，21 岁的杨某攻击福建省图书馆计算机系统，造成省图书馆服务器两次关闭。2000 年 2 月攻击雅虎、亚马逊等著名网站的黑客嫌疑人之一是 15 岁少年，而编写攻击程序的是一位不满 20 岁的德国青年米克斯特。

2. 从所受文化教育程度来看，这些犯罪人往往受到了较好的计算机技术教育，相当一部分人具有大学本科以上学历。他们在犯罪过程中，能够有效地运用所学的计算机技术，表现出较高的智能性。但是，随着计算机、网络应用的迅速发展和计算机教育的普及，犯罪人与教育程度之间的正比关系越来越不明显，相当一部分人不是通过接受高等教育，而是通过自学掌握了计算机、网络技术，包括黑客攻击技术。此外，由于互联网中有许多黑客软件和攻击网站的犯罪方法信息下载，具有一般计算机操作技能的人根据黑客软件的说明文件按图索骥，就可以侵入他人网站。

3. 从黑客攻击的组织形式看，黑客攻击活动由单个人实施向黑客团伙协作实施发展。目前攻击中小网站的大多是具有一般黑客技术的单个黑客，攻击安全性能较高、影响较大的大型网站

和军事网络的，多是具有较高黑客技能的黑客团体。如 1998 年 2 月 26 日，五角大楼重地的四个海军系统和七个空军系统的电脑网页遭侵入，更令人吃惊的是黑客的侵入在美国国防部已经发现的情况下，连续进行了整整一周的“骚扰”活动。黑客在网络系统内安置了一个“暗门”，使得他们随时可以进出而不被发现。美国国防部特别办案组经过调查，发现黑客是两名 15 岁的美国少年和一名 18 岁的以色列少年“分析家”，他们在因特网上的“聊天室”里认识后，与其他两名以色列青年共同组成了一个名叫“力量”的组织，在入侵机密网页时分工协作，一个人进入系统，一个人写 HTML 文本语言，两个人负责在网上“冲浪”搜寻网址，另外一个人则负责安全工作，消灭经过的路径。目前黑客组织发展非常迅速，数量不断增加，他们经常召开黑客技术交流会，“切磋技艺”，黑客组织的建立及其活动，大大增强了攻击网站的能力，如果引导管理跟不上，将对世界各地网站安全构成极大威胁。1999 年以来屡屡有所表现的黑客组织有：Forpaxe（出现于 1999 年初，与侵入一些大学网站、少数政府和军事网站的黑客事件有关，在黑客圈子和公众媒体中很有名）、Goat Security-GS（也称“山羊组”）、GH（也称“全球地狱”，是世界最具知名度和被媒体曝光最多的黑客团体，攻击过诸如白宫、军队主页等这样高度敏感的网站）、Level Seven（也称“第七层”）、Keebler Elves（到 1999 年为止技术最高的黑客组织，有很多经验丰富的成员，曾经袭击教育部、Monmouth 军事基地等）、HFD（Hacking for Drunks，曾经袭击 20 世纪福斯公司网站）、Blow Team（巴西黑客组织，曾经制造 2600.co.uk 和 Telemar 黑客事件）以及中国的“绿色兵团”和“中国天语”等。

（二）黑客犯罪的目的与动机

黑客团体组成复杂，各类黑客侵入他人计算机信息系统的目的动机各不相同：

1. 白帽子黑客的动机多为测试和提高个人技术能力，学习

系统安全技术，也有帮助他人发现、堵塞系统漏洞的。例如，1995 年美国加州大学的研究生伊恩·戈德伯格和大卫·瓦格纳两人，发现网景公司设计的用于网上购物的软件程序中的一个漏洞，并将其公诸于众，网景公司随即推出了该程序的修正版，但紧接着这两名黑客又发现了新程序的漏洞。伊恩·戈德伯格和大卫·瓦格纳自诩为爱挑剔的学生。

2. 黑帽子黑客的目的动机有多种，归纳起来主要有以下几种：(1) 以窃取他人财物或者谋取其他利益为目的。如 1998 年 8 月我国原工商银行职员郝景龙利用熟悉银行计算机终端机的操作和银行业务程序的便利，与其弟郝景文合谋盗窃金融机构资金，郝氏兄弟在银行计算机系统专用线路上接入的无线侵入装置，非法侵入金融计算机系统，向事先准备的 16 个账号转移资金 72 万元，实际取出 26 万元人民币①。(2) 以盗窃秘密信息为目的，同时还可能有牟利、政治目的等其他间接目的。如 2000 年 3 月 30 日欧盟议会证实，美国在全球有一个名为“梯队”的监听网，并大肆对欧洲盟国进行商业窃听活动②。(3) 以骚扰破坏为目的，其中有些黑客有报复、泄愤等动机。2000 年 6 月，中国太平洋保险公司郑州分公司的公司计算机系统遭“黑客”非法侵入，部分关键数据被更改。经警方调查，发现是原在这家公司主管计算机系统维护编程的系统管理员王波所为，其侵入网络破坏的动机，主要是听人说公司经理认为他的技术不行，心理上感到不平衡，想借此办法显示一下自己的技术能力并进行报复③。(4) 以政治破坏为目的。如 2000 年 4 月，被怀疑是塞族支持者的黑客连续攻击了五十多家网站，令网络世界再度紧张，

① 《扬州公审电脑“黑客”》，《楚天都市报》，1999 年 1 月 10 日。

② 《欧盟强烈反对美监听活动》，《科技日报》，2000 年 4 月 4 日。

③ 《显示自己水平高，电脑“黑客”修改保险公司七百多份保单》，《电脑日报》，1999 年 8 月 9 日。

在被攻击的网站中，不乏知名网站，如 addidas.com、mgm.com、viagra.com 等，这些网站大多都在巴尔干地区，被黑客攻入的网站，其页面都被修改，网页被贴上双头鹰标志及支持科索沃塞族人的标语口号，如“科索沃是塞尔维亚的”等字句。

3. 灰帽子黑客的目的、动机，一般不是为了骚扰、破坏、窃密或者窃取财物，大多是显示技能、制造恶作剧或者戏谑取趣。有此目的、动机的人，大多是黑客技术、计算机网络技术一般，而希望引起网络同行关注的人。

（三）黑客犯罪客观方面的特征

黑客犯罪在客观方面表现为极强的隐蔽性和极严重的社会危害性。

其极强的隐蔽性的原因在于：(1) 在计算机、网络设备设施组成的信息空间里，行为人的网络身份难以确定，即使发觉犯罪事实、犯罪痕迹，也难以发现犯罪人。(2) 互联网络连通全球计算机信息系统，各计算机信息系统安全性能差别悬殊，安全性能差的可能被黑客利用来攻击其他计算机信息系统。如果黑客利用几地的计算机信息系统转接后再实施侵入的，要发现黑客留下的痕迹、追踪犯罪人就更加困难了。在 2000 年 2 月发生的黑客攻击美国大型商业网站事件中，美国斯坦福大学海洋研究所内的大约 50 台电脑曾被黑客用于攻击雅虎等大型网站，由于黑客使用上述方法，虽然美国政府费尽九牛二虎之力，仍然没有发现黑客的“真身”。(3) 计算机信息系统的技术特性使黑客能够及时消除留下的痕迹，如果没有专业技术人员的仔细调查，很难发现犯罪。(4) 现行法律关于犯罪证据的规定不适应这类犯罪，使黑客难以被有效起诉。(5) 被害单位鉴于破案率低，犯罪难以有效追究，加之担心企业信誉受损、受到犯罪人的继续报复，往往不报案，也使相当一部分犯罪得不到暴露。英国的星期日时报曾发表文章暗示，一些计算机黑客通过侵入银行计算机系统敲诈银行已经持续好几年了，由于担心投资者知道后影响银行股票价格，这

些银行都将此事件压下不表，默默地忍受黑客的敲诈，他们认为向黑客支付金钱要比银行系统被入侵事件曝光后带来巨额损失要划算。这导致黑客没有受到惩罚，从而更频繁地攻击银行系统。

其极严重的社会危害性在于，黑客犯罪能够造成极为严重的经济损失和极为恶劣的社会影响。以 2000 年 2 月发生的美国大商业网站黑客攻击事件为例，美国著名的研究和咨询公司扬基集团发表报告说，这次事件给 8 家大型网站所造成的经济损失可能在 12 亿美元以上，其中受害公司在 3 天内的损失高达 10 亿多美元，营销和广告收入损失 1 亿美元以上。受影响的公司及其互联网合作伙伴为了更新安全设施，将要另外花费 1 到 2 亿美元。这次袭击还给受害公司的品牌、合作关系以及未来的客户造成损害。不仅如此，这次黑客攻击事件还给美国经济带来巨大冲击，华尔街股市震荡，投资人信心动摇，道琼工业指数重挫 258.44 点，前三天连创新高的那斯达克指数也跌掉 64.26 点，雅虎公司股价跌了 10.813 美元，e-Bay 公司股价也跌了 5.75 美元。这就使人们对电子商务留下一个不安全的印象，给新兴的电子商务以沉重打击。

（四）黑客攻击的对象

根据被黑客攻击的计算机信息系统的性质和特点，可以分为以下几类：(1) 影响大、安全性能好的商业网站，如雅虎、微软等大型商业网站。黑客攻击这类网站，有的是为了检验黑客技术、挑战新的技术高度，有的是借以扩大影响。(2) 军事、政府网站。黑客攻击这类网站多是出于政治目的，或者是为了扩大影响。(3) 中小电子商务网站。这些网站因为安全性能较差，多被灰帽子黑客“欺负”。(4) 金融、证券行业等大型经营类商业网站。这些网站的安全往往直接联系着巨大的经济利益和企业的竞争优势，多被有牟利目的的黑客攻击，或者窃取财物，或者威胁、勒索。

三、黑客攻击的常用手段

黑客犯罪不同于传统的刑事犯罪，具有高技术性的特点，为了更好地遏制黑客犯罪，保护网络信息交流安全，有必要分析研究黑客攻击的一般过程和常用方法。

黑客攻击方法有多种，每种攻击方法的过程不尽相同，其一般过程如下：

1．收集被攻击方的有关信息，分析被攻击方可能存在的漏洞

了解被攻击的目标是黑客攻击的第一步。黑客要了解目标计算机所在网络的类型、IP 地址、操作系统类型和版本、系统管理人员的邮件地址等。根据这些信息进行分析，发现有关被攻击方系统中可能存在的漏洞，如运行一个 host 命令，可以获得目标网络中有关机器的 IP 地址信息，还可识别出目标机的操作系统类型，利用 WHOIS 查询，可了解技术管理人员的名字信息等。

2．建立模拟环境，进行模拟攻击，测试对方可能的反应

根据第一步所获得的信息，建立模拟环境，然后对模拟目标机进行一系列的攻击。通过检查被攻击方的日志，可以了解攻击过程中留下的“痕迹”。这样攻击者就知道需要删除哪些文件来毁灭其入侵证据。

3．利用适当的工具进行扫描

收集或编写适当的工具，并在对操作系统分析的基础上，对工具进行评估，判断有哪些漏洞和区域没有覆盖到，然后在尽可能短的时间内对目标进行扫描。完成扫描后，可对所获数据进行分析，发现安全漏洞，如 FTP 漏洞、NFS 输出到未授权程序中、不受限制的 X 服务器访问、不受限制的调制解调器、Sendmail 的漏洞、NIS 口令文件访问等。

4．实施攻击

根据已知的漏洞实施攻击。通过猜测程序可对截获的用户账号和口令进行破译，利用破译程序可对截获的系统密码文件进行破译，利用网络和系统本身的薄弱环节和安全漏洞可实施电子引诱（如安放特洛伊木马）等。黑客们或者修改网页进行恶作剧，或者施放病毒使系统陷入瘫痪，或者窃取政治、军事、商业秘密，或者进行电子邮件骚扰或转移账户资金等。

目前黑客攻击互联网的计算机信息系统的常用方法主要有以下几种：

1. 骗取口令法

在被攻击主机上启动一个可执行程序，该程序显示一个伪造的登录界面。当用户在这个伪装的界面上键入登录信息（用户名、密码等）后，该程序将用户输入的信息传送到攻击者的计算机，然后关闭界面给出提示信息“系统故障”，要求用户重新登录。此后，才会出现真正的登录界面。

2. 口令破译法

目前计算机信息系统安全保护的主要方法是口令保护，用户输入用户名和正确的口令，经系统查证后允许用户进入系统。口令破译是指破解口令保护或屏蔽口令保护。在实践中，真正的加密口令是很难逆向破解的，黑客常用的口令破译工具所采用的技术是仿真对比，利用与原口令程序相同的方法，通过对比分析，用不同的加密口令去匹配原口令。互联网上大多数服务器运行的是 UNIX 或类 UNIX 操作系统。在 UNIX 平台上，用户登录 ID 和口令都存放在 etc/passwd 中。UNIX 以数据加密标准 DES 为基础，以 ID 为密钥，对口令进行加密。黑客们破解口令的过程大致如下：首先将大量字表中的单词用一定规则进行变换，再用加密算法进行加密。看是否与 etc/passwd 文件中加密口令相匹配：若有，则口令很可能被破解。单词变换的规则一般有：大小写交替使用；把单词正向、反向拼写后，接在一起（如 cannac）；在每个单词的开头或结尾加上数字 1 等等。同时，在互联网上有

许多字表可用。如果用户选择口令不恰当，口令落入了字表库，黑客们获得了 etc/passwd 文件，基本上就等于完成了口令破解任务。

3. 特洛伊木马术

所谓特洛伊木马程序是指隐藏用户不希望的功能的程序，这些功能可能导致系统的私有信息泄露或系统被控制。例如黑客编写一种看起来像合法的程序，放到商家的主页，诱导用户下载。当一个用户下载软件时，这个特洛伊木马程序与用户的软件一起下载到用户的机器上，它会跟踪用户的电脑操作，静静地记录着用户输入的每个口令，然后把它们发送给黑客的电子邮件信箱。黑客据此获得了使用系统的密码，并对系统进行非法操作。

4. IP 地址欺骗法

互联网络中的数据是以数据包的形式，通过网络中的不同节点发送到目的地址，TCP/IP 协议允许给 IP 数据包设定通往目的主机的路径。黑客利用 TCP/IP 协议的这一特点，攻击企业防火墙保护下的内部主机。黑客要攻击防火墙后面一个受到保护而不可到达的主机 A，他只需在送出的请求报文中设置 IP 源路径选项，使报文有一个目的地址指向防火墙，而最终地址是主机 A。当报文到达防火墙时将被允许通过，因为它指向防火墙而不是主机 A，防火墙的 IP 层处理该报文的源路径域后，将其发送到内部网上，报文就这样到达了原本不可到达的主机 A。

5. 源地址欺骗法

防火墙过滤数据包的方法主要有两种，即“没有拒绝的就是允许的”和“没被允许的就是被拒绝的”。后者的安全性更强，只允许从指定范围的主机发来的数据包通过防火墙。即使如此，黑客也可以使用源地址欺骗法通过防火墙进入企业内部网络，黑客将有害数据包的源地址设定为内部主机地址，防火墙服务器会相信这个报文并使数据包顺利通过。

6. 网络嗅探器（Sniffer）攻击法

Sniffer 用来截获以太网或其他共享传输介质的网络上传输的信息，放置 Sniffer 后可使网络接口处于广播状态，对网络中传输的所有数据进行监视，从而截获网上传输的信息。黑客可以利用 Sniffer 截获口令、秘密的和专有的信息，用来攻击网络中的其他计算机信息系统。黑客使用 Sniffer 窃取秘密的好处在于，Sniffer 是被动的程序，本身在网络上不留下任何痕迹，使被攻击方无法发现自己被窃密。

7. 邮件炸弹攻击法

邮件炸弹是指不停地将无用信息传送给攻击方，填满对方的邮件信箱，使其无法接收有用信息。另外，邮件炸弹也可以导致邮件服务器的拒绝服务。常用的 E-mail 炸弹有：UpYours、Ka-Boom、Avalanche、Unabomber、Extreme Mail、Homicide、Bombtrack、FlameThrower 等。除了邮件炸弹外，诸如“PING 炸弹”这类的程序也可以用于攻击他人服务器，“PING 炸弹”是一种用来测试网络速度的小程序，这个程序会向服务器发送数据包，如果使用多个“PING”程序不间断地向服务器发送数据包，服务器也会因无法接受过多的请求而导致瘫痪。

8. 远交近攻法

互联网络连通着许多计算机信息系统，黑客先设法登录到安全性能较差的一个计算机信息系统上，并取得系统较高权限，然后以此为根据地访问其余主机，这种方法被称为“跳跃（Island hopping）”，在目前黑客攻击事件中被较多采用。黑客在到达目的主机之前往往会这样跳几次，例如，一个在美国的黑客在进入美联邦调查局的网络之前，可能先登录到亚洲的一台主机上，从那里登录到加拿大的一台主机，然后再跳到欧洲，最后从法国的一台主机向联邦调查局发起攻击，被攻击的网络即使有所察觉，也很难顺藤摸瓜地找到他。

9. 窃取 TCP 连接法

网络协议的设计初衷是方便信息的交流，而较少顾及安全问

题，这一特点可以被黑客利用来攻击网站。一般而言，用户在请求与服务器建立连接时，服务器用一个含有初始序列号的回答报文来确认用户请求，这个序列号没有特殊要求，只要是惟一的就可以了，客户端收到回答后，再对其确认一次，连接便建立了。TCP 协议规范要求每秒钟更换序列号 25 万次。但大多数 Unix 系统的实际更换频率远小于此，而且下一个更换的数字往往是预知的，正是这种可预知服务器初始序列号的能力，使得攻击得以实现。

此外，黑客的常用方法还有像驱动攻击法，虚假路径攻击法，系统管理员失误攻击法，重放攻击法，ICMP 报文的攻击法，地址模报文攻击法等。

四、黑客对电子商务发展的影响

由于发生了多次黑客破坏事件，在舆论的引导下人们一般对黑客作否定性评价，有的甚至谈“黑”色变，欲诛之而后快，而同情黑客或者自身就做过黑客的人则认为，黑客是一支新的社会力量，在一定程度上对社会具有积极作用。作者认为，任何事物都具有两重性，黑客的存在对电子商务发展具有积极的和消极的两方面作用。

（一）黑客对电子商务发展的积极影响

黑客技术是计算机科学的一种，其本身是中性的，和一切科学技术一样，它所起作用的好坏取决于使用它的人。白帽子黑客没有破坏和干扰他人计算机信息系统的目的和动机，主观上是出于技术探索的目的，甚至是希望帮助他人发现和堵塞系统缺陷和漏洞。虽然其行为侵犯了他人的权利，违反了国家法律，但是，在一定程度上对电子商务发展具有积极作用：（1）由于黑客的侵入，计算机系统和网络漏洞被发现，促使开发商修补产品的安全缺陷和在设计时更加注意安全问题，促使计算机信息系统管理员研究黑客技术，把系统和网络配置得更安全；（2）黑客攻击事件

引起了人们对黑客技术的关注，认识到黑客技术在检测系统和产品开发的安全性上的积极作用，促使世界各国政府和组织对黑客技术进行系统、深入地研究；(3) 黑客技术不仅可用于进攻，也可用于系统的防御；黑客不仅是系统的攻击者，也可以成为系统的防御者，如果黑客被引导利用得当，同样可以为电子商务发展保驾护航。培养、保持一支强有力的黑客保卫队伍，是抵御国外敌对势力攻击我国电子商务网站的有生力量。

(二) 黑客对电子商务发展的消极影响

1. 对用户个人的消极作用

随着社会信息化和电子商务的发展，黑客攻击影响人们日常生活的各方面，主要表现为：(1) 侵犯个人财产。如 2000 年 2 月重庆一名黑客秦某盗用他人“一卡通”账户密码，给被害人造成严重经济损失①。(2) 侵犯个人秘密。黑客攻击商业网站，往往造成存储在网站上的用户个人数据泄露。(3) 干扰用户的正常生活。黑客侵入并控制用户计算机的运作，使用户无法操作自己的计算机系统。

2. 对电子商务企业的消极作用

电子商务企业的计算机信息系统是黑客攻击的主要目标，黑客攻击给电子商务企业造成严重危害：(1) 黑客侵入给电子商务企业造成巨大的心理震撼，迫使企业频频更新安全措施，增大了电子商务企业的营运开支。有资料显示，有八成的美国企业内部的智能财产是以数字方式存储，而 1999 年投资在网络安全软件的金额高达 44 亿美元。调查机构 International Data 估计，此类支出在 2003 年将达到 83 亿元②。(2) 黑客攻击干扰电子商务企业的正常经营活动，有的降低服务质量甚至造成瘫痪，有的删改

① 张劲：《重庆抓获电子商务扒手》，《人民公安报》，2000 年 3 月 21 日。

② 刘洋《从黑客攻击事件谈网络安全》，http://www.chinaeb.com.cn/

系统中的经营数据，致使生产经营长时间无法恢复正常。(3) 黑客攻击往往给电子商务企业造成极为惨重的经济损失。根据旧金山的 Computer Security Institute (CSI) 和美国联邦调查局 Computer Intrusion Squad 的一份报告，美国 1999 年因为计算机受攻击引起的损失达 2.66 亿美元，是过去 3 年中年平均损失的两倍①。(4) 黑客攻击严重损害了电子商务企业安全经营的信誉，使企业在竞争中处于不利的地位，因此导致的间接损失要远大于直接损失。全球最大的网络安全公司安氏公司 ISS 占有全球网络安全市场一半的份额，其网络安全技术被全美 25 家最大商业银行中的 24 家认可。2000 年 6 月在黑客事先打电话预告的情况下，安氏公司的网站被黑客攻击，首页被删除。据称，这次黑客攻击事件是为了证实安氏公司的网络安全技术并不安全，显然给安氏公司信誉以沉重打击。

3. 对社会信息化的消极作用

电子商务是国家信息化建设重点，目前尚处于发展的关键时期，需要广大企业和用户的参与和支持。由于电子商务不安全，许多企业和用户对电子商务持观望态度，致使电子商务发展速度迟缓。

五、世界各国对黑客的态度

(一) 国际上对黑客犯罪的态度

黑客事件引起各国政府的高度关注，为维护国家信息安全，保障电子商务的顺利发展，惩治黑客犯罪，各国政府先后采取一系列对策。

1. 美国

美国是信息化基础设施最完善、电子商务发展最快的国家，也是遭受黑客危害最严重的国家之一，因此，美国在反黑客犯罪

① 《网上攻击造成巨大损失》，《计算机世界》，2000 年 4 月 5 日。

方面较早拥有较完备的法律和专门的司法机构。2000 年 2 月黑客攻击大型商业网站的事件进一步刺痛了美国政府，除了加强原有的国家基础设施保护中心、联邦调查局等反黑客犯罪的司法力量外，克林顿总统还提议，在 2001 年度财政预算草案中为加强网络安全和信息技术基础设施建设拨款 20 亿美元，并同时拨款 900 万美元启动其中的关键项目。

2. 德国

德国在保障网络安全方面起步较早。1996 年通过了《信息安全法》，对网上安全、个人自由和隐私权作了一系列规定，并成立了联邦信息技术安全局，配合内政部和刑警局进行技术执法。在技术上加强预防性和前瞻性研究，向企业和个人普及信息安全意识，推广安全技术标准等。黑客攻击美国大型商业网站的事件使德国更加关注网络安全，政府准备组织一支特别行动队，这支特别行动队由联邦内政部、联邦信息技术安全局和联邦刑事局成员组成，主要对付潜在的危害经济安全的黑客事件。

3. 日本

过去日本法律中有关黑客犯罪的立法比较少，对黑客非法侵入、偷看数据不作处罚，只对篡改数据影响业务的行为，依刑法第 234 条第 2 项追诉。近年来日本发生的黑客攻击事件越来越多，为了加大对黑客行为的打击力度，日本国会于 2000 年通过了《对付黑客等基础设施整备行动计划》，并于 2 月 13 日开始实施《电脑不正当入侵法》，对黑客非法侵入电脑的行为，可处以一年以下惩役或 50 万日元以下罚款。

4. 印度

印度是世界软件输出大国，对信息安全和反黑客犯罪特别重视。2000 年印度人民院通过了一项信息技术议案，强调在进一步发展信息产业的同时，也要加强网络安全管理。根据这项议案，印度将在警察部队中组建一支专门负责打击网络犯罪的特别行动部队，这支部队被赋予一定的特权，它可以在没有搜查证的

情况下，对网络犯罪嫌疑人的住宅及办公室的电脑进行突击检查。该议案还规定了对于网络犯罪行为的处罚条例，对那些侵入他人电脑系统的黑客，将视其所造成的危害程度量刑，最高可判处 3 年徒刑，并课以 20 万～1 000 万卢比（约合 4 600～23 万美元）的罚款。目前，印度已经步入世界上制定了有关打击电子犯罪法律的 12 个国家的行列。

其他国家在反黑客犯罪方面的行动也很快。如原来巴西刑法中尚无计算机、网络犯罪的规定，由于 2000 年初该国总统府、18 个政府部门和空军飞行指挥中心屡遭黑客袭击，激起了国家领导人的震怒，司法部长迪阿斯下令组建特别委员会，借鉴外国经验制定有关互联网犯罪的法律；韩国较早成立了国家警察局的黑客调查队（HIT），隶属国家警察局国际刑警组织，是同黑客犯罪作斗争的特殊部队，其检察部门还在 2000 年 3 月底成立了一个网络犯罪咨询委员会。同时，反黑客犯罪的国际合作也发展很快，2000 年 5 月西方 8 国部长就联合对付网络犯罪举行了网络刑事犯罪的会议。

在世界各国打击黑客犯罪的潮流中，也存在着逆流。有的国家为维护本国短期利益，对本国黑客进行包庇，不仅不处罚，反而给予某种荣耀，例如 1998 年 3 月，美国警方破获侵入美国国防部站点的黑客案件，发现是以色列青年黑客埃胡德·特南鲍姆所为。这个“分析家”被捕后，以色列总理内塔尼亚胡称赞他干得十分漂亮，“为以色列争足了脸”，以色列政府不仅不处罚这名黑客，反而忽略埃胡德·特南鲍姆患有轻微失语症的生理缺陷，让他参军专门从事信息战。

（二）我国对黑客应采取的对策

黑客，无论是黑帽子黑客、灰帽子黑客，还是白帽子黑客，其未经授权侵入他人计算机信息系统的行为，为社会秩序所否定，为国家法律所不容。因此，对黑客行径应当予以坚决反对，构成犯罪的还应依法追究刑事责任。

同时，我们应看到，黑客技术作为一种科学技术，有利于推进互联网安全和电子商务安全，黑客群体作为一类智慧群体，是信息社会的智力资源，如果他们被引导管理得当，可以造福于社会。另外，在黑客群体中，十几岁到三十几岁的青年人占有很大比例，如果对这些人不加区分，以一个尺度进行打击，不利于国家人力资源的有效运用，不利于社会信息化和电子商务的发展。因此，对待黑客团体必须“有导有堵”，区别对待。作者认为，我国对黑客应该采取以下对策：

第一，要给黑客用武之地，将他们的聪明才智引入正轨。黑客都有强烈的表现欲，用适当的方式给他们提供表现的机会，有利于黑客们正确认识自己，并获得心理上的满足。例如 1999 年在新加坡举办的一次信息技术（IT）贸易展览会上，里德展览公司与一家计算机系统公司共同举办信息技术安全贸易展厅，设置黑客攻击区域并提供资金，希望黑客们现场展示他们的攻击技巧，并把这项活动作为展览会的内容之一。建议政府和电子商务企业设立类似“靶子”网站，既为不存恶意的黑客提供一显身手的场所，避免黑客攻击营运中网站，还可从黑客攻击“靶子”网站中发现营运网站的漏洞，及时予以弥补。

在青少年黑客中，确有一些难得的电脑网络天才，一旦将他们的聪明才智引入正轨，加以充分发挥，对电脑网络技术的发展，将发挥极大的推动作用。以色列对青年计算机人才给予高度重视，年轻人在计算机网络领域创造辉煌的报道屡屡见报。比如，有 3 名 25 岁的计算机天才曾创建了一家名为米拉比尔斯（Mirabilis）的网上“聊天”公司，出售给实力强大的美国联机公司获得 2.87 亿美元的收入；4 名以色列青年创建一个专门从事互联网安全业务的公司，目前在华尔街的身价已超过 10 亿美元。这些成功的范例，大大激发了以色列青年的创业热情，也使不少网络黑客的心往正道上想，劲往正道上使。

第二，对黑客实行“思想教育在前，法律制裁在后”的方

针。黑客的出现既然是一个全球性的问题，对黑客的防治就应引起全社会的重视。必须看到，计算机网络与黑客犯罪没有必然的联系，一些图谋不轨的黑客，并不因为有了计算机网络才危害社会，而一般是因为事先就有了不健康的思想基础，只不过是计算机网络成为他们施展“抱负”的场所罢了。所以，要防止黑客对社会的危害，必须从黑客产生的根源入手，尽可能动摇黑客产生的思想基础和社会基础，通过各种行之有效的措施，提高全社会的道德水准。我们应在建设我国信息高速公路和完善计算机安全立法的同时，在全社会进行计算机网络道德教育和信息网络安全法制教育，提高公民道德水平。

第三，加大对黑客犯罪的打击力度，坚决取缔黑客犯罪组织。黑客犯罪主要是黑帽子黑客和灰帽子黑客所为，因此必须严厉惩治犯罪的黑客。目前黑客犯罪组织化趋势越来越明显，黑客组织的破坏能力远大于单个黑客攻击能力的简单相加，具有极大的社会危害性，因此，对黑客犯罪组织必须坚决取缔，对黑客组织犯罪应从重惩治，否则，不足以威慑以身试法的犯罪分子。此外，对已犯罪的黑客应该实行区别对待的刑罚政策，严格贯彻惩办与宽大相结合的刑事政策。对那些年满 16 周岁未满 18 周岁的未成年黑客犯罪人，避免适用自由刑，多适用非刑罚处理措施；对于必须判处徒刑的，坚持从轻或减轻处罚，放宽缓刑的适用。

第二节　有害计算机程序问题

一、有害计算机程序的概念与分类

（一）有害计算机程序的概念

何为计算机程序？我国《计算机软件保护条例》第 3 条规定：计算机程序是指“为了得到某种结果而可以由计算机等具有信息处理能力的装置执行的代码化指令序列，或者可被自动转换

成代码化指令序列的符号化指令序列或者符号化语句序列。计算机程序包括源程序和目标程序。同一程序的源文本和目标文本应当视为同一作品”。从该规定可以看出，计算机程序具有以下特性：(1) 目的性。计算机程序是编程人员为实现一定目标，或者得到一定结果而编制的，是编程人员目的、意图的反映和实现目标的工具。(2) 可执行性。计算机程序是可以被执行的代码化指令序列、可被自动转换成代码化指令序列的符号化指令序列或者符号化语句序列，它必须按照一定的计算机指令语法编制，并且可能被信息处理设备执行。不具有可执行性的指令序列或者语句序列不是计算机程序。(3) 特定的执行体。计算机程序的执行体是具有信息处理能力的装置，既包括计算机，还包括如具有邮件收发能力的移动电话、商务通，数据筛选转发能力的网络通信设备设施等，计算机系统是计算机程序的主要执行体。

如何理解有害计算机程序的有害性。一种看法认为，有害性表现为对执行计算机程序的信息处理装置的硬件、软件和数据的破坏作用，如 CIH 病毒能够损坏主板，删除硬盘中的全部数据。另一种看法认为，有害性应该是对信息处理设备安全性的破坏，既包括对信息处理装置硬件、软件和数据的损坏，也包括对存储信息的完整性和保密性的侵害，如 Melisa 病毒可能导致计算机信息系统中的秘密数据的泄露。作者同意后一种观点，有害性应该包括对信息处理装置的完整性、可用性和保密性的危害，即对装置安全性的危害。有害计算机程序（以下称有害程序）是指危害计算机等信息处理装置安全性的计算机程序。

这里要对黑客程序作一说明。黑客程序以 Back Orifice（简称 BO）为代表，BO 是一个基于 Windows 的远端控制软件，类似的还有 Netspy（网络间谍）、Xspy 等等，它们的工作原理基本相同。首先，犯罪人把服务器程序秘密植入被攻击方的计算机系统中，当用户运行了 Boserve.exe 之后，Win95 的注册表会被 BO 修改，并把自己复制到 System 目录下面，再把原来的

Boserve.exe 文件删除掉，以后每次启动 Win95 时，它都会根据注册表自动加载 System 目录下面的 Boserve.exe 服务程序。此时表面上来看 Win95 没有任何的变化，实际上 Boserve.exe 服务程序正在悄悄地运行，接受从网络客户端传来的控制命令。从危害计算机信息系统安全的角度来看，黑客程序无疑是有害程序，但是，它所扮演的角色是在被害人计算机信息系统内部，“策应”犯罪人的黑客攻击行为，属于黑客工具，因此，把它放在黑客问题讨论更合理。本节所称有害程序不包括黑客程序。

（二）有害计算机程序的分类

1. 根据有害程序对信息处理系统安全危害的大小，可分为恶性有害程序和干扰性有害程序

所谓恶性有害程序，是指严重危害信息处理系统安全的有害程序，如 CIH 病毒。1999 年 4 月 26 日，全球爆发 CIH 病毒灾难，造成俄国十多万台计算机瘫痪，涉及一百二十多家公司和机构；在韩国被感染的计算机涉及总统府、国防部、汉城市政府等多个部门，估计被感染的电脑数量达到数十万台，造成的直接、间接损失高达数千亿韩元；我国受到损害的计算机总量估计为 36 万台，造成的直接、间接经济损失超过十亿元。CIH 病毒可以毁坏电脑主板，删除硬盘所有数据，是已知电脑病毒中危害最大的一种①。

所谓干扰性有害程序，是指对信息处理系统危害不大，只是在一定程度上干扰系统正常运作的有害程序。如 IBM 圣诞树病毒，它可令计算机系统在圣诞节时显示问候的话语，并在屏幕上出现圣诞树的画面，而不对计算机信息系统有其他负面影响。

2. 根据有害程序的特征，可分为计算机病毒和其他有害程序

① 周文林：《电脑病毒肆虐全球，预防为主乃为上策》，《电脑日报》，1999 年 5 月 6 日。

所谓计算机病毒，依照我国《计算机信息系统安全保护条例》第 28 条规定，是指“编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码”。计算机病毒是有害程序中比较特别的一种，有其独特的行为方式，对信息处理系统安全有严重威胁。其他有害程序是指不具有计算机病毒特征的有害程序，这类有害程序可分为若干种类，如特洛伊木马、逻辑炸弹、意大利香肠等。

二、计算机病毒

（一）计算机病毒的起源

计算机病毒的起源，可追溯到 1949 年，当时计算机的先驱者冯·诺依曼发表了一篇题为《复杂自动机的理论与结构》的文章，在该文中提出计算机程序自我复制的假说。十年后美国电报电话公司贝尔实验室的研究人员编制的电子游戏《内核战争》为冯·诺依曼假说注入了活力，在游戏中两个程序员释放出一组叫做“生物体”的程序，让它们相互争夺计算机的控制权。20 世纪 70 年代，有两部科幻小说《震荡波骑士》和《P－1 春天》对自我复制程序的运作进行了预示性描述：一组程序能够不为人所觉察地把自身从一台计算机传输到另一台计算机。1983 年著名的美国计算机安全专家 Fred.Cohen 在实验中证实了计算机病毒实现的可能性。1984 年 Fred.Cohen 公布了他对计算机病毒的研究成果，让全世界的学者知道了计算机病毒这一概念。1986 年他在博士论文中第一次为计算机病毒作出了严格的数学定义。计算机病毒从此正式面世，成为人类社会挥之不去的阴影，而且随着计算机的广泛应用而愈演愈烈。

（二）计算机病毒的含义

什么是计算机病毒？国内外有多种看法：

1. 计算机病毒之父 Fred.Cohen 于 1984 年把计算机病毒定

义为，“计算机病毒是一种计算机程序，它通过修改其他程序把自身或其演化体插入它们之中，从而感染它们”①，并于 1988 年著文强调，“计算机病毒不是利用操作系统的错误或缺陷的程序，它是正常的用户程序”②。

2. 美国国家计算机安全中心在《计算机安全术语汇编》一书中，给计算机病毒的定义是：“计算机病毒是一种自我繁殖的特洛伊木马，它由任务部分、触发部分和自我繁殖部分组成。

3. 日本通产省在《计算机病毒对策基准》中的定义是：病毒是为了对第三者的程序和数据库施加某种危害而制作的程序，它至少含有下述一种功能：a. 感染功能；b. 潜伏功能；c. 发病功能。

4. 我国计算机安全监察司给计算机病毒所下的定义是：计算机病毒是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。

上述定义都从不同角度上反映了计算机病毒的特征，但是，由于计算机病毒技术发展非常迅速，有些定义已经不能适应计算机病毒发展现状，如第一种定义和第四种定义都认为计算机病毒只能是“编制或者在计算机程序中插入”的计算机指令或者程序代码，而目前引导型病毒不需要感染正常的计算机程序，它在系统引导时进入系统，获得系统控制权，在完成自身的安装后才去引导系统，米开朗琪罗病毒是这类病毒的典型。第四种定义把计算机病毒对信息系统的作用限定为“破坏计算机功能或者毁坏数据，影响计算机使用”，而“梅利莎”病毒和“爱虫”病毒都不

① Fred.Cohen，“Computer Viruses－Theory and Experiments”，IFIP TC-11 Conference，Toronto，1984.

② Fred.Cohen，“On the Implication of Computer Viruses and Methods of Defense”，Computer &Security Vol. 7，1998.

会破坏计算机功能或者毁坏数据，它的危害作用在于其泄露他人个人数据，造成网络上的电子邮件数量大量增加，导致邮件服务器不堪重负而瘫痪，因此，第四种定义不能囊括这两种新的病毒。作者认为，计算机病毒技术是计算机技术的一种，近年来发展极为迅速，并向多样化、复杂化等方面发展，如果给计算机病毒作过于狭窄的定义，势必影响正确认定计算机病毒，进而影响对相关违法犯罪的正确认定。计算机病毒的定义应当是具有主动传染性的、危害计算机系统安全的计算机程序。

（三）计算机病毒的分类

计算机病毒种类繁多，可以根据不同的标准分类。根据其活动方式可分为 4 类：(1) 文件型病毒。这类病毒能将其代码附加在系统引导程序上，当系统引导时病毒程序被带入，其代表为黑色星期五病毒、维也纳病毒等。(2) 引导型病毒。这类病毒在系统引导时进入系统中，获得系统控制权，在完成自身的安装后才去引导系统，其代表为米开朗琪罗病毒、2708 病毒等。有些病毒同时具有引导型病毒和文件型病毒的特征，它感染硬盘的主引导扇区和所有在系统中的执行文件，如 2153 病毒。(3) 宏病毒。字处理软件 Word 是当前最流行的文字编辑软件，它功能很强，跨越多种系统平台，可向用户提供宏功能，使用宏功能可将一系列 Word 指令组织到一起，成为一条独立使用的指令，从而进行连续操作。宏病毒正是针对 Word 编写的一种病毒，它寄生在 Word 文档中，利用 Word 文档功能传染另外一个 Word 文件，其危害作用根据编写者的意图各不相同，其代表是 WM/ConceptA。其他的分类方法还有，根据攻击对象，可分为攻击 IBM－PC 及其兼容机的病毒、攻击 Apple 公司生产的 Macintosh 系列的计算机的病毒和攻击 Unix 系统的计算机病毒；根据连接方式，可分为源码病毒、入侵型病毒、操作系统病毒和计算机外壳型病毒；根据计算机病毒可能造成危害作用的大小，可分为恶性病毒和干扰性病毒。

（四）计算机病毒的特性

1. 主动传染性

主动传染性是衡量一种程序是否病毒的首要条件，是病毒的再生机制。病毒进入计算机系统后主动与其中的合法程序连接，在运行被传染的程序时继续传染其他的程序。

2. 潜伏性和可触发性

病毒传染计算机后，往往不立即攻击，而是有一段潜伏期，短则几周，长则几年。潜伏期内病毒秘密传染其他计算机程序或计算机系统。潜伏性和传染性相辅相成，病毒潜伏得越好，其传染范围就越广泛。病毒程序一般有触发条件，包括传染条件和攻击条件。潜伏性与触发性紧密联系，如果病毒潜伏得不好，不到病毒潜伏期结束，病毒程序就被发现和清除。

3. 危害性

当攻击触发条件满足时，病毒对计算机系统进行主动攻击，或者破坏系统功能，或者破坏系统中的数据或应用程序，或者窃取、泄露秘密数据资料，或者制造恶作剧戏弄使用者等等。其破坏作用的大小取决于病毒程序设计者的初衷和目的。

近年来，计算机病毒技术在与反病毒技术的对抗中，技术越来越先进、越来越复杂，新产生的病毒除了具有传统病毒普遍具有的三个主要特征外，还增添了许多新特点，如病毒的网络化、多形化、密码化、智能化、军用化和病毒生产的自动化等，这些新特点使它们能够更好地隐蔽自己，对抗反病毒工具的检测，使人防不胜防。

（五）计算机病毒的侵入途径和方式

虽然计算机病毒的传染方式存在较大差别，但是它们都必须借助于一定的媒介传播，早期的计算机病毒传染的介质主要是硬盘和软盘，而后，随着计算机网络技术、光盘存储技术及其应用的发展，光盘和互联网逐渐成为主要传染介质。目前计算机病毒借以传染的介质主要有三种：网络、光盘和磁盘，即计算机病毒

通过网络通信从一个计算机信息系统转移到其他计算机信息系统中，然后利用其自身的传染机制传染给受害的计算机信息系统，前面提到的“梅利莎”病毒和“爱虫”病毒就是其中的典型；光盘和磁盘是计算机数据的常用载体，当携带计算机病毒的光盘和磁盘在不同计算机系统上使用时，计算机病毒就秘密传播出去。

计算机病毒侵入的方式主要有以下三种：(1) 以引导区被感染的磁盘光盘为媒介。例如 1990 年美国阿托丁格公司出售的 FAR SIDE MOON 游戏软件磁盘被病毒感染，其中一片磁盘的引导区被计算机病毒侵入，这些受计算机病毒传染的磁盘售出后，进一步传染给其他用户。(2) 以电子邮件为媒介。目前电子邮件服务在互联网络中应用最为广泛，其功能也越来越强，它的附件功能使得在电子邮件中可以附带其他文件，计算机病毒往往藏身于这个附件中，一旦用户打开附件，计算机病毒就秘密侵入计算机信息系统。(3) 利用系统安全漏洞。目前广泛应用的互联网、计算机信息系统的安全体系都存在一定的缺陷，技术高超的编程人员能够利用这些漏洞编写网络病毒程序，通过网络侵入计算机信息系统。

三、其他有害计算机程序

主动传染功能是计算机病毒与其他有害计算机程序的分水岭，其他有害计算机程序是指不具有主动传染功能的有害计算机程序，但它们的其他功能可以与计算机病毒完全相同，这些有害计算机程序一般隐藏在看似正常的计算机程序中，一旦被执行，就在计算机信息系统中潜伏下来，待机危害系统安全。这类有害计算机程序有多种，常见的有以下两种：

(一) 特洛伊木马程序

典型的特洛伊木马程序有 AIDS，1989 年 12 月美国人类学博士鲍伯编制了 AIDS 特洛伊木马程序，并把它免费寄给世界各地用户，用户运行了 AIDS 后，系统被有害程序侵入。

（二）“逻辑炸弹”程序

“逻辑炸弹”程序（简称逻辑炸弹）是指被编制或者安插在其他计算机程序中的有害计算机程序，当系统满足一定条件，如特殊时间的到来、特殊事件的出现，就触发逻辑炸弹危害系统安全。例如吕科制造“逻辑炸弹”案，软件程序员吕科向公司索要20万元高额奖励被拒绝后，秘密在公司出产的电脑程序中安置了“逻辑炸弹”进行报复，由于这枚逻辑炸弹作梗，该公司的“网络快速发布系统”产品只要当时间大于2000年3月1日时，系统就会处于瘫痪状态①。

四、有害计算机程序危害事件的发展态势与特点

（一）有害计算机程序危害事件的发展态势

1987年5月，全球有据可查的第一桩计算机病毒危害案在美国《普罗威斯顿日报》编辑部发生之后，有害计算机程序危害事件迅速增加，社会危害性日益严重，有害计算机程序成为威胁信息社会和电子商务发展的“达摩克利斯剑”。

第一，有害计算机程序危害范围越来越广。有害计算机程序也是计算机程序，它可以像其他计算机程序一样，在计算机信息系统上运行。因此，凡是使用计算机的地方，就有遭受有害计算机程序危害的可能，计算机应用程度越高，应用范围越广泛，有害计算机程序扩散越广，危害越大。目前，全世界已经发现的计算机病毒及其他有害计算机程序超过两万种，而且几乎以每月一百多种的速度增加，其中包括了各种类型、各种危害程度的有害程序。如此之多的有害计算机程序无疑对信息系统安全构成严重威胁，据美国国家计算机安全协会的一项调查，几乎100%的美国大公司的内部网络或台式机经历过有害计算机程序的危害。

---

① 《北大毕业生为索20万元，造“逻辑炸弹”被抓》，《南方都市报》，2000年4月12日。

第二，有害计算机程序危害越来越大。20 世纪 90 年代国际互联网的迅速发展为有害计算机程序提供了一条更快捷、更方便的传播途径，其影响的范围更加广泛，造成的危害更加严重，如 CIH 病毒、爱虫病毒事件。

有害计算机程序技术是计算机技术领域的一个分支，在与有害计算机程序防御技术的对抗中，始终处于主动、进攻的态势，难以被彻底清除。因此，计算机应用和电子商务的发展过程中，有害计算机程序危害事件将长期存在，并且，严重危害事件还可能多次发生。

（二）有害计算机程序危害事件的特点

1. 行为人结构特征

在有害计算机程序危害事件中，直接危害信息处理系统安全的是有害计算机程序，然而，它们只是为一定目的而编制出来的计算机程序，实施危害行为的是施放这些有害程序的人，就如枪炮杀人而杀人者是人一样。根据不同的标准，可对有害计算机程序危害事件的行为人进行不同分类。

第一，根据行为人能否编写有害计算机程序，可分为编写（或改写）并施放有害程序的行为人和仅实行施放有害程序的行为人

前者一般受教育程度较高，熟悉有害计算机程序的工作原理，能够熟练编写有害计算机程序，或者能够分析他人编写的有害计算机程序并予以改写，属智能型行为人。在这些人中，有相当一部分是青年学生。如名噪一时的蠕虫病毒是美国康奈尔大学计算机科学专业的研究生 Robert Morris 的实验作品，不过，蠕虫危害作用如此之强也出乎其意料，以致蠕虫病毒发作后他也无法遏制其在网上蔓延。有害计算机程序技术发展很快，互联网上存在许多计算机病毒资料的网站如“中国毒岛”，这些网站提供了大量有关有害计算机程序的编写方法甚至源码资料，编写或者改写有害计算机程序无需丰富的编程经验和精湛的编程技能，只

要具有一般的计算机操作技能和计算机语言知识，按照他人提供的方法，就可以制作出具有相当危害作用的有害计算机程序。另外，有害计算机程序技术的发展也使有害程序的制作更加简单，目前有一种被称为病毒生产自动机的程序如 Crazy Lord Mutation Engine（CLME），使用者只需运行这个程序就可以生产计算机病毒。病毒自动生产机技术的出现，使他人更容易得到有害计算机程序，进而向网络或者他人的计算机信息系统施放有害计算机程序。

仅施放有害计算机程序不需要高深的计算机技术，只要能够获得有害计算机程序，具有一般计算机使用知识的人都可以顺利施放。这类行为人既可能是计算机初学者，也可能是计算机高手。

第二，根据制造有害程序危害事件的是否为单个自然人，可分为单个行为人、组织和单位

有组织地制作、施放病毒的有维也纳病毒事件。维也纳病毒是一种恶性病毒，它侵入计算机信息系统后，修改指定路径上后缀为 .com 文件的头 5 个字节，使该文件报废。维也纳病毒的作者是德国汉堡市的一个计算机俱乐部的三名成员，他们在见到病毒的报道后出于好奇编写了这个病毒。

单位施放有害计算机程序的案件在软件产业多次发生。计算机软件盗版现象令软件生产商非常恼火，一部分软件制造商为打击盗版维护自己的权利，在自己的软件产品中施放有害计算机程序，如 1985 年巴基斯坦一家计算机软件公司为保护自己的软件不被盗版，编制了“巴基斯坦智囊”病毒，并将它加入公司的所有软件中，一旦用户非法使用这些软件，该病毒就会发作，破坏计算机中的数据文件①。

---

① 黄学彬：《接近零点——全球反计算机犯罪透视》，四川人民出版社 1997 年版，第 66～67 页。

2. 行为人的目的和动机

(1) 出于好奇的动机。如汕尾视聆通病毒案。汕尾市庄某一次上网时无意中发现了一个破坏性程序，在好奇心驱使下，他将该程序放置在广东视聆通汕尾站的留言板上，致使每个上网浏览该留言板的用户的计算机马上“死机”①。

(2) 出于恶作剧的动机。如 1987 年 12 月圣诞节前，IBM 公司的国际电子信息网中忽然出现了大量的“圣诞贺卡”，在网络上胡乱传递，并且越来越多，最终使整个计算机网络不堪重负而瘫痪，这就是“圣诞树”病毒的杰作②。

(3) 出于泄愤报复的动机。如张文明设置破坏性程序案。1998 年 12 月 27 日，北京顺义某中学发现该校从北京无忧电脑软件开发公司购得的一张软盘“全国计算机等级考试”有“逻辑炸弹”，只要运行该学习软件，破坏程序便会删除硬盘、破坏分区。警方抓获了犯罪嫌疑人张文明，据张交代，1998 年他在北京无忧公司任程序员期间，因经常迟到受到领导批评，由此怀恨在心，便利用职务之便在该公司开发的计算机等级考试 DOS 学习软件中植入破坏性程序③。

(4) 出于保护软件知识产权的目的。利用有害计算机程序危害信息处理系统安全的功能，威慑非法盗版用户，保护自己软件的知识产权，是一些从事计算机信息产业的制作商不得已的行为，除了前文提到的“巴基斯坦智囊”病毒事件外，我国也发生了类似的案件，如江民公司在杀毒软件中设置“逻辑炸弹”案。

---

① 《网上设置死机程序，广东“网虫”被罚五千元》，《电脑日报》，1999 年 4 月 14 日。

② 黄学彬：《接近零点——全球反计算机犯罪透视》，四川人民出版社 1997 年版，第 67 页。

③ 刘晓玲：《北京破获首例电脑“投毒”案》，《检察日报》，1999 年 2 月 24 日。

3. 客观方面的特征

(1) 危害范围广泛、破坏力大

有害计算机程序有特殊的传染机制，在互联网环境下能够在较短的时间内传染范围极为广泛的计算机系统。同时，各种有害计算机程序危害作用各不相同，有的能够造成硬件设备设施的损坏，有的能够毁坏硬盘中的数据，这种恶性有害程序一旦发作，可能危害数量巨大的计算机信息系统，造成巨大经济损失，CIH 病毒、Melissa 病毒和“爱虫”病毒事件就是佐证。

(2) 隐蔽性更强

在网络空间里，用户的真实身份和网络身份可以不一致，因此，凭借行为人在网络上留下的痕迹追踪施放有害程序的行为人非常困难。此外，由于有害计算机程序具有潜伏特性，潜伏期为行为人销毁证据、逃匿提供了机会。

(3) 造成的损失难以统计

被有害程序侵害的计算机系统分散，当损害发生时，危害后果不易被准确计算，其实际危害后果往往比统计结果严重得多。另外，由于有害计算机程序的交叉感染和变种，有害程序的危害作用可能与初始设计时不同，这也给正确计算犯罪造成的损失增加了难度。例如，CIH 病毒有 v1.2、v1.3、v1.4 等几个版本，破坏力一个比一个大，2000 年出现的“爱虫”病毒在短时间内就有 29 种变种，要准确统计某种版本的病毒所造成的危害，几乎是一件不可能实现的事。

4. 被害人特征

从理论上讲，所有计算机信息系统都可能成为有害计算机程序危害的对象，但计算机信息系统安全管理不同，遭受危害的可能性也不同。较容易遭到侵害的被害人有两类：一类是缺乏计算机信息系统安全保护措施的单位和个人。目前计算机应用越来越广泛，计算机数据交换越来越频繁，将有害计算机程序完全排除于计算机信息系统之外是不可能的，因此，必须常备检查清除有

害计算机程序的工具，如杀毒软件、病毒防火墙等。忽视计算机信息系统的安全防护，将使自己遭受有害程序的侵害。另一类是缺乏完善的计算机信息系统内部安全管理的单位或者个人。坚固的防线防不住来自内部的攻击，内部人员安插施放有害计算机程序更加隐蔽，如果缺乏完善的安全管理，再强大的安全防护技术都无济于事。

五、电子商务安全和有害计算机程序

有害计算机程序对电子商务发展的作用，有人认为，有害计算机程序危害事件为生产杀毒软件、病毒防火墙产品的公司提供了市场机会，提高了人们的安全意识，对电子商务的发展具有一定的积极作用。作者认为，有害计算机程序对电子商务发展主要起阻碍作用，这是因为：首先，有害计算机程序技术始终处于积极攻击的优势位置，杀毒软件、病毒防火墙等产品不能有效地保障计算机信息系统安全，它们不可能成为灾难来临之前的有效屏障，而只能防范同样灾难重演。有害计算机程序危害事件创造的市场机会是有害计算机程序危害后果的反映，人们的警惕意识是由有害计算机程序危害所致。其次，有害计算机程序一经施放出去，其影响范围大到行为人本身都无法估计的程度，所造成的危害后果也远远超过行为人的想象，更难以控制局面。1999 年“梅利莎”病毒传播后的 16 小时内，有超过 6 万台计算机信息系统遭到侵害，而制作者戴维·史密斯编写该病毒的目的，不是要窃取他人隐私资料和危害互联网安全，而是希望为一些色情网站进行宣传①。再次，有害计算机程序危害作用越来越严重，对电子商务安全构成极大的威胁。有些电子商务数据一经毁坏或丢失，给电子商务企业造成的损失不是能够以金钱可以弥补的；有

① 陈凤丽：《色情网站造毒，电脑罪犯被捕——“梅利莎”来得凶，完得快》，《环球日报》，1999 年 4 月 9 日。

害计算机程序还给广大电子商务用户造成不安全感，担心个人隐私数据被泄露，担心自己的电子资金记录被删除，从而形成对电子商务的不信任。电子商务没有广大用户的参与和支持，将使一国电子商务发展迟缓。鉴于有害计算机程序对电子商务的严重危害，对于利用有害计算机程序实施违法犯罪的，应当依法予以严厉打击。

第四章 英美德日等国及我国电子商务领域刑事立法状况

第一节 英美德日等国电子商务领域刑事立法状况

一、概述

随着电子商务的发展，电子商务领域犯罪日益猖獗，为维护本国电子商务的正常秩序，许多国家制定了打击这类犯罪的刑事法律。由于各国电子商务和电子商务领域犯罪的发展状况不同，政治文化、法律制度传统各异，世界各国惩治电子商务领域犯罪的刑事立法完善程度有较大差别。在立法模式上，一些国家采取制定单行法律的立法模式，如美英等国；另一些国家则采取修改刑法，增补相关法律规定的模式，如德、日和法国等。目前，电子商务发展比较顺利且电子商务领域犯罪刑事立法比较完善的国家，主要是一些发达资本主义国家，研究分析这些国家在该方面的刑事立法体系，借鉴其成功的立法经验，有助于我国电子商务领域刑事立法的完善。

分析这些国家的电子商务领域刑事立法，可以发现它们具有以下特点：

（一）从法律条文制定的时间来看，电子商务领域犯罪的刑

事立法体系由传统法律条文、修改的法律条文和新制定的法律条文三部分组成

电子商务领域犯罪虽然是在电子商务发展中出现的犯罪形式，但是，其中有相当一部分犯罪仍然可以适用传统法律条文，如侵入他人电子商务信息系统窃取商业秘密的，仍然适用侵犯商业秘密罪的规定，因此，传统法律规定是电子商务领域犯罪刑事立法体系的重要组成部分。一些国家之所以迟迟没有修改法律条文，或者只是增补法律法规，其原因除了本国电子商务发展还没有面临严重的犯罪问题以及对电子商务领域犯罪的研究尚未成熟之外，一个重要原因是传统法律还可以处理这类犯罪问题。有的电子商务领域犯罪在适用法律时，虽然没有明确的法律依据，但无需对法律条文进行大的增补改动，只需要对所涉及的传统法律中的有关法律概念进行扩展延伸。如英国 1981 年的《伪造文书及货币法》规定，“意图使人相信系真正者并实施对其本人或第三人不利益之作为或不作为，而制作虚伪文书者”为伪造文书罪，该法除了基于复制设备的发达而将复制影印本纳入伪造文书罪中外，还基于计算机设备运用日益普及的考虑，将“以机械、电子或其他方法记录或记忆之磁碟、磁带、音带或其他设备”纳入文书的范畴，并规定“以对于机器行使下述文书为目的，而由机器予以识别、操作或不操作时者”，视作行为人所为①。但是，有些新形式犯罪，如制作施放有害计算机程序危害电子商务信息系统安全，适用传统法律条文和修改扩展后的法律条文都不恰当，必须针对这类新形式犯罪制定新的法律法规。同时，专门针对电子商务领域犯罪制定的法律法规要比适用一般的刑法条文更加有效，正如德国犯罪学家施奈德所说，“专门针对计算机犯罪的刑法条款比之把计算机犯罪归属于一般的刑法条款（诈骗、盗

① 刘广三：《计算机犯罪论》，中国人民大学出版社 1999 年版，第 154 页。

窃、侵吞、贪污等）具有更大的威慑作用，而且也能够为形成一种计算机职业内部的职业道德打下基础”①。这些新的法律条文、法律法规在各国电子商务刑事立法体系中所占比例各不相同，却是各国刑事立法适应电子商务发展的重要标志。

（二）从法律条文规范的内容来看，电子商务领域刑事立法由保护电子商务信息系统安全的法律条文和保护电子商务交易秩序的法律条文两部分组成

保护电子商务交易秩序的刑事立法是电子商务领域刑事立法的重要组成部分。在这方面，大多数国家都制定了相关法律，并且这些法律正随电子商务的发展不断扩充，将在电子商务刑事立法体系中占有较大比例。

电子商务是建立在信息技术物质基础上的经济活动，电子商务信息系统安全直接关系到电子商务的顺利发展，因此，打击危害电子商务信息系统安全的犯罪行为，维护电子商务信息系统安全是电子商务刑事立法的重要内容。这部分刑事立法主要规范未经授权侵入他人计算机信息系统、扰乱计算机信息系统正常工作、破坏计算机信息系统的功能、数据和应用程序等犯罪行为。

二、美国电子商务领域刑事立法状况

美国是世界上计算机网络技术最发达、电子商务发展最早最具规模的国家，也是遭受电子商务领域犯罪危害最早最严重的国家，因此，美国电子商务领域的刑事立法较早且比较完善。美国政府从 1965 年起就着手立法保护计算机信息系统安全，1970 年颁布了《金融秘密权利法》，其中规定了限制一般个人和法人了解银行、保险业以及其他金融业的计算机中所存储的数据，禁止在一定时间内把有关用户的“消极信息”向第三者转让。1973

① ［德］汉斯·约阿希姆·旋奈德著：《犯罪学》，中国人民公安大学出版社 1990 年版，第 72 页。

年美国召开了首届计算机安全与犯罪会议，1977 年美国参议员亚伯拉罕·利比柯夫向国会提出了“联邦计算机系统保护法案”，该法案虽未通过，却引起了美国政府对计算机安全与犯罪的关注。美国联邦关于计算机安全与犯罪的第一部法案是 1984 年通过的《欺骗存储装置与计算机欺诈、滥用法》，该法案在 1996 年 10 月 11 日修订后，改为美国联邦刑法第 18 篇第 1030 条，名为“与计算机相关的欺诈及其他行为”。1984 年还通过了《中小企业计算机安全教育培训法》，1986 年通过了《计算机欺骗与滥用法》，对计算机使用作了严格限制，1987 年通过了《联邦计算机安全处罚条例》，1989 年通过了《计算机病毒根除法》，1994 年颁布了《计算机滥用法修正案》，1996 年《国家信息基础设施保护法》经克林顿总统签署通过，但是其中的《正当通信法案》遭到民权组织强烈反对而被废止。

美国是一个联邦制国家，联邦法律和州法律并存是美国法律体系的特点，所以在电子商务领域刑事立法上，不仅有联邦刑法法规，还有各州的刑法法规。1978 年佛罗里达州制定了美国第一个有关计算机安全与犯罪的法律——《与计算机相关犯罪法》，随后，各州相继颁布了计算机犯罪法，到目前为止，已有 47 个州制定了关于计算机安全与犯罪的法律，如亚利桑那州的《有组织犯罪及欺诈法》、明尼苏达州的《阻碍商业犯罪法》、康涅狄格州的《与计算机相关的犯罪法》、弗吉尼亚州的《弗吉尼亚州计算机犯罪法》，等等。这些州关于计算机安全与犯罪的法律大致包括以下内容：（1）禁止非授权进入计算机系统窥探他人信息。计算机信息系统中保存了大量个人数据或者商业秘密数据，为了保护公民个人隐私和商业秘密，多数州立法将非授权进入他人计算机信息系统，窥探信息而尚未造成数据、程序修改和删除，或者系统功能损害的行为规定为犯罪，如密苏里州、西弗吉尼亚州、肯塔基州等。（2）禁止危害计算机信息系统正常工作的行为。大约 1/4 的州法律规定，任何损坏计算机设备、网络设备、

应用程序、计算机数据文件，阻碍计算机信息系统正常工作的行为违法，如怀俄明州、路易斯安那州等。(3) 禁止施放破坏性计算机程序，危害计算机信息系统安全的行为，如加利福尼亚州、明尼苏达州等。(4) 禁止利用计算机实施贪污或者欺诈行为。许多州立法把用计算机手段非法获取财产或者服务的行为规定为犯罪，如弗吉尼亚州、亚利桑那州等。

目前美国联邦刑法中，有关电子商务领域犯罪的刑事立法主要有以下几部法律①：《与计算机相关的欺诈及其他行为法》、《与存取设备有关的欺诈及其他行为法》（《18 U.S.C.1029. Fraud and Related Activity in Connection with Access Devices》）、《通信线路、站台或系统法》（《18 U.S.C.1362. Communication Lines, Station, or System》）、《禁止窃听、披露有线通信线路、无线通信或者电子通信信息法》（《18 U.S.C.2511. Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited》）、《非法进入信息存储的通信系统法》（《18 U.S.C.2701. Unlawful Access to Stored Communications》）、《信息披露法》（《18 U.S.C.2702. Disclosure of Contents》）、《与联邦政府相关的存取要求法》（《18 U.S.C.2703. Requirements for Governmental Access》），这些法律、法规将以下行为规定为犯罪。

(一) 保护计算机信息系统安全的法规

1. 明知没有授权或者超越授权存取范围，使用计算机获取以下信息：依据美国总统命令或者法令应当保密，以防止因为国防及外交关系原因而未被授权披露的信息，或者由 1954 年原子能法第 11 条 R 项所规定的应当管制的任何数据，并有理由相信行为人获取这些信息时知道它们能够用于危害美国利益，或者为了他国利益。有意交流、传递、传播，或者使可以交流、传递、

① 资料来源：http://www.cybercrime.gov/compcrime.html，美国司法部计算机犯罪站点。

传播，或者意图交流、传递、传播，或者意图使交流、传递、传播这些信息给无权接收的人，或者有意持有这些信息并没有把它们交给有权接收的美国联邦官员或者职员的行为。(《美国联邦法典》第 18 篇第 1030 条第 a 款)

2. 有意非授权存取美国联邦部门或者机构的非公用的计算机，这些计算机是为联邦政府专门使用的，或者虽非为联邦政府专用，但是由美国联邦政府使用或者为其服务，而这些行为影响了这种使用。(《美国联邦法典》第 18 篇第 1 030 条第 a 款)

3. (A) 明知而故意引起程序、信息、指令、命令的传送，并有意引起受保护计算机的非授权性破坏。(B) 意图存取受保护的计算机，并鲁莽地引起破坏结果。(C) 意图存取受保护的计算机，而导致破坏结果。(《美国联邦法典》第 18 篇第 1030 条第 a 款)

4. 未授权有意进入一设备，该设备用于提供电子通信服务。(《美国联邦法典》第 18 篇第 2701 条第 a 款)

5. 有意超越授权进入一设备，并因此获得、修改、阻止对有线和电子通信已授权的使用的行为。(《美国联邦法典》第 18 篇第 2 701 条第 a 款)

6. 有意地非授权或者超越授权存取范围，使用计算机获取以下信息：(A) 金融财政机构或者第 15 篇 1602 条 (n) 规定的信用卡发行人的金融记录中的信息，或者消费者报告机构有关消费者文件中的信息，这些概念由《公正信用报告法》(15U.S.C.1681 et seq) 规定。(B) 美国联邦任何部门或者机构的信息。(C) 来自任何受到保护的计算机中的信息，如果这些信息涉及州际的或者与国外交流。(《美国联邦法典》第 18 篇第 1030 条第 a 款)

(二) 保护电子商务交易秩序的法规

7. 明知并且意图诈取，非授权或者越权存取受保护的计算机，并进一步诈取，或者获取任何有用的东西，除非这种诈取的

目标仅仅是计算机的使用，并且这种使用的价值一年内不超过5 000美元。(《美国联邦法典》第18篇第1030条第a款)

8. 明知并意图诈取使用密码或者类似信息而无需再授权即可访问计算机的服务，而且这种服务的诈取影响了州际或者与外国的商务，或者被使用的计算机由美国联邦政府使用或者为其服务。(《美国联邦法典》第18篇第1030条第a款)

9. 意图从个人、公司、协会、教育机构、金融机构、政府部门或者其他法律团体勒索钱物或者其他有价值的东西，在州际或者国际商务中传送任何包括威胁破坏受保护计算机的信息。(《美国联邦法典》第18篇第1030条第a款)

10. 明知并有意通过一台或者多台欺骗式存取装置，诈取产品、使用或者服务。(《美国联邦法典》第18篇第1029条第a款)

11. 明知并且有意利用或者通过一台或者多台非授权存取装置，诈取服务，在任何一年内获取的总价值超过1 000美元或者更多。(《美国联邦法典》第18篇第1029条第a款)

12. 明知并有意欺诈支配15台或者更多欺骗性或者未授权的存取装置。(《美国联邦法典》第18篇第1029条第a款)

13. 在控制或者监管情况下，明知并有意诈取产品、服务，或者欺骗地支配设备制造装置。(《美国联邦法典》第18篇第1029条第a款)

14. 在控制或者监管情况下，明知并有意诈取使用权、产品、服务，或者修改通信设备后获取非授权的通信服务，并支配该通信设备的行为。(《美国联邦法典》第18篇第1029条第a款)

15. 在控制或者监管情况下，明知并有意诈取使用权、产品、服务，或者支配扫描接收设备的行为。(《美国联邦法典》第18篇第1029条第a款)

16. 在控制或者监管情况下，明知而使用、生产、交易，或

者支配硬件、软件设备，而且行为人已知通信设备包括或者相关的识别信息已经被插入或者修改，这样的通信设备可以被非授权地获取通信服务。(《美国联邦法典》第 18 篇第 1029 条第 a 款)

17. 未获得信用卡系统成员或者其机构的授权，明知并有意欺诈，致使或者安排他人代替该成员或者机构支付，而用存取设备进行了一起或者更多的交易，并且这种犯罪已经影响了州际或者国际商务的行为。(《美国联邦法典》第 18 篇第 1029 条第 a 款)

18. 提供公众电信服务的自然人或者实体将服务中存储的交流内容泄露给任何他人或者团体的行为。(《美国联邦法典》第 18 篇第 2702 条第 a 款)

19. 提供公众远程计算机服务的自然人或者实体将服务中承载或者保存的任何交流信息内容泄露给任何他人或者团体的行为。(《美国联邦法典》第 18 篇第 2702 条第 a 款)

三、英国电子商务领域刑事立法状况

英国在 1990 年以前没有针对计算机安全和犯罪的单行立法，司法界一般把计算机相关罪案中的计算机视做犯罪工具，对于这类案件，根据犯罪危害的对象和造成的后果，按照传统的犯罪处罚。因此，英国关于电子商务领域刑事实体法律、法规不多，主要有 1981 年《伪造文书及货币法》、1984 年《资料保护法》和 1990 年《计算机滥用法》。

20 世纪 80 年代末，计算机安全及犯罪问题在英国日益严重，依照现有的法律已经不能有效惩治。1990 年英国制定了《计算机滥用法》，该法的重点是保护计算机信息系统安全，把以下行为规定为犯罪：

1. 非法侵入计算机信息系统的行为：(A) 使计算机执行任何意图获取访问存储在计算机内的应用程序或者计算机数据；(B) 其意图获取的访问是未经授权的；(C) 其明知自己的行为是在使计算机执行前述操作。(《计算机滥用法》1.1)

2. 非法修改计算机内程序或数据的行为：（A）实施了使计算机未经授权对计算机内应用程序或者数据进行修改的行为；（B）实施以上行为时具有这样的意图和认识：意图引起对计算机任意内容的修改，并以此损害计算机运行，或者妨碍或阻止对计算机内的应用程序和数据的合法访问，或者损害了上述应用程序的执行和数据的可靠性。行为人认识到自己所意图进行的任何修改都是未经授权的行为。

英国保护电子商务交易秩序的法律主要有 1981 年《伪造文书及货币法》和 1984 年《资料保护法》。其中，1981 年《伪造文书及货币法》规定了伪造、变造文书的行为为犯罪，即“意图使人相信系真正者并实施对其本人或第三人不利益之作为或不作为，而制作虚伪文书者”，“基于同样之目的而复制虚伪文书”，或者“行使虚伪文书或其影本者”。该法除了基于复制设备的发达将复制影本纳入伪造文书罪外，并基于计算机设备运用的普及，将“以机械、电子或其他方法记录或记忆之磁碟、磁带、音带或其他设备”纳入文书的范围，并规定“以对于机器行使下述文书为目的，而由机器予以识别、操作或不操作时者”，视为行为人所为。1984 年《资料保护法》规范对计算机所处理记录的个人资料的搜集、持有、公开等行为，以防止不当侵害个人隐私权。该法规定，个人资料的使用者有向资料保护登记处申报登录其姓名、住所、持有资料的概要、持有或使用的目的、搜集资料的来源、拟公开此资料的对象等事项，自己不持有资料而为他人提供资料处理的计算机服务站还必须同时申报其经营者的姓名及住所。该法规定，未经登录而持有个人资料，或者明知或有意持有与登录内容不同的个人资料，或者不遵从资料保护登记处对违反资料保护准则者所发布的处置命令的，都属于犯罪行为。

四、德国电子商务领域刑事立法状况

虽然德国犯罪学刑法学界关于计算机安全与犯罪的理论研究

比较领先，然而德国是大陆法系国家，严守罪刑法定主义，在计算机安全与犯罪问题上立法十分谨慎，一直到 1986 年 8 月 1 日刑法修正案（第二次经济犯罪防治法）才加入了若干涉及计算机安全与犯罪的条款。现行德国刑法中有关电子商务领域刑事立法主要有①：

（一）保护电子商务信息系统安全的法条

1. 变更数据。非法删除、隐匿，使其不能使用或变更数据（《德国刑法典》第 202 条 a 第 2 款）的。犯本罪未遂的，亦应处罚。（《德国刑法典》第 303 条 a）

2. 破坏计算机。为下列行为之一，非法干扰对他公司、企业或当局具有重要意义的数据处理程序的：实施 303 条 a 第 1 款之犯罪的，或对数据处理设施或计算机加以毁损、损坏，使其不能使用、删除或变更的。犯本罪未遂的，亦应处罚。（《德国刑法典》第 303 条 b）

3. 探知数据。非法为自己或他人探知不属于自己的经特别保护的数据的。这里的数据仅指以电子或其他不能直接提取的方法存储或传送的数据。（《德国刑法典》第 202 条 a）

4. 对数据处理的影响视同在法律事务交往中的欺骗。在法律事务交往中对数据处理施加错误影响的。（《德国刑法典》第 270 条）

（二）保护电子商务交易秩序的法条

5. 伪造支付证卡和欧洲支票。为下列行为，意图在法律交往中进行欺骗，或使此等欺骗成为可能的：（1）伪造或变造本国或外国的支付证卡或欧洲支票；或（2）为自己或他人获取、持有转让或使用此等伪造的证卡或支票。这里所述支付证卡、欧洲支票是指下列证卡或支票：（1）使制造商在支付周转中相信对方

① 徐久生，庄敬华译：《德国刑法典》，中国法制出版社 2000 年版，第 136～205 页。

一定支付；且（2）通过设置或译成电码防止伪造。（《德国刑法典》第 152 条 a）

6. 散发淫秽文书。以无线电方式传播淫秽文书的。（《德国刑法典》第 184 条）

7. 侵害邮政或电讯秘密。未经授权，将其作为从事邮政或电讯业务企业所有人或雇员，而获悉的属于邮政或电讯秘密的事实告知他人的。非从事邮政或电讯业务之公务人员，经授权或未授权而知悉邮政或电讯秘密，未经授权而将其告知他人的。（《德国刑法典》第 206 条）

8. 计算机诈骗。意图使自己或第三人获得不法财产利益，以对他人的计算机程序作不正确的调整，通过使用不正确的或不完全的数据，非法使用数据，或使用其他手段对他人的计算机程序作非法影响，致他人的财产遭受损失的。（《德国刑法典》第 263 条 a）

9. 伪造有证据价值的资料。意图在法律事务交往中进行欺骗，存储或变更具有证据价值的资料，在使用时提供不真实的或伪造的文书，或使用此等存储的或变更的资料的。（《德国刑法典》第 269 条）

进入 20 世纪 90 年代，德国在计算机安全与犯罪方面的理论研究和立法建设发展十分迅速，1997 年 6 月 13 日德国联邦议院通过了世界上第一部全面调整信息时代新型通信媒体的法律——《信息和通信服务法》（德文简称 IUKDG），又称为《多媒体法》，并于 1997 年 8 月 1 日开始实施。该法由三个新的联邦法律和六个附属条款组成，三个新的联邦法令分别为：远程服务法（The Tele-Service Act）、数据保护法（The Data Protection Act）和数字签名法（The Digital Signature Act）。该法涉及互联网的方方面面，从 ISP 的责任、保护个人隐私、数字签名、网络犯罪到保护未成人等，是一部全面的综合性法律。在计算机安全与犯罪方面，《多媒体法》修改了刑法和与行政违法有关的法律，主要的

变化是扩大了刑法中“出版物”的概念，即“出版物”包括电子的、视觉的或其他类型的数据存储介质。《德国刑法典》对那些发布含有违禁内容“出版物”的人施以处罚，如煽动民族仇恨、描写暴力或某些色情的内容。根据《多媒体法》，目前出版物包括存储在计算机内或网络中但未“打印出”的电子数据。刑法条文不适用于‘实时’传输的信息，即未进行某种形式固化的信息。

五、日本电子商务领域刑事立法状况

日本和德国都是大陆法系国家，其电子商务领域刑事立法模式与德国极为相似，一直到1987年才修订刑法，增加了若干关于计算机安全与犯罪的条文。修订后的日本刑法还为新增条文中所使用电磁记录这一概念作了法律上的定义，即“是指用电子方式、磁气方式及其他不能通过人的知觉认识的方式制作的、供电子计算机进行信息处理所使用的记录”。现行日本刑法关于电子商务领域刑事立法条文规定了以下犯罪行为①：

（一）保护电子商务信息系统安全的刑法条文

1. 损坏电子计算机等妨碍业务。损坏供他人业务上使用的电子计算机或者供其使用的电磁记录，或者向供他人业务上使用的电子计算机输入虚伪信息或者不正当的指令，或者以其他方法使电子计算机不能按照使用目的运行或者违反使用目的运行，妨害他人业务的。（《日本刑法典》第234条）

2. 毁弃公用文书。毁弃供公务机关使用的文书或者电磁记录的。（《日本刑法典》第258条）

3. 毁弃私用文书。毁弃他人的有关权利、义务的文书或者电磁记录的。（《日本刑法典》第259条）

（二）保护电子商务交易秩序的刑事条文

4. 公正证书原本不实记载。对公务员作虚伪申述，使其在

① 张明楷译：《日本刑法典》，法律出版社1998年版，第47～80页。

登记簿、户籍簿及其他权利或者公正证书原本上作不实记载，或者使其在作为有关权利或者义务的公正证书原本使用的电磁记录上作不实记录的。(《日本刑法典》第 157 条)

5. 行使伪造的文书。行使第 154 条至 157 条的文书或者图画，或者将前条第一项的电磁记录供作公正证书的原本使用的。(《日本刑法典》第 158 条)

6. 不正当制作和提供电磁记录。以使他人的事务处理出现错误为目的，不正当制作供该处理事务使用的有关权利、义务或者证明事实的电磁记录的。以使他人的事务处理出现错误为目的，将不正当制作的有关权利、义务或者证明事实的电磁记录，提供给他人处理事务使用的。犯罪未遂的，亦应当处罚。(《日本刑法典》第 161 条之二)

7. 使用电子计算机诈骗。向他人处理事务使用的电子计算机输入虚伪信息或者不正当的指令，从而制作与财产权的得失或者变更有关的不真实的电磁记录，或者提供与财产权的得失、变更有关的虚伪电磁记录给他人处理事务使用，取得财产上的不法利益或者使他人取得的。(《日本刑法典》第 246 条)

2000 年初日本中央机关网站频频遭到黑客的入侵，一连串黑客入侵事件，使当局认识到网络安全及电子商务交易安全是一大难题，也暴露了日本在电子商务刑事立法上的漏洞。日本政府仿效欧美，决定从 2000 年 2 月 13 日起实施黑客法，禁止对计算机网络未经授权的访问。该法将未经授权的网络存取定义为使用他人的身份及密码侵入电脑网络。若该行为被认定为黑客等其他电脑相关犯罪的第一步，将被处以最高一年的徒刑。在未经所有人许可下，交易他人之身份，将被处以最高 30 万日元的罚款①。

① 《日本开始实施黑客法》，http：//www.ccidnet.com.cn/，2000 年 2 月 14 日。

六、法国电子商务领域刑事立法状况

法国也是大陆法系国家，其计算机安全与犯罪方面的立法采用的是修改刑法的模式。现行的《法国刑法典》于 1992 年 7 月修改，1994 年 3 月 1 日生效，该刑法典中关于电子商务领域犯罪的刑事立法包括以下部分：

（一）保护电子商务信息系统安全的刑事立法

现行《法国刑法典》设立专章规定了侵犯资料自动处理系统罪，规定了以下犯罪行为：

1. 采用欺诈手段，进入或不肯退出某一资料数据自动处理系统的全部或一部分的行为。（《法国刑法典》第 323－1 条）

2. 妨碍或扰乱数据资料自动处理系统的运作行为。（《法国刑法典》第 323－2 条）

3. 采取不正当手段，将数据资料输入某一自动处理系统，或取消或变更该系统存储的资料的行为。（《法国刑法典》第 323－3 条）

4. 为准备第 323－1 条至第 323－3 条所指一项或多项犯罪，并以一项或多项实际活动表明在进行此种准备，参加由此形成的小集团或参与为此目的达成默契者，处上述所指犯罪本身当处的刑罚，或者处其中受到最严厉制裁的犯罪当处的刑罚。（《法国刑法典》第 323－4 条）

（二）保护电子商务交易秩序的刑事立法

5. 不怀好意地截收、隐匿、使用或泄露经电讯渠道发出、转达或收取的通信信件，或者安装截收设备，以期实际进行此种截收的行为。（《法国刑法典》第226－15 条）

6. 对记名信息资料进行自动化处理，其中包括不慎而进行了处理，或指使他人进行此种处理而未遵守法律规定的在开发此种信息时应当事先履行的手续的行为。（《法国刑法典》第226－16条）

7. 对记名信息资料进行自动化处理，或者指使他人进行此种处理，而不采取一切必要的审慎措施，以确保信息安全，尤其是防止受到歪曲、损坏或被透露给未得到允许的第三人的行为。(《法国刑法典》第 226－17 条)

8. 在法律规定的情况之外，将有关犯罪、判刑或关押措施的记名信息资料输入计算机或者以信息存储保留的行为。(《法国刑法典》第 226－19 条)

9. 毁坏、损坏或隐匿任何文件资料、材料、建筑、设备、设施、机械、技术、装置或信息自动处理系统或者对其加以仿制的，具有危害国家基本利益的性质的行为，实施上述行为的目的在于为外国国家、外国企业或外国组织服务，或者在外国控制下实施此种行为的。(《法国刑法典》第 411－9 条)

10. 本法典第三卷所指的盗窃、勒索、破坏、毁坏、损坏财产以及在计算机信息方面的犯罪，在其同以严重扰乱公共秩序为目的，采取恐吓手段或恐怖手段进行的单独个人或集体性攻击行为相联系时，构成恐怖活动罪。(《法国刑法典》第 421－1 条)

第二节　我国惩治电子商务犯罪的刑事立法

我国对计算机安全与犯罪问题关注较早，20 世纪 80 年代初就制定了大量行政法规和法律，为相关的刑事立法积累了经验。1981 年公安部成立计算机安全监察机构，并着手制定有关计算机安全方面的法规。1986 年 4 月开始草拟《中华人民共和国计算机信息系统安全保护条例》(征求意见稿)。1988 年 9 月 5 日第七届全国人民代表大会常务委员会第三次会议通过的《中华人民共和国保守国家秘密法》在第三章第 17 条中第一次提出：采用电子信息等技术存取、处理、传递国家秘密的办法，由国家保密工作部门会同中央有关机关规定。1989 年首次在重庆西南铝厂发现计算机病毒后就引起有关部门的重视。公安部发布了《计

算机病毒控制规定（草案）》，开始推行“计算机病毒研究和销售许可证”制度。1991 年 5 月 24 日，国务院第 83 次常委会议通过了《计算机软件保护条例》，该条例是我国颁布的第一个有关计算机的法律。1991 年 12 月 23 日，国防科学技术工业委员会发布了《军队通用计算机系统使用安全要求》，对计算机实体（场地、设备、人身、媒体）的安全、病毒的预防以及防止信息泄露提出了具体措施。1992 年 4 月 6 日机械电子工业部发布了《计算机软件著作权登记办法》，规定了计算机软件著作权管理的细则。1994 年 2 月 18 日，国务院发布了《中华人民共和国计算机信息系统安全保护条例》。1996 年 2 月 1 日国务院发布了《中华人民共和国计算机信息网络国际联网管理暂行规定》。1996 年 3 月 14 日，国家新闻出版署公布了电子出版物暂行规定，加强包括软磁盘、只读光盘、交互式光盘、图文光盘、照片光盘、集成电路卡和其他媒体形态的电子出版物的保护。1997 年 6 月 3 日，国务院信息化工作领导小组在北京主持召开了“中国互联网信息中心成立暨《中国互联网络域名注册暂行管理办法》发布大会”，宣布成立中国互联网络信息中心（CNNIC），并发布了《中国互联网络域名注册暂行管理办法》和《中国互联网络域名注册实施细则》。1997 年 12 月 8 日，国务院信息化工作领导小组制定了《中华人民共和国计算机信息网络国际联网管理暂行规定实施办法》。同年公安部也发布了《计算机信息网络国际联网安全保护管理办法》。1998 年国家保密局发布了《计算机信息系统保密管理暂行规定》，公安部、中国人民银行发布了《金融机构计算机信息系统安全保护工作暂行规定》。与此同时，原邮电部也出台了《国际互联网出入信道管理办法》，通过严把信息出入关口、与用户签订责任书、设立监测点等方式，加强对互联网使用的监督和管理。

随着计算机安全与犯罪问题日益严重，公安部授权起草涉及计算机安全与犯罪问题的专门性法条，建议立法机关将其纳入

1997 年新刑法典中，这些专门性法条建议增设以下犯罪：非法侵入计算机信息系统罪，窃取计算机信息系统程序、数据罪，破坏计算机信息系统程序、数据罪，破坏计算机信息系统设备罪，窃用计算机服务罪。除此之外，还建议对于利用计算机实施贪污、盗窃、诈骗，制作、传播反动、淫秽文字、图像等其他涉及计算机的犯罪行为，可分别包含在刑法分则的其他有关条款中。立法机关经过讨论研究，采纳了其中一部分建议，在 1997 年刑法修订中，增加了关于计算机安全与犯罪的三个条款，即第 285 条、第 286 条和第 287 条。1997 年 12 月 9 日最高人民法院审判委员会第 951 次会议通过的《关于执行〈中华人民共和国刑法〉确定罪名的规定》，规定了两个新罪名，即非法侵入计算机信息系统罪和破坏计算机信息系统罪。对于涉及计算机的其他犯罪行为，1997 年新刑法典第 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。"2000 年 12 月 28 日全国人大常委会通过了《关于维护互联网安全的决定》，对以上行为"构成犯罪的，依照刑法有关规定追究刑事责任"。此外，最高人民法院还根据司法实践中遇到的问题，先后制定了《关于审理盗窃案件具体应用法律若干问题的解释》、《关于审理扰乱电信市场管理秩序案件具体应用法律若干问题的解释》等若干司法解释。1997 年新刑法是我国第一部规范计算机安全与犯罪的刑事法律，与《关于维护互联网安全的决定》和相关的司法解释共同构筑了我国打击电子商务领域犯罪的刑事法律体系。

目前我国关于电子商务领域犯罪的刑事法律体系规定了以下犯罪行为：

（一）危害电子商务计算机信息系统安全的犯罪

1. 非法侵入计算机信息系统罪。刑法第 285 条规定："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。"

2. 破坏计算机信息系统罪。刑法第 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作，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作，后果严重的，依照第一款的规定处罚。"

（二）危害电子商务秩序的犯罪

3. 利用计算机实施的其他犯罪。刑法第 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。"刑法第 287 条规定，对利用计算机实施所列犯罪，按照相应的一般形式的犯罪进行定罪处罚。《关于维护互联网安全的决定》也作了相似的规定。

3. 由于计算机有关犯罪具有许多新的犯罪形式，这种概括性的规定不能适应计算机相关犯罪的特殊情况，在司法实践中出现问题较多。为此，最高人民法院通过司法解释的方式，对刑法第 287 条规定的一部分犯罪行为的定罪量刑进行了解释，例如《关于审理盗窃案件具体应用法律若干问题的解释》第 10 条规定，"根据刑法第 196 条第 3 款的规定，盗窃信用卡并使用的，以盗窃罪定罪处罚；其盗窃数额应当根据行为人盗窃信用卡后使用的数额认定"。《关于审理扰乱电信市场管理秩序案件具体应用法律若干问题的解释》第 7 条规定，"将电信卡非法充值后使用，造成电信资费损失数额较大的，依照刑法第 264 条的规定，以盗窃罪定罪处罚。"第 8 条规定，盗用他人公共信息网络上网账号、密码上网，造成他人电信资费损失数额较大的，依照刑法第 264 条的规定，以盗窃罪定罪处罚。

根据我国电子商务领域刑事立法的特征，本书把电子商务领域犯罪分为危害电子商务计算机信息系统安全的犯罪、电子商务

犯罪和电子商务关联犯罪三类，在以后的章节进行研究。

目前，世界各国电子商务领域刑事立法基本上有两种立法模式，一种是以美国、英国为代表的制定单行法律的模式，一种是以德国、日本、法国为代表的修改刑法的模式。这些国家之所以采用不同的立法模式，是与其法律制度传统有着密切的联系。但是，在适应电子商务发展需要上，两种立法模式的优劣有别。首先，由于一国刑法具有相当程度的稳定性，修改刑法典是比较庞大而漫长的工程，修改刑法增补电子商务领域刑事立法的模式难以适应电子商务迅猛发展的需要。其次，对于已经发展比较成熟、理论研究比较透彻和实践经验积累比较丰富的犯罪形式，采用单独立法的方式要比按照一般犯罪形式的法律规定处罚更具威慑力和打击力。由于修改刑法典模式固有的缺陷，大陆法系国家中有一些也在采纳单独立法的模式，如德国的《多媒体法》和日本的《黑客法》。

我国刑事立法模式与大陆法系国家类似，采取修改刑法的模式构建电子商务领域刑事立法体系，但是这一法律体系尚未完备，目前在没有修改刑法的情况下，大多通过司法解释的方式，解决司法实践中遇到的新形式犯罪的定罪处罚问题。由于我国刑法明确规定了罪刑法定原则，司法解释不能代替刑事立法进行越权解释，司法解释能够发挥的作用十分有限。面对日趋严重的电子商务领域犯罪问题，我国现行电子商务领域刑事法律体系缺乏灵活性、适应性的缺点越来越突出，因此作者建议尽快制订电子商务领域的单行刑事法律，理由如下：(1) 我国电子商务发展迅速，电子商务领域犯罪问题已经十分严重，其中许多犯罪形式无法在现行刑法中找到适当的条款惩治，不宜在各章中都增补条款。(2) 电子商务领域犯罪侵犯的犯罪客体非常广泛，不适应我国刑法将犯罪按犯罪客体分类规定的体系，不宜将相关条款分布在刑法分则的各章节中，如果将其分布在刑法分则各章节中，难免条款内容的重复和冗余，影响刑法分则章节的协调性和完整性。

第五章　电子商务犯罪

第一节　电子商务犯罪概述

电子商务秩序是电子商务的活动规则，没有正常的电子商务秩序，电子商务主体的合法权益得不到保障，就会严重影响电子商务发展的社会公众基础。因此，建立和维护正常的电子商务秩序，对保障我国电子商务发展起着至关重要的作用。电子商务犯罪严重侵害电子商务秩序，同时给现行刑事法律体系带来许多新的问题，本章主要研究电子商务犯罪问题。

电子商务是开放性数字网络上的经济活动，不仅包括电子商务交易方之间的交易活动，还包括网络通信服务商、金融结算机构、认证机构和其他主体之间与电子商务相关的各种活动。电子商务犯罪是发生在电子商务活动过程中侵害电子商务秩序的犯罪，不仅包括发生电子商务交易过程中的犯罪，如电子商务领域的信用卡诈骗罪、诈骗罪、合同诈骗罪和非法行医罪等，而且包括电子商务企业经营管理、商品广告、售后服务等活动中的犯罪，如电子商务领域的侵犯著作权罪、侵犯商业秘密罪等。电子商务犯罪具有以下特征：

（1）主体群不断扩大。我国互联网络应用发展迅速，截至2000年3月底，共有电子商务类网站一千一百多家，其中购物网站八百多家，拍卖网站一百多家，远程教育网站一百八十多家，远程医疗网站二十多家。中国网民有28.6%参与过电子商

务，20.3%进行过网上购物①。从电子商务参与者的结构特点来看，参与电子商务活动的多为青年人，而且主要集中在经济较发达的大中城市，文化程度偏高，年龄呈下降趋势。据香港一家调查公司的调查报告，中国上网人口的平均年龄为 30 岁，该年龄段的人多具有大学学历，同时，这一平均年龄正在逐渐下降，一些只受过初级或中级教育的民众也使用互联网②。这一趋势表明电子商务正日益为公众所接受，电子商务活动主体群日益扩大。作为网络用户组成部分的电子商务犯罪的犯罪人，当然具有以上特性，他们可能来自多个行业，可能是一般的网络用户、电子商务消费者、电子商务商户、金融结算机构职员、认证机构职员、网络通信服务商、服务电子商务的政府机构工作人员等。

（2）犯罪心态多表现为以牟利为目的，或者出于其他与经济利益直接相关的目的动机。如利用金融网络系统窃取金融机构资金、利用电子商务进行诈骗、利用国际电子资金过户系统进行洗钱等，都是牟利型的犯罪。但是，也有为不正当竞争目的进行的犯罪，如窃取竞争对手商业秘密、侵犯著作权等，还有为避免经济损失而泄露证券内幕消息，进行证券内幕交易等犯罪。

（3）危害行为多种多样，且都表现为充分利用电子商务计算机信息系统特性。电子商务犯罪的具体危害行为有多种，共同特征是行为人在实施这类犯罪过程中，一般不会侵犯计算机信息系统安全，反而希望计算机信息系统能够正常工作，以利于按照行为人的指令实现犯罪意图。当然，在行为人实现犯罪的主要目的后，不排除为毁灭罪证、干扰侦查进行的破坏计算机信息系统安全的行为。

---

① 《中国 28.6%网民参与电子商务》，http://www.enews.com.cn/，2000 年 7 月 1 日。

② 《中国网民平均 30 岁多具大学学历》，http://www.enews.com.cn/，2000 年 6 月 25 日。

（4）危害电子商务秩序的犯罪侵犯的法益有多种，既可能是单位、个人的财产权、保守秘密权，也可能是单位、个人的名誉权，还可能是国家管理电子商务的正常秩序。

电子商务立法是众望所归，而我国尚没有关于电子商务的专项立法。我国惩治危害电子商务秩序犯罪的法律根据主要是《刑法》中涉及电子商务的、规定传统犯罪的若干法条，以及《关于维护互联网安全的决定》和最高人民法院、最高人民检察院颁布的有关司法解释。由于我国现行的电子商务刑事立法体系尚不完备，对于某些严重危害电子商务的行为甚至找不到可以适用的法律，急需立法完善。

电子商务犯罪中的具体犯罪多，而且随着电子商务的进一步发展，其范围将进一步扩大。这些犯罪中，有些犯罪只是在犯罪形式、犯罪方法上有所改变，采用计算机、网络技术手段或者利用电子商务系统的功能实施犯罪行为，一般没有产生新的法律问题，在刑法适用上不会发生困难，如电子商务领域的非法经营罪、损害商业信誉、商品声誉罪等；有些犯罪带来了新的法律问题，但是在现行法律体系内仍然可以依法处理，如电子商务领域合同诈骗罪，虽然利用在互联网络签订电子合同的方法进行合同诈骗是新的法律问题，但是，修订后的《合同法》把数据电文规定为合同书面形式的一种，行为人通过电子商务进行合同诈骗的，可以依据刑法中合同诈骗罪的相关条款和《合同法》的相关规定进行定罪量刑；有些犯罪是电子商务发展中新出现的犯罪，超出了现行刑事法律的范围，司法实践中对这些犯罪适用刑法存在困难，这类犯罪是本书研究的重点。下面仅就目前表现比较突出、司法实践中遇到法律问题较多的若干种犯罪进行讨论。

第二节 电子商务领域的信用卡诈骗罪

一、电子商务领域的信用卡应用现状

电子商务的优越性之一，是能通过数字化网络实现安全、实时、便捷的远程商品交易。其中，资金流动便利是实现电子商务的关键，虽然目前的电子商务中，还存在汇款、货到付款等形式的资金支付，但是国际电子商务应用的主流和未来发展趋势是信用卡网上支付。我国的金融业为适应电子商务发展的需要，迅速推进金融电子化、网络化建设，适应电子商务应用需要的新信用卡业务不断产生，提供网上支付功能信用卡越来越多，如招商银行的“一卡通”、中国银行的“长城卡”和建设银行的“龙卡”等。同时，使用信用卡进行的电子商务数量日增，交易金额越来越大。

在研究电子商务领域信用卡诈骗犯罪前，有必要先了解信用卡及信用卡业务运作原理。信用卡是银行或其他财务机构签发给那些资信状况良好的人士，用于在指定的商家消费或在指定银行机构存取现金的特制卡片，是一种特殊的信用凭证，具有转账结算、存取现金和消费信贷等功能。电子商务领域的特种信用卡业务主要有两种，一种是本地或者异地的信用卡消费或者存取现金业务，一种是电子商务交易中的网上支付业务。前者通常通过ATM（自动柜员机）、POS机（销售终端）等设备来使用，顾客把信用卡插入这些设备的插口中，机器读入信用卡上的磁条信息，这些信息中包含了发卡银行、发卡营业点、密码号、开支用途的区分等，然后先进行信用卡的合法性检查、密码核对，如果以上两步都正确，则按照顾客的要求设定的存取款或者转账操作。后者可直接用于互联网上的商品交易，应用日益普遍。首先，电子商务商户要从银行等金融服务机构获得商务账户（这种

特殊商务账户是用来接收信用卡并处理信用卡业务，获得资金支付的一种账户），然后，进行网上购物的消费者确定选购商品后，填写维护交易安全的加密表格，该表格中既包含了所选购商品的信息，也包含了消费者网上支付信用卡的信息。该加密表格直接传送到一个支付网关，由支付网关来全权处理。支付网关又称为支付处理软件或支付处理商等，它实际上是一个连接电子商务商户和银行的网关。当支付网关收到商店转发来的信用卡资料后，首先会将它们传送到这张信用卡的发卡银行进行有效性验证，包括估计潜在的信用卡诈骗的可能性。验证完毕后，发卡银行将资金转入支付网关，由支付网关将资金转移到网上商店的商务账户中，最终完成整个交易。

二、电子商务领域的信用卡诈骗犯罪现状

伴随电子商务和信用卡业务的迅速发展，电子商务领域的信用卡诈骗犯罪日益猖獗。据付款和清账联盟（The Association for Payment and Clearing Services）在 1995 年年度总结报告中提到，仅在英国一个国家，1995 年信用卡诈骗案的总金额超过 8 000 万英镑；维萨信用卡公司（VISA）报告，1997 年信用卡诈骗造成直接经济损失为 4.9 亿美元。电子商务领域的信用卡诈骗犯罪在我国也十分严重，据有关资料，截止 1994 年这类案件已经超过万起，造成银行直接经济损失数千万元，犯罪分子非法获利数额呈逐年上升趋势，1998 年我国台湾地区信用卡刷卡金额达到 5 000亿元台币，因此导致的亏损也超过 7.4 亿元台币。目前电子商务领域信用卡诈骗犯罪主要有以下几种表现形式：

（1）破解信用卡密码秘密，伪造信用卡并使用

行为人利用技术手段破解金融机构信用卡加密密钥，并使用这一密钥伪造能够被 ATM 机等自动取款装置或者特约商户刷卡机认可的信用卡，然后使用这种伪造的信用卡获取钱款或者货物。典型案例是青岛曾某伪造并使用伪造信用卡案：1998 年青

岛工商银行技术人员曾某在计算机系统的升级测试和机器维修中，发现可以破解中国某银行的密钥，于是用自己编写的计算机程序破解了该密钥，并在单位的机器设备上制作了 100 多张伪造的信用卡。曾某把伪造的信用卡交给自己的朋友王某等人，详细告知如何使用伪造的信用卡，并及时配合王某在自动柜员机上取款，其本人也使用伪造的信用卡在自动柜员机上取款，他们在多个城市提取现金共计 70 多万元①。

（2）窃取他人信用卡信息，伪造信用卡并使用

信用卡一般使用两种方式存储用户账户信息，即磁条存储和 IC 卡存储，这些存储的信息如果被他人盗取，可能被用于伪造与被害人信用卡账户信息完全相同的信用卡。香港曾经发生过一起特约商户窃取客户信用卡信息并伪造信用卡的案件。某家“易办事”信用卡特约商户工作人员事先准备了用于窃取信用卡账号的读卡机，并在客户刷卡位正上方安装了微型摄像机，在客户刷卡时，行为人非常隐蔽地将信用卡在自己的读卡机上刷卡，获得了该客户信用卡中的全部信息，并摄取客户输入的密码。而后，行为人将窃取的信用卡信息提供给国际信用卡伪造集团，利用这些信息伪造了信用卡，使被害人蒙受了巨大的经济损失。

（3）金融机构内部人员利用职务便利，制作与他人信用卡账户信息相同的信用卡并使用

金融机构内部人员，特别是信用卡业务的管理人员，能够接触到用户的信用卡账户密码等秘密资料，加之具有工作便利条件，有机会伪造与客户信用卡完全相同的信用卡。1999 年中国银行南京分行信用卡部职员孙某私自用磁卡机伪造与唐某账户卡号信息相同的信息磁卡，并持伪造的磁卡先后在白下路、中山东

① 钱欣：《全国首例自制信用卡“盗”款 70 余万元巨案上海告破》，《楚天都市报》，1999 年 1 月 10 日。

路 ATM 自动取款机上取得人民币 2 500 元①。

（4）窃取他人网上支付信用卡账户、密码，进行网上消费

犯罪人利用计算机技术，非法侵入信用卡公司或者电子商务商户计算机信息系统，窃取客户信用卡网上支付账户密码信息，然后进行网上消费或者转账。如 2000 年 3 月意大利警方逮捕了两名非法进入美国银行电脑系统，并冒用他人信用卡作案的电脑黑客夫妇，他们通过破译口令，不断“潜入”美国花旗银行的信用卡电脑系统库，盗窃用户的个人资料，并用客户的信用卡参与网上博彩和消费。

（5）虚增网上支付信用卡账户密码，并使用其进行网上消费

信用卡发卡金融机构管理网上支付账户密码，这些个人资料一般存储在金融机构的计算机信息系统中，在电子商务交易中，只要验证计算机信息系统中存在对应的账户密码，交易就被核准同意。行为人可能非法侵入这些机构的计算机信息系统，在用户资料数据库里虚增网上支付账户密码，行为人如果是金融机构内部管理人员，可能利用管理上的疏漏直接修改用户数据库，虚增信用卡账户，然后使用该账户进行网上消费或者转账。

（6）特约商户与盗窃他人网上支付账户密码者勾结，使用他人网上支付账户资金

在这类犯罪中，网上商店与盗窃他人网上支付账户密码的行为人勾结，使用他人账户在该网上商店大量购物，而实际根本不交付商品，被害人的资金却源源不断地转移到网上商店的账户中。2000 年俄罗斯警方破获一个电脑犯罪团伙，他们涉嫌从互联网零售商那里偷窃信用证号码，并非法诈取 63 万美元。这个网上犯罪团伙由一名 22 岁的俄罗斯青年担任头目，他首先注册了一个名为 Politshop 的互联网零售商店，并与莫斯科银行达成

① 《自编程序伪造信用卡，南京一银行职员被判刑》，《电脑日报》，1999 年 8 月 1 日。

协议允许其开展信用卡业务。然后，他指使同伙从其他互联网零售商那里窃取顾客的信用卡号码，使用这些信用卡从 Politshop 购物，这样顾客的钱就转到 Politshop 零售商店的账上，他们也就可以堂而皇之地从银行把赃钱提走。

三、信用卡诈骗罪的概念和犯罪构成

我国打击电子商务领域的信用卡诈骗犯罪的刑事法律条文主要是《刑法》第 287 条和第 196 条。《刑法》第 287 条关于“利用计算机实施金融诈骗……或者其他犯罪的，依照本法有关规定定罪处罚”的规定和《关于维护互联网安全的决定》，是认定利用电子商务领域的信用卡诈骗犯罪的法律前提，行为人在电子商务活动中实施信用卡诈骗犯罪的，依据我国《刑法》第 196 条信用卡诈骗罪定罪量刑。

信用卡诈骗罪，是指以非法占有为目的，利用信用卡进行诈骗活动，达到法定数额或者具有法定情节的行为。本罪分为基本罪和派生的重罪与极重罪三个构成类型。

（一）基本罪的构成要件

本罪的基本罪是结果犯，由一般主体、直接故意、选择危害行为、特殊犯罪结果、被害法益 5 个要件构成，它们的具体内容和形式分述如下：

1. 一般主体

本罪的主体是一般主体，指年满 16 周岁未满且具有刑事责任能力的人。单位不能构成本罪。

2. 直接故意

本罪在犯罪心态表现为故意，而且只能是直接故意。直接故意内容的一般犯罪目的是：明知自己进行信用卡诈骗会给他人财产和国家信用卡管理秩序造成严重危害，而故意实施这种行为并且希望危害结果发生的心理态度。间接故意和过失不构成本罪。除了以上一般犯罪目的外，还必须有特殊犯罪目的，即非法占有

他人资金。

3．选择性危害行为

行为人实施信用卡诈骗，具体表现为下列四种并列选择行为：(1) 用伪造的信用卡。指使用伪造的信用卡购买商品、在银行或自动柜员机上支取现金以及接受服务等。根据我国发行信用卡的各有关银行规定，申请信用卡的用户，都应在发卡银行设立相应的账户，并存入一定数额的信用卡起用金。使用伪造的信用卡，由于没有起用金，如果使用得逞，就使特约商户经济上受到直接损失。(2) 使用作废的信用卡。所谓使用作废的信用卡，是指使用因法定原因失去效用的信用卡。根据规定，作废的信用卡主要有三种情形：一是信用卡超过有效使用期限而自动失效。二是信用卡持卡人如果在信用卡有效期间内停止使用，应办理退卡手续并将该信用卡退回发卡机构，此时该信用卡虽未过有效期，但已办理退卡手续，故属作废的信用卡。三是因挂失而使信用卡失效。在一些信用卡管理不太完善和技术落后的地方，从银行传递信用卡挂失的申请到特约商户收到银行的止付令，常常需要较长的时间，这段时间差就成了不法分子的作案时间。由于持卡人已经挂失而特约商户又未接到银行命令，因而给发卡银行造成损失。(3) 冒用他人的信用卡。指行为人非法以持卡人的名义使用信用卡骗取财物或服务。如使用拾得的信用卡，使用代他人保管的信用卡，骗取他人信用卡并予以使用等。如果持卡人将本人信用卡借给亲朋好友使用，这是经持卡人同意的，虽然也是一种违规行为，但不构成本罪。(4) 恶意透支。信用卡的透支是指持卡人在其发卡银行信用卡账户上资金不足或已无资金的情况下，按信用卡章程、协议约定，持卡人可以在一定额度内使用信用卡进行消费，但须在约定时间补充资金并支付一定利息，这种透支叫善意透支。所谓恶意透支，是指持卡人以非法占有为目的，超过规定限额与期限透支，经发卡机构催还后仍不归还的行为。根据中国人民银行的规定，人民币信用卡透支的额度，个人普通卡为

1 000 元，单位普通卡为 5 000 元。善意透支和恶意透支的区别在于，前者是先用后还，在法定期限内还本付息，后者是以非法占有为目的，根本就不想归还透支的资金。

4. 特殊犯罪结果

本罪是结果犯，只有利用信用卡诈骗取得的财物达到数额较大程度，才构成犯罪。根据 1996 年 12 月 16 日最高人民法院《关于审理诈骗案件具体应用法律的若干问题的解释》（以下简称《解释》）规定，使用伪造的信用卡、使用作废的信用卡、冒用他人信用卡诈骗或恶意透支在 5000 元以上的，属于数额较大。在无新的司法解释时，可参照这一规定认定。如果数额不是较大，则不构成犯罪。

5. 被害法益

本罪的被害法益是复合的，即国家对信用卡的管理制度和他人的财产所有权。

（二）重罪的构成要件

本罪的重罪构成要件，是指罪行在符合基本罪构成要件的基础上，诈骗“数额巨大或者有其他严重情节”的行为。诈骗“数额巨大”和“其他严重情节”是构成重罪的两个选择要件，只要具备其中一项，重罪便可成立。根据前述司法解释规定，使用伪造的信用卡、使用作废的信用卡、冒用他人信用卡诈骗或恶意透支在 5 万元以上的，属于数额巨大。在无新的司法解释时，仍可适用这一规定。至于何为“其他严重情节”有待有权解释作出规定。

（三）极重罪的构成要件

本罪的极重罪构成要件，是指罪行在符合基本罪构成要件的基础上，诈骗“数额特别巨大或者有其他特别严重情节”，的行为。诈骗“数额特别巨大”和“其他特别严重情节”是构成极重罪的两个选择要件，只要具备其中一项，极重罪便可成立。根据前述司法解释规定，使用伪造的信用卡、使用作废的信用卡、冒

用他人信用卡诈骗或恶意透支在 20 万元以上的，属于数额特别巨大。在无新的司法解释时，仍可适用这一规定。至于何为“其他特别严重情节”，有待有权解释作出规定。

根据《刑法》第 196 条和第 287 条规定，利用计算机犯信用卡诈骗罪基本罪的，处 5 年以下有期徒刑或拘役，并处 2 万元以上 20 万元以下罚金；犯重罪的，处 5 年以上 10 年以下有期徒刑，并处 5 万元以上 50 万元以下罚金；犯极重罪的，处 10 年以上有期徒刑或无期徒刑，并处 5 万元以上 50 万元以下罚金或者没收财产。

四、对几类典型犯罪行为的审判处理意见

1. 窃取他人信用卡信息，伪造信用卡并使用的，如何处理？

前面曾提到窃取客户“易办事”信用卡磁条信息并伪造信用卡的案件。如果该案发生在我国内地应该如何处理？作者认为，如果该案发生在我国内地，行为人的以上行为属于共同犯罪。伪造信用卡属于伪造金融票证的行为，构成伪造金融票证罪；使用这些伪造的信用卡的行为属于信用卡诈骗行为，同时，给被害人造成了巨大经济损失，构成信用卡诈骗罪重罪，由于伪造信用卡和使用伪造信用卡的行为是方法行为和目的行为的关系，构成伪造金融票证罪和信用卡诈骗罪重罪的牵连犯，按“从一重罪处罚”的原则，按信用卡诈骗罪重罪定罪量刑。如果行为人伪造信用卡并使用，给被害人只造成数额较大的经济损失，构成伪造金融票证罪和信用卡诈骗罪基本罪的牵连犯，由于两罪法定刑相同，以目的行为所构成的犯罪，即按信用卡诈骗罪基本罪定罪量刑；如果行为人伪造并使用信用卡，数额达不到较大的标准的，只构成伪造金融票证罪。如果行为人伪造并使用信用卡，意图窃取数额较大的资金，由于意志以外的原因未得逞的，构成伪造金融票证罪和信用卡诈骗罪（未遂）的牵连犯，以伪造金融票证罪定罪量刑。如果特约商户只窃取他人信用卡信息，而没有参与伪

造信用卡和使用信用卡诈骗的，按照我国共同犯罪理论，属于前述犯罪的从犯，按前述罪名定罪，按从犯量刑。如果特约商户参与伪造和使用信用卡诈骗的行为的，构成前述犯罪的实行犯，以所参与的全部犯罪定罪量刑。

2. 虚设信用卡信息，伪造信用卡并使用或者使用虚设信用卡账户的，如何处理？

在前面提到曾某破译信用卡加密密钥，虚设信用卡信息，伪造信用卡并使用的案件中，曾某的破译行为属于非法行为，如不构成犯罪。但其伪造信用卡并使用的，则构成伪造金融票证罪和信用卡诈骗罪的牵连犯，按“从一重罪处罚”原则定罪量刑。

有些信用卡如中国银行的长城卡具有网上支付功能，如果行为人破译的是这种信用卡加密密钥，虚设该种信用卡账户，并在电子商务中进行网上消费或者转账的，该如何处理？我国《刑法》第177条规定的伪造金融票证罪和第196条规定的信用卡诈骗罪的行为对象都是信用卡，司法解释也没有规定将虚增信用卡账户、使用虚增的信用卡账户的行为，视同伪造信用卡和使用伪造的信用卡的行为，根据《刑法》第3条规定“法律没有明文规定为犯罪行为的，不得定罪处刑”，以上行为不构成犯罪。

作者认为，信用卡的核心和本质部分是存储在信用卡磁条或者IC卡芯片中的信用卡账户等信息，信用卡卡片本身价值微不足道，其真正价值是用户的商业信用和信用卡账户中存储的资金。用户使用信用卡，无论是通过使用信用卡卡片，或者是使用信用卡账户密码，二者都要由相应设备验证信用卡账户等信息的合法性，而后才能享用金融机构提供的信用服务，因此，伪造信用卡和虚增信用卡账户在其本质上是相同的，都是利用一定的技术手段，骗取金融机构的信用服务，而只是在使用的技术手段上有所差别，同样，使用虚增信用卡账户和使用伪造信用卡也是如此。两种行为的目的、本质完全相同，而只是犯罪手段有所差异，何以就存在罪与非罪的本质差别呢？明显地，这是由于我国

刑法立法机关和司法解释机关没有充分考虑电子商务发展的现状，法条设计疏漏，导致刑事立法的滞后。

3. 银行内部人员利用职务之便，伪造与客户信用卡信息相同的信用卡并使用的，如何处理？

在发卡机构和信用卡用户之间关于信用卡的合约中，一般都规定了信用卡使用中发卡机构的免责条款，即由于信用卡用户自身原因和不可抗力原因所造成的经济损失，发卡机构概不负责。但发卡银行内部人员利用职务便利，伪造与客户信用卡信息相同的信用卡并使用的，造成的经济损失由银行负责，因为行为人侵犯了银行的财产权，同时也侵犯了国家对信用卡的管理秩序。如果造成的经济损失较大的，构成刑法理论中的职务侵占罪和信用卡诈骗罪的想象竞合，按其中的重罪定罪量刑，即按职务侵占罪定罪量刑。

4. 非法窃取他人信用卡账户密码，用于网上消费或者转账的，如何处理？

前面曾提到意大利黑客窃取并使用网上支付信用卡信息的案件和我国重庆发生的窥视他人网上支付信用卡账户密码并用于网上消费的案件，对这类犯罪应该如何处理？窥探他人网上支付信用卡账户密码，并用于网上消费，虽然在行为性质上与盗窃信用卡并进行使用的行为相似，但是由于我国刑法和相关司法解释对这种行为没有明确规定，因此，对这种行为不能以犯罪论处。意大利黑客案件如果发生在我国，也只能以侵犯商业秘密罪追究其刑事责任，而不能构成盗窃罪或者信用卡诈骗罪。刑法没有把窃用他人信用卡账号密码的行为规定为犯罪，这一疏漏使惩治这种严重危害行为处于无法可依的尴尬境地。

五、电子商务领域信用卡诈骗罪的犯罪形态问题

行为人使用伪造的信用卡或者冒用他人信用卡，一般是用于取款、购物或转账。在实施取款和购物行为时，可能发生两种结

果，一种是行为人实际取得钱款或者货物，由于电子商务中业务处理几乎完全由计算机完成，行为人实施以上行为大多数即时完成，即取得钱款或者购物交易完成（包括先付款后送货）；另一种是行为人在实施以上行为时被发觉而无法完成交易，如使用的伪造信用卡被“吞卡”，购物交易被发觉非法而被拒绝等。在实施转账行为时，也可能发生两种情况，即成功实施转账和转账不成功，前者还可能有行为人消费了转入账户中的资金和没有消费两种情况。以上行为的不同状况可能引起本罪处理的不同结果。

信用卡诈骗罪的基本罪是结果犯，行为人必须诈骗了法定数额的他人财物，否则不能构成本罪。被诈骗的法定数额的他人财物，是以被害人失去控制的财物数额为准，还是以行为人诈骗所得的财物为准，对此存在不同看法。在实践中，这个问题对于传统的信用卡诈骗犯罪是不存在的，行为人进行信用卡诈骗一般是用于提款，被害人所失去控制的财物就是行为人控制的财物数量，两者数额是相同的。而在电子商务时代，行为人实施信用卡诈骗的方式有多种，网上消费和网上转账等新的行为方式使以上两者不再统一。以网上消费为例，行为人使用伪造的信用卡或者冒用他人信用卡购买货物，交易成功后，货物要迟一段时间才能送达行为人手中，如果行为人在得到货物前被发觉和逮捕，那么，行为人根本得不到该货物。在这种情况下，以两者中哪一种财物数额为标准，就影响到本罪能否成立。作者认为，信用卡诈骗罪侵犯的法益是复合的，即国家信用卡管理制度和他人的财产所有权，前者是主要被侵犯的法益，因此，判断本罪成立与否必须首先考虑国家信用卡管理制度被侵犯的程度，即以因行为人行为导致的财物变动的数额，也就是以被害人失去控制的财物数额为准，来确定是否满足本罪的法定数额。达到基本罪法定数额的，构成本罪基本罪既遂，否则不构成本罪，本罪基本罪无未遂犯、预备犯和中止犯。

电子商务给本罪带来的另一个问题是，金融电子化系统账户

中资金记录，或称电子货币能否成为本罪中的“财物”？电子商务时代电子货币得到广泛应用，大量的信用卡诈骗犯罪都与电子货币相关，如利用信用卡网上购物、网上转账等。如果不把电子货币作为本罪中的“财物”的一种形式，那么，即使行为人给社会及被害人造成再大的损害，也不能构成犯罪，从而导致放纵犯罪，使犯罪人逍遥法外。实际上，刑法中“财物”概念随时代的发展不断扩展范围，在电子商务时代，电子货币成为日益广泛应用的社会财富的一种，大量的社会活动中使用电子货币，已是不争的事实，确认电子货币是本罪“财物”的一种形式，符合刑法现代化发展的趋势，也必将为刑法立法所采纳。因此，行为人将被害人信用卡账户中的电子货币转入其他账户中，即使他没有消费或者继续转移转入账户中的资金，也可以认为行为人给被害人造成了财物的损失，如果该损失达到基本罪法定数额的，构成本罪基本罪既遂。

本罪的重罪和极重罪是选择加重犯，即诈骗财物数额达到重罪或极重罪的法定数额，或者有其他严重或特别严重情节的，都可以构成本罪的重罪或者极重罪。行为人意图诈骗达到重罪或极重罪的法定数额的他人财物，由于意志以外的原因而未能得逞的，如取款、网上购物或者转账被拒绝等，此种情况因行为人的行为已经对国家信用卡管理制度构成严重的现实的威胁，并且行为人表现出严重的人身危险性，因此，应当认为其行为具有严重的社会危害性，即本罪的重罪和极重罪有未遂犯。至于行为人预备实施本罪重罪和极重罪的，由于其尚未对国家信用卡管理制度构成现实的威胁，行为人的人身危险性也没有充分表露，应当认为其行为社会危害性显著轻微，不构成犯罪，即本罪重罪和极重罪无预备犯。但是，根据其预备行为的不同，可能构成伪造信用卡罪等其他犯罪。实施信用卡诈骗行为，能够完成犯罪而自动中止的，比如行为人着手实施诈骗行为但未达到本罪基本罪法定数额的，行为人自动将资金归还被害人的，应当认为行为人构成犯

罪中止，即本罪重罪和极重罪有中止犯。

六、对电子商务领域信用卡诈骗罪的立法建议

《刑法》第196条规定了信用卡诈骗罪的四种行为方式，并规定“盗窃信用卡并使用的”，依照盗窃罪定罪处罚，我认为，该条需要进行以下修改：

1. 信用卡诈骗行为不应限于“持卡”方式

前面提到曾某虚设信用卡信息伪造信用卡并使用的案件。如果行为人非法设置可用于网上消费的信用卡账户，并进行网上消费或者转账的，该如何处理？根据我国《刑法》第196条的规定，信用卡诈骗罪的行为对象必须是信用卡，司法解释也没有规定使用非法设置的信用卡账户的行为视同使用伪造的信用卡，以上行为不具备信用卡诈骗罪的犯罪构成，不构成信用卡诈骗罪。同时，刑法其他罪名也不能适用于这种行为，根据我国《刑法》第3条规定“法律没有明文规定为犯罪行为的，不得定罪处刑”，这种行为不构成犯罪。很明显，这种立法状况放纵了此类犯罪行为。

信用卡的核心是存储在信用卡磁条或者IC卡芯片中的信用卡账户等信息，信用卡卡片本身价值微不足道，其本质是用户的商业信用。用户使用信用卡，无论是通过使用信用卡卡片，或者是使用信用卡账户密码，都是用户商业信用的使用，在应用环节上都要由相关人员或者设备验证信用信息的真实性、合法性后，才能享用金融机构提供的信用服务。因此，使用非法设置的信用卡账户和使用伪造信用卡本质是相同的，都是利用一定的技术手段，骗取金融机构的信用服务，而只是在具体使用的技术手段上有所差别。两种行为的目的、本质完全相同，而只是犯罪手段有所差异，何以就存在罪与非罪的差别呢？这种立法上不应有的区别，是由法律的滞后所造成的。同样地，冒用他人信用卡账户密码，与冒用他人信用卡也只在使用方法上有区别，其实质是相同

的，而在刑法处遇上有与上面类似的情况。在实际生活中，使用“无卡”方式的信用卡诈骗犯罪发案率日益升高，造成的危害日益严重，如果不及时修订刑法，对其予以恰当的处理，将严重损害社会合法利益。

另外，有的网络金融结算系统如电子钱包，为了保护用户信用卡信息的安全，给每一位用户的信用卡设置了一个特殊的号码如 PIN 号码，用户使用 PIN 号码和密码进行电子商务，而避免信用卡信息被恶意的电子商务商户窃取和使用。这种措施虽然增强了用户信用卡信息的保密性，但这种 PIN 号码密码本身也可能被冒用或者被虚设使用，因此，冒用用户 PIN 号码密码及使用虚设 PIN 号码的，也应视做信用卡诈骗行为。

基于以上观点，我建议《刑法》第 196 条增补一款，“使用信用卡账户密码，或者使用由信用卡账户密码合法产生的信用信息的，等同使用信用卡”。

2. 盗窃他人信用卡并使用的，不应构成盗窃罪，而应构成信用卡诈骗罪

《刑法》第 196 条第 3 款规定，“盗窃信用卡并使用的，依照本法第 264 条的规定定罪处罚”，即以盗窃罪定罪量刑。关于该款的规定，刑法理论界存在肯定与否定两种不同观点，肯定的观点中，有的认为这种情况属于牵连犯，按从一重罪即盗窃罪处罚①；有的认为盗窃行为是主行为，诈骗行为是盗窃行为的继续，属于从行为，主行为吸收从行为，故按盗窃罪论处②；还有的学者把盗用信用卡等同于盗窃使用印鉴齐全的支票③。否定的

① 王作富主编《刑法》，中国人民大学出版社 1999 年版，第 319 页。

② 陈明华主编：《刑法学》，中国政法大学出版社 1999 年版，第 508 页。

③ 陈兴良主编：《刑法新罪评释全书》，中国民主与法制出版社 1995 年版，第 531 页。

观点中，有的认为盗用信用卡的行为中，信用卡诈骗行为是主行为，盗窃是辅行为，按照牵连犯的理论，应当定信用卡诈骗罪①；有的认为，盗用信用卡的行为中，根本不能成立盗窃罪，因此不存在盗窃罪和信用卡诈骗罪的牵连犯问题②。

我认为，虽然刑法对这种行为有明文规定，而且司法解释规定，“盗窃数额应当根据行为人盗窃信用卡后使用的数额认定”，但是这种规定与立法精神和刑法基本理论相去甚远：

（1）行为人盗窃他人信用卡并使用的，实际是盗窃信用卡和冒用他人信用卡两个行为，由于信用卡卡片本身的价值不大，单有盗窃信用卡的行为，根本不能构成犯罪，它只是冒用信用卡的预备行为，当后者构成犯罪时，后者将前者吸收，以信用卡诈骗罪定罪量刑。

（2）行为人盗窃信用卡并使用的，不仅侵犯公私财物的所有权，还侵犯了国家对信用卡的管理秩序，将这类行为规定为盗窃罪，明显没有正确反映被害法益的实际情况。而且，行为人非法获取他人财物，最终是使用他人信用卡后才能实现，把盗窃和使用两个行为概括为一个盗窃行为，不符合行为方面的实际情况。同时，信用卡诈骗罪除了没有盗窃罪的最重罪外，其他对应的法定刑都比盗窃罪重，以盗窃罪定罪量刑轻纵了犯罪。

（3）前面曾论证，盗窃他人信用卡并使用的行为，与偷窥他人信用卡账户密码并直接使用的，应当同样对待。依《刑法》第196条第3款的规定，后者也应定盗窃罪。但是，后者只有侵犯个人数据的违法行为和使用该个人数据的行为，根本没有盗窃信用卡的行为，整个行为与盗窃行为迥然不同，把这种行为定为盗

① 单长宗等编：《新刑法研究与适用》，人民法院出版社2000年版，第427页。

② 刘明祥著：《财产罪比较研究》，中国政法大学出版社2000年版，第259页。

窃罪显然不妥。

基于以上理由，盗窃信用卡并使用的，其性质仍然是利用信用卡诈骗，不宜定盗窃罪，建议删除《刑法》第 196 条第 3 款的规定。

第三节　电子商务领域的侵犯著作权罪

一、电子商务领域侵犯著作权犯罪发展现状

计算机、网络技术应用在文化领域，首先表现为创造出了多种新作品，有绚丽多彩、构思奇特的网页，有“网虫爬格子”留下的网络文章，有功能强大的计算机软件和游戏软件等等。其次为传统文化提供了新的表现形式和传播方式，作品表现形式不再是单一的某种媒体形式如文字或图片，而是以多媒体形式展现在用户面前，互联网络成为承载文化作品的第四种媒体，能将数字化作品在一瞬间传遍全球，用户获取这些文化作品不再是被动地接受，而是主动地选择，实现个人化的文化传播。总之，计算机、网络技术的广泛应用促成了人类文化领域的一次革命。

这次文化领域的革命使各种作品大量涌现，使电子商务文化市场迅速发展起来，但同时，电子商务领域侵犯著作权犯罪也日益严重，主要有以下几种形式：

1. 商业网站提供免费下载他人版权软件服务

一些商业网站为吸引网络用户访问，设立软件免费下载服务，合法经营的商业网站一般只提供免费软件或者共享软件，而一些急于提升网站知名度的商业网站不惜侵犯他人版权，将他人享用产权的软件向网上免费提供，如香港的网上盗版软件案。香港海关曾接到“香港商业软件联会”的投诉，称他们在互联网上发现有人盗用版权作非法商业用途，向外界提供的软件包括 Windows 2000，以及中文桌面出版系统等 8 种计算机软件，供人

在网上免费下载，藉此提高网站浏览人次，从中收取广告费牟利①。

2．盗版软件公司通过电子邮件倾销盗版软件

网上销售软件具有便捷、实惠等特点，深受计算机软件用户欢迎。但这种途径也成为盗版软件的单位“发财致富”的捷径，他们常常以广播式电子邮件的方式向网络用户寄送软件价格目录，以低廉的价格销售盗版软件。这种行为在互联网络上极为普遍，根据商业软件联盟的统计，大约有 84 万个网站在销售盗版软件，这种行为令软件公司深受其害。

3．商业网站提供 MP3 音乐免费下载

网上销售音乐作品并不是新鲜事情，但 MP3 技术的出现使音乐作品可以直接在网上销售。MP3 是最近开发的一种文件格式，可用来紧密压缩音乐文件，而又不失去音乐的质量，压缩后的文件很小，易于发行。该格式没有任何内在的版权保护措施，而且使用的解码器很容易从网上下载。一些商业网站为提高网站知名度，将他人有著作权的音乐作品压缩成 MP3 形式并提供免费下载，这类犯罪在世界各国都十分严重。

4．商业网站抄袭他人网页

商业网站的网页有如公司的门面和产品，商业网站网页设计制作的好坏直接影响网站的经营效益，一个好的网页需要相当的创造力并花费相当的人力、物力。信息社会中网页经济价值不菲，设计制作不易，而复制剽窃却非常容易，稍有技术力量的网络公司都可以轻松剽窃。近年来商业网站抄袭、剽窃他人网页的案件屡屡发生，例如创联诉汇盟网页抄袭案。1999 年 7 月不少网民发现，北京汇盟国际商务咨询有限公司（以下简称汇盟公司）和北京创联通信网络有限公司（以下简称创联公司）的网页

① 王蓬：《香港海关首次破获网上盗版集团》，《检察日报》，2000 年 4 月 26 日。

竟然一模一样，特别奇怪的是，汇盟公司的网页中却有创联公司的企业名称、创联公司的服务器名称和联系代号，两家都是以提供网络服务为主的企业，业务范围基本相同。1999 年 9 月，创联公司向北京市海淀区法院提起诉讼，指控汇盟公司通过恶意抄袭其网页及广告进行不正当竞争，创联公司在诉讼中称，汇盟公司从 1999 年 5 月 8 日起，一直抄袭创联公司的广告创意和设计①。

5. 商业媒体侵犯文字作品著作权

互联网络已经成为事实上的“第四种媒体”，商业网站上提供的新闻信息、专题文章等，是吸引网络用户依恋网站的重要原因，各大商业网站无不极力“笼络”新奇、有创见、能够吸引读者的文章，传统报刊媒体也不示弱，也积极寻找网络空间中有价值的作品，在媒体之间激烈的竞争中，侵犯他人文字作品著作权的行为不断发生。目前，电子商务中侵犯文字作品著作权的行为主要有以下三种形式：其一是将传统介质形式的文字作品上载到网站；其二是网站之间互载，即网站之间内容复制、转载；其三是将网上的作品下载到其他媒体上发表。例如《电脑商情报》侵犯著作权案，陈卫华以“无方”为笔名撰写的《戏说 MAYA》一文刊载于个人网页《3D 芝麻街》上，并注明“版权所有，请勿转载”，但成都《电脑商情报》却未经陈卫华同意刊登了这篇文章。

6. 计算机软件的非法破密

面对计算机软件盗版问题的严重局面，各计算机软件生产厂家都对自己的产品设置安全措施，如加密、逻辑锁、序列号等等。盗版侵权人为进行盗版就必须首先破解安全措施，于是破解计算机软件措施就成为社会上某些非法组织的专业市场，这些人有些自己不直接销售盗版软件，但向专业盗版组织出售已破密的计算机软件来牟取暴利。世界盗版软件犯罪严重的状况与这些人

① 唐旬：《网上行需要立规矩》，《光明日报》，1999 年 10 月 27 日。

的非法破密行为有密切关系。

为打击电子商务领域侵犯著作权犯罪，世界各国纷纷制定法律。美国 1997 年通过了禁止电子盗窃法，该法律规定非营利性散布他人著作权作品的行为可能构成犯罪，任何人只要分发价值超过 2 500 美元的 10 件或 10 件以上拥有版权的作品，都可能被判监禁长达三年和罚款多达 25 万美元；德国巴伐利亚州地方法院曾裁定，从互联网上复制音乐为非法行为，提供音乐复制操作功能的网络服务公司将受处罚；加拿大议会对联邦复制权法进行了修改，对非法复制计算机软件的案犯最高可处以 2 万加元的罚款；1998 年 1 月日本新版权法生效，以打击借助 MP3 进行音乐盗版等活动。

二、侵犯著作权罪的概念和犯罪构成

我国打击电子商务领域侵犯著作权犯罪的刑事法律条文主要是《刑法》第 287 条和第 217 条。《刑法》第 287 条关于“利用计算机实施金融诈骗……或者其他犯罪的，依照本法有关规定定罪处罚”的规定和《关于维护互联网安全的决定》，是认定利用电子商务领域侵犯著作权犯罪的法律前提，行为人在电子商务活动中实施侵犯著作权犯罪的，依据我国《刑法》第 217 条侵犯著作权罪定罪量刑。

侵犯著作权罪，是指以营利为目的，未经著作权人或与著作权有关的权益人许可，复制发行其作品，出版他人享有专有出版权的图书，未经录音录像制作者许可复制发行其制作的音像制品，或者制售假冒他人署名的美术作品，违法所得达到法定数额，或者具有法定情节的行为。本罪分为基本罪和派生的重罪两个构成类型。

（一）基本罪的构成要件

本罪的基本罪由选择主体、直接故意、复杂危害行为、特殊犯罪时间、特殊犯罪后果、特殊犯罪对象和被害法益 7 个要件构

成，它们的具体内容和形式分述如下：

1．选择主体

本罪的犯罪主体是选择主体，即年满 16 周岁且具有刑事责任能力的人或者一般单位。

2．直接故意

本罪的犯罪心态表现为故意，而且只能是直接故意。直接故意内容的一般犯罪目的是：明知自己实施侵犯他人著作权，而故意实施这种行为并希望危害结果发生的心理态度。间接故意和过失不构成本罪。本罪除了以上一般犯罪目的外，还必须有特殊犯罪目的，即具有营利的目的。

3．复杂危害行为

侵犯著作权的行为，有如下四种并列选择的行为方式：（1）未经著作权人许可，复制发行其文字作品、音乐、电影、电视、录像作品、计算机软件及其他作品。所谓复制，是指采取印刷、临摹、复印、拓片、翻录、翻拍、拷贝等方法，将他人作品制作一份或多份的行为；所谓发行，是指将非法复制的他人作品以批发、零售、出租等方式向社会传播的行为。复制和发行两种行为必须同时具备才能成立本罪。（2）出版他人享有专有出版权的图书。所谓图书专有出版权，指图书出版者根据与著作权人签订的图书出版专有合同，对著作权人交付出版的作品在合同指定的时间和地区内通过原版、修订版方式以图书形式出版的独占权利。（3）未经录音、录像制作者的许可，复制发行其制作的录音、录像。根据著作权法的规定，录音、录像的制作者对其作品，享有许可他人复制发行并获得报酬的权利，该权利的保护期为 50 年。这就确认了录音、录像作者对其作品在保护期限内的专有出版权。（4）制作、出售假冒他人署名的美术作品。这种行为又包括三种具体形式：一是以临摹的方法，临摹他人的美术作品，然后署上他人的姓名，假冒他人的作品出售，牟取非法利益。二是以自己的美术作品，署上他人的姓名，假冒他人作品出售牟利。通

常是署上名画家、名雕塑家等美术界知名作者的姓名，以提高作品的价值。三是在他人的美术作品上，署上名家的姓名，然后假冒名家的作品出售牟利。所谓美术作品，既指绘画，也包括书法、雕塑、建筑、工艺美术等艺术作品。由于法律对制作、复制等侵权行为的具体方法、手段未作特别限制，因而利用计算机也可以实施上述各种危害行为。

在电子商务领域，以上四种行为都可能发生，只是在方法、手段、经历的过程上有较大差异，行为人既可以把传统的实物介质作品数字化后，在互联网络环境中传播他人的版权作品，也可以把网络上的数字化作品依着在实物介质上，在传统流通环境中传播。与传统的侵犯著作权犯罪的行为方式所不同的是，电子商务领域侵犯著作权犯罪的行为不仅有单纯地由行为人向使用者提供的方式，也即“推”方式，还有“使用者请求 + 行为人提供”的所谓“拉推”方式。以采取文件下载方式传播作品为例，使用者要获取目标作品，首先要点击网站网页上的链接，这种链接下隐藏着下载目标作品文件的命令，该命令送达网站服务器后，网站服务器根据命令向使用者的计算机发送目标作品文件。

4. 特殊犯罪时间

本罪的特殊犯罪时间是著作权有效保护期限内，如果行为发生在著作权保护期以后，不构成本罪。根据《著作权法》规定：(1) 作者的署名权、修改权、保护作品完整权的保护期不受限制。(2) 公民的作品，其发表权、使用权和获得报酬权的保护期为作者终身及其死亡后 50 年，截止于作者死亡后第五十年的 12 月 31 日；如果是合作作品，截止于最后死亡的作者死亡后第五十年的 12 月 31 日。(3) 法人或者非法人单位的作品的著作权（署名权除外）由法人或者非法人单位享有的职务作品，其发表权、使用权和获得报酬权的保护期为 50 年，截止于作品首次发表后第五十年的 12 月 31 日，但其作品自创作完成后 50 年内未发表的，著作权法不再保护。(4) 电影、电视、录像和摄影作品

的发表权、使用权和获得报酬权的保护期为 50 年，截止于作品首次发表后第五十年的 12 月 31 日，但作品自创作完成后 50 年内未发表的，著作权法不再保护。

5. 特殊犯罪后果

本罪是结果犯，构成本罪必须是违法所得数额较大或者有其他严重情节。所谓数额较大，根据最高人民法院 1998 年 12 月 11 日发布的《关于审理非法出版物刑事案件具体应用法律若干问题的解释》，是指个人违法所得在 5 万元以上 20 万元以下，单位违法所得数额在 20 万元以上 100 万元以下。所谓其他严重情节，是指有下列三种情况：(1) 因侵犯著作权曾经两次以上被追究行政责任或者民事责任，两年内又实施前述侵犯著作权行为之一的；(2) 个人非法经营数额在 20 万元以上，单位非法经营数额在 100 万元以上的；(3) 造成其他严重后果的。

6. 特殊犯罪对象

本罪的犯罪对象是他人依法享有著作权的作品。

7. 被害法益

本罪的被害法益是他人的著作权和与著作权相关的权益。所谓著作权，指公民依法对文学、艺术和科学作品所享有的各种权利的总称。其中包括著作人身权和著作财产权。人身权指作者对其作品依法享有的发表权、署名权、修改权和保护作品完整权；著作财产权主要指使用作品的权利和获得报酬的权利以及许可他人使用作品并由此获得报酬的权利。所谓与著作有关的权益，指传播作品的人对他赋予作品的传播形式所享有的权利，也即著作邻接权。包括出版者、表演者、电台、电视台和录音录像者的权利。

(二) 重罪的构成要件

本罪的重罪构成要件，是指罪行在符合基本罪构成要件的基础上，违法所得数额巨大或有其他特别严重的犯罪情节的行为。根据前述司法解释，所谓违法所得数额巨大，指个人违法所得数额在 20 万元以上，单位违法所得数额在 100 万元以上。所谓有

其他特别严重情节，指具有下列情形之一：(1) 个人非法经营数额在 100 万元以上，单位非法经营数额在 500 万元以上的；(2) 造成其他特别严重后果的。

根据《刑法》第 287 条、第 217 条和第 220 条规定，利用计算机犯本罪基本罪的，处 3 年以下有期徒刑或者拘役，并处或者单处罚金；犯重罪的，处 3 年以上 7 年以下有期徒刑，并处罚金。单位犯本罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照个人犯本罪的规定处罚。

三、对几类典型犯罪行为的审判处理意见

1. 商业网站利用邮件方式销售侵权计算机软件、MP3 音乐的，如何处理？

商业网站利用邮件方式联络网络用户、销售侵权作品，包含了复制和销售侵权作品两种行为，因此不构成《刑法》第 218 条规定的销售侵权复制品罪的危害行为，而构成本罪的危害行为。并且，商业网站明显具有营利目的，如果其行为非法所得数额较大或者有其他严重情节，可能构成侵犯著作权罪。

2. 商业网站未经著作权人同意，在网站上刊登其文字作品的，如何处理？

1999 年我国曾发生六位著名作家诉网站侵权案，诸如此类的商业网站侵犯文字作品著作权的行为在互联网络信息提供业界经常发生，对于其中危害严重的，应该如何处理？当网络用户访问该网站点击相关链接时，商业网站的网络服务器根据用户请求，将侵权文字作品的复制件传送到用户计算机上，网络服务器的这种复制发送行为，不仅是商业网站经营人所认识的，而且是其经过技术设备方面的努力所希望达到的，当然应由商业网站经营者承担责任，因此，可以认定商业网站经营者有复制发行侵权作品的行为。此外，由于商业网站刊载侵权作品的行为能够提高网站的知名度，故可以认定存在营利目的。如果因侵犯著作权被

追究行政或者民事责任两次以上，或者有其他严重后果的，可能构成侵犯著作权罪。

3．商业网站提供免费计算机软件、MP3 音乐下载能否构成本罪？

商业网站的这种行为是为具有营利目的？商业网站提供计算机软件、MP3 音乐等侵权作品免费下载，其目的是为了扩大商业网站的影响，提高网站知名度，因此，提供免费下载行为实质是一种类似广告宣传、招揽顾客的行为，有利于商业网站经营。因此，虽然商业网站免费提供他人作品看似没有营利，但实质上仍然具有商业营利的目的。

商业网站的行为是否为复制发行侵犯著作权作品的行为？商业网站提供计算机软件和 MP3 音乐等侵权作品免费下载，主要有两种方式：其一是直接在自己的网站上存储侵权作品并提供下载服务；其二是虽然自己的网站上没有放置侵权作品，但是通过超链接（Hyperlink）指向其他提供免费下载的网站。文件下载具有这样的特点，服务器根据用户下载请求命令，将目标文件的复制件传送给用户，这种与前面情况相同，可以认为文件下载服务器的权利人有复制发行侵权作品的行为。第二种的情况则必须进一步分析，它可以再分为两种情况：(1) 如果链接指向的是其他商业网站（简称被动方），该网站有前述第一种情况的，被动方可能构成侵犯著作权罪。这是因为，对于被动方而言，他人在自己的网页上建立指向被动方的链接的行为，被动方可能预见，但不能确切地认识，建立链接者则对被动方及自己的行为有确切的认识，其行为符合我国刑法理论中的片面帮助犯的构成要件，应按侵犯著作权罪的从犯论处。(2) 如果链接指向的不是商业网站，而是非营利性的网站（以下简称网站），网站传播他人版权作品的行为，无论造成何种严重后果，由于缺乏营利目的，不能构成侵犯著作权罪，只是一般违法行为。该建立链接者的行为符合我国刑法理论中的间接正犯的特征，如果满足其他构成要件，

可以构成侵犯著作权罪。

如何认定商业网站的免费下载侵权作品的危害后果？行为人构成侵犯著作权罪的基本罪，必须非法所得数额较大，或者有其他严重情节。由于计算商业网站非法所得比较困难，可以根据其严重情节予以认定，即：(1) 因侵犯著作权曾经两次以上被追究行政责任或者民事责任，两年内又实施前述侵犯著作权的行为之一的；(2) 个人非法经营数额在 20 万元以上，单位非法经营数额在 100 万元以上的；(3) 造成其他严重后果的。这里的“非法经营数额”应当以免费提供的所有侵权作品的市价总额计算。

由于本罪规定了单位犯罪，所以商业网站从事免费下载侵权作品，数额较大或者有其他严重情节的，构成侵犯著作权罪。

四、对电子商务领域侵犯著作权罪的立法建议

在以纸张等有形介质承载作品的时代，侵犯著作权犯罪都具有营利目的，这是因为实施侵权行为需要付出成本，而且侵害越严重，成本就越大。但是在信息时代，借助于计算机、网络技术，复制他人的作品变得简单、便利，所耗成本极低，这样不以营利为目的的侵犯著作权行为大量衍生起来。为吸引网络用户光顾商业网站，许多商业网站提供了免费的虚拟主机服务，个人可以免费建立个人主页并在个人主页上刊登、发布各种信息，有些人为了吸引网络用户对其网页的关注，在个人主页上发布盗版软件。由于网络联系十分广泛，网络用户数量庞大，可能有成千上万套的盗版软件被分发出去，给著作权人造成严重损害。而依据我国《刑法》第 217 条规定，只有以营利为目的，侵犯他人著作权违法所得数额较大，或者有其他严重情节的，才构成侵犯著作权罪，如果行为人不以营利为目的，即使给权利人和社会造成的危害再大，也不能构成本罪，不能予以刑事处罚。显然，这与当今时代要求不符，是我国打击侵犯著作权犯罪刑事立法的严重缺陷，不利于电子商务领域著作权的有效保护。

作者认为应当借鉴美国等国家的立法经验。美国《禁止电子盗窃法案》（No Electronic Theft Act）将营利性和非营利性的复制发行侵权作品的行为都规定为犯罪，并规定了不同的刑罚。针对非营利性的犯罪，每件作品被复制、传播 10 件/次以上，零售价值达 2 500 美元以上的，判处 3 年以下监禁或罚金，或两者并处；如果是累犯或连续犯，判处 6 年以下监禁或罚金，或两者并处；对每件作品复制、传播 1 件/次以上，零售价值在 1 000 美元以下的，判 1 年以下监禁或罚金，或两者并处。1999 年 8 月美国一位在互联网上向他人免费赠送音乐、电影和软件的学生杰弗里·杰勒德·利维，成为根据该法被认定犯有重罪的第一人，利维承认，他在 1999 年 1 月曾在互联网上非法提供电脑软件程序、音乐录音、娱乐软件和数码录制的电影，使一般公众得以下载和复制这些拥有版权的产品，同时，没有任何证据说明利维通过这些免费提供的作品赚取任何利润。

综上，应修改《刑法》第 217 条，对非营利性侵犯著作权，情节严重的，定罪处罚。具体罪状表述为：有下列侵犯著作权情形之一，以营利为目的，违法所得数额较大或者有其他严重情节的，处 3 年以下有期徒刑或者拘役，并处或者单处罚金，不以营利为目的，情节严重的，处 2 年以下有期徒刑或者拘役，并处或者单处罚金；以营利为目的，违法所得数额巨大或者有其他特别严重情节的，处 3 年以上 7 年以下有期徒刑或者拘役，并处罚金，不以营利为目的，情节特别严重的，处 3 年以上 5 年以下有期徒刑或者拘役，并处罚金……

第四节　电子商务领域的侵犯商业秘密罪

一、电子商务领域的侵犯商业秘密犯罪的发展现状

为提高工作效率、增强企业竞争力，现代企业特别是电子商

务企业普遍使用计算机、网络技术进行生产经营管理。这些企业的计算机信息系统中存储、处理、传输着大量商业秘密，如用户数据库、处于开发阶段的计算机软件、企业经营战略、商务来往信息等。在市场经济条件下，商业秘密意味着利益和财富，商业秘密信息一旦被他人非法获取、披露或使用，就会给商业秘密的权利人造成重大损失。计算机、网络技术应用在提供有效管理商业秘密手段的同时，也给不法分子创造了新的犯罪方法。20 世纪 80 年代以来，侵犯商业秘密犯罪成为世界各国普遍的经济犯罪，给权利人带来了难以估量的经济损失。据美国马里兰商业管理中心估计，由于侵犯商业秘密犯罪，美国每年蒙受的经济损失高达 500 亿美元以上①。而美国也一直在窃取他国商业秘密，UKUSA 联盟（由英国、美国、加拿大、澳大利亚和新西兰组成）一直在利用其遍布全球的间谍网络来截获商业公司的大量商业机密，并将窃取的内容交给这些公司的竞争对手②。实际上，冷战结束后，各国遍布全球的谍报网的工作重心由政治、军事领域转到经济领域，尤其是新兴的电子商务领域。据德国巴符州宪法保卫局反间谍处负责人沃尔透露，1998 年他们处理的数百起涉外间谍案件中，经济和科技间谍案高达 62%，政治和军事间谍案只占 38%③。不仅国家间侵犯商业秘密事件愈演愈烈，国家内企业间侵犯商业秘密犯罪也越来越严重，这一状况在信息化程度高、利润更丰厚的电子商务领域表现得更加突出。电子商务领域侵犯商业秘密犯罪主要有以下几种表现形式：

---

① 高铭暄、赵秉志主编：《刑法论丛》第 2 卷，法律出版社 1999 年版，第 60 页。

② 《美国动用一切技术手段 从互联网上大肆获取商业机密》，《电脑日报》，1999 年 5 月 26 日。

③ 方祥生：《西方国家间经济间谍战愈演愈烈》，《光明日报》，1999 年 3 月 2 日。

1. 截取电子邮件，从中获取商业秘密

电子邮件是电子商务活动中一种快捷、廉价的信息交换手段，许多电子商务企业利用电子邮件联系客户、传递购销合同或进行其他商务活动，同时这种通信方式很容易遭到犯罪分子的侵犯，行为人一旦得到电子邮件邮箱的用户名及密码，就能窃取他人的电子邮件。1999 年乐清市某厂经理余某发觉商务电子邮件全部丢失，经警方调查发现，为该企业电脑操作员章某利用工作之便，从本厂的电子邮件信箱中探悉一俄罗斯客户欲与公司进行大宗电器产品贸易后，与其朋友李晓峰谋划将该商业秘密窃归己有。章、李二人经过周密策划，在公司电脑上另设了自己的电子邮件信箱，并通过改变传送路径等手段，将公司所有商业贸易往来的电子邮件转到自己设立的信箱里，而后，私下选择一俄罗斯客商签订了贸易额达 50 万美元的经济合同。不久，该客商向他们汇出了 6 000 多美元的首期货款定金，随后，章、李二人将所需产品委托当地一家企业进行加工生产，此举共造成公司十余万美元的经济损失①。

2. 利用互联网络披露非法获取的商业秘密，或者违反约定披露商业秘密

互联网络是一个覆盖广泛的交流空间，在这一空间上披露被害单位的商业秘密，能够在极为广泛的范围造成严重影响，给被害单位造成惨重损失。行为人披露商业秘密的方法有多种，如发送广播式或多址电子邮件，或者在电子公告栏上披露信息等等。例如，在 Religious Technology Center V. Netcom 一案中，行为人在国际互联网络上将被害人的商业秘密广泛发布，给被害人造成严重损失。

3. 从电子商务企业的计算机信息系统中窃取商业秘密

电子商务企业计算机信息系统中往往存储着大量的商业秘

① 周咏：《电子邮箱失窃》，《南方周末》，1999 年 5 月 28 日。

密，行为人可以通过各种手段窃取计算机信息系统中的商业秘密，其行为方式主要有以下两种：(1) 非法侵入计算机信息系统并窃取商业秘密。例如章某等窃取证券公司商业秘密案，1999年章某为帮助田某“解套”股票，专门编写了一套计算机程序准备输入证券公司的电脑系统。3月中旬的一个夜晚，章某和田某将电缆线的一头接入自己的便携式电脑，另一头用铁丝绑扎后接入该证券公司的终端插口内，他们输入有关程序后，就看到并测出该公司的信息和密码系统。此后，他们多次采用同样的方法，获取了该公司上万股民的地址、资金额度、证券种类、账号和买卖记录等信息①。(2) 单位职员离职后，利用以前了解的技术秘密，非法侵入计算机信息系统窃取商业秘密。一些电子商务企业的技术人员或者管理人员离职后，如果单位安全防范措施不健全，他们还能继续使用原来的密码或者其他技术秘密进入原单位的计算机信息系统窃取商业秘密。例如在美国佛罗里达州，一个叫夏皮罗的人原在一家电视公司工作，转到另一家公司工作后，新公司的上司与其合谋，利用他以前掌握的密码，上网进入原单位的计算机信息系统并窃取商业秘密。

4. 单位内部人员违反约定向他人提供商业秘密

企业内部人员根据合同约定对单位的商业秘密负有保密义务，不得向他人透露商业秘密，但有些犯罪行为人出于利益驱动等原因，不惜出卖本单位商业秘密。

二、侵犯商业秘密罪的概念和犯罪构成

我国打击电子商务领域的侵犯商业秘密犯罪的刑事法律条文，主要是《刑法》第287条、第219条、第220条。《刑法》第287条关于“利用计算机实施金融诈骗……或者其他犯罪的，

① 陶双庆：《上海抓获两名“电脑黑客”》，《光明日报》，1999年5月17日。

依照本法有关规定定罪处罚”的规定和《关于维护互联网安全的决定》，是认定电子商务领域的侵犯商业秘密犯罪的法律前提，行为人在电子商务活动中实施侵犯商业秘密犯罪的，依据我国《刑法》第 219 条、第 220 条侵犯商业秘密罪定罪量刑。

侵犯商业秘密罪，是指违反国家商业秘密保护法规，侵犯他人商业秘密，造成法定后果的行为。本罪具有基本罪和派生的重罪两个构成类型。

（一）基本罪的构成要件

本罪的基本罪由选择主体、犯罪故意、选择性危害行为、特殊犯罪结果、特殊犯罪对象、被害法益 6 个要件构成，具体内容和形式如下：

1. 选择主体

本罪主体是选择主体，即年满 16 周岁且具有刑事责任能力的人，或者一般单位。犯本罪的自然人通常是合同约定负有保密义务的当事人和本公司、企业知悉或掌握商业秘密的人；犯本罪的单位，法律未作限定。

2. 犯罪故意

本罪在主观上表现为故意，即明知是权利人已采取保密措施加以保护的商业秘密，而故意实施侵犯他人商业秘密的行为；明知或者应知自己的行为是侵犯商业秘密行为，而非法获取、使用或者披露他人的商业秘密的，以侵犯商业秘密罪论。无论行为人出于何种动机、目的，均不影响本罪的认定。

3. 选择性危害行为

本罪的危害行为表现为以下三种选择性行为方式：（1）以盗窃、利诱、胁迫或者其他不正当手段获取权利人的商业秘密。商业秘密权利人，指商业秘密的所有人和经商业秘密所有人许可的商业秘密使用人。盗窃，即秘密窃取。利诱，指给予知情人一定的物质或其他好处进行引诱，使其透露所知商业秘密。胁迫，指以人身、名誉、财产损害相威胁，对秘密知情人进行精神强制，

使其迫于压力，而被迫交出商业秘密。其他不正当手段，包括以高薪挖走、以重金收买知悉商业秘密的人，甚至派遣商业间谍，等等。实施这种行为的人，一般是商业秘密权利人的竞争对手，希望通过这些不正当手段获取对方商业秘密，使对方丧失竞争优势，提高自己的竞争地位。(2) 披露、使用或者允许他人使用以前项手段获取的权利人的商业秘密。此行为具有两个特征：一是行为人已经获得了盗窃、利诱、胁迫或者其他不正当手段获取了权利人的商业秘密；二是除前述行为外，又实施了披露、使用或者允许他人使用这些商业秘密的行为。(3) 违反约定或者违反权利人有关保守商业秘密的要求，披露、使用或者允许他人使用其所掌握的商业秘密。此行为具有三个特征：一是行为人通过合法途径掌握了权利人的商业秘密；二是行为人按照与权利人的约定，或者按照权利人有关保守商业秘密的要求，承担有保守这些商业秘密的义务；三是违反这些约定和保密要求，向第三人披露、自己使用或者允许第三者使用这些商业秘密。实施这类行为的人，通常是与拥有商业秘密的企业订立许可使用合同的一方当事人，也可能是本企业内部因工作关系知悉商业秘密的技术人员、管理人员。只要实施了上列任何一种行为，即可构成本罪行为。

本罪对行为人如何“获取”、“披露”、“使用”、“允许使用”等行为的方法没有特别要求，在电子商务领域，本罪的行为方法通常是利用电子商务计算机信息系统的特性。

4. 特殊犯罪结果

本罪是结果犯，侵犯商业秘密的行为必须给权利人造成重大损失。所谓重大损失，是指经济上的重大损失，包括在竞争中处于不利地位、产品大量积压、营利性服务严重受挫、减少盈利、增加亏损等。如果损失不严重，可按照一般民事侵权行为处理。

5. 特殊犯罪对象

本罪的犯罪对象是商业秘密。关于商业秘密，国内外学者说

法不一，一般认为，商业秘密有广义和狭义之分。广义的商业秘密，又称工商秘密，包括所有生产领域（工、农、牧）和商品流通领域里的未经公布的经营信息与技术信息；狭义的商业秘密则仅指其中的经营信息。根据刑法第 219 条的规定，“商业秘密，是指不为公众所知悉，能为权利人带来经济利益，具有实用性并经权利人采取保密措施的技术信息和经营信息”。它具有以下特征：(1) 信息性。即这些秘密本身是种信息，这种信息能对某方面的经济活动产生积极影响。(2) 经济性。指这种秘密的内容是技术信息和经营信息，这些信息是商业经营中所需要使用的，有利于使用者的经营活动，能给其带来经济上利益的信息。“技术信息”，通常指技术配方、技术诀窍、工艺流程等。“经营信息”一般指采取什么方式进行经营等有关经营的重大决策以及与自己有业务往来的客户情况等。(3) 实用性。指这种信息是直接与生产、经营相关的、应用性比较强的具体信息，而不是一般抽象的观点或思路。(4) 保密性。指这些信息不为公众所知悉，只限于少数人知道，并且商业秘密的权利人已对这些信息采取了保密防范措施，防止他人轻易获取。如果某些信息已为大家所知悉，不具有秘密性质，或者权利人没有采取保密措施而使他人通过正常渠道了解到信息内容，都不属于商业秘密范围。

6. 被害法益

本罪侵犯的直接客体是商业秘密的专有权。

（二）重罪的构成要件

本罪的重罪构成要件，是指罪行在符合基本罪构成要件的基础上造成特别严重后果的行为。至于什么是“造成特别严重后果”，目前尚无有权解释，根据刑法理论联系司法实践，一般是指给权利人的生产经营造成特别重大的经济损失或者导致公司、企业破产等。

根据《刑法》第 287 条、第 219 条、第 220 条的规定，个人利用计算机犯本罪基本罪的，处 3 年以下有期徒刑或者拘役，并

处或者单处罚金；犯重罪的，处3年以上7年以下有期徒刑，并处罚金。单位利用计算机犯本罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照个人犯本罪的规定处罚。根据《关于进一步加强知识产权司法保护的通知》，犯侵犯商业秘密罪造成被侵权人损失的，除依照上述规定追究行为人的刑事责任外，还应按照刑事附带民事诉讼的规定追究民事责任。

三、对几类典型犯罪行为的审判处理意见

1. 未经允许获取电子邮件，进而获取商业秘密，如何处理？

在前面提到的章、李转移公司电子邮件，窃取商业秘密的案件中，章、李擅自改变公司电子邮件信箱设置，攫取他人电子邮件，窃取商业秘密。对于该案件，作者认为，电子邮件是目前广泛应用的、快速、廉价的邮件服务，当然属于我国刑法规定的信件范围，行为人截获他人电子邮件的行为构成侵犯通信自由罪。行为人从电子邮件中获得了公司业务往来的商业秘密，并使用该商业秘密与客户交易，造成公司特别巨大的经济损失，构成侵犯商业秘密罪重罪。由于行为人隐匿、非法开拆公司电子邮件的行为，与侵犯商业秘密的行为构成方法和目的的关系，因此行为人的行为构成侵犯通信自由罪和侵犯商业秘密罪的牵连犯，按照“从一重罪处罚”的原则，以侵犯商业秘密罪重罪定罪量刑。如果行为人没有给被害人造成重大损失，或者行为人从电子邮件中获取的只是一般的信息而非商业秘密，但有多次实施隐匿、打开电子邮件的，只构成侵犯通信自由罪。本案中章、李二人构成共同犯罪。

2. 行为人在互联网络上披露他人商业秘密的，如何处理？

前面提到Religious Technology Center V. Netcom的案件中，行为人在国际互联网络上将被害人的商业秘密广泛发布，给被害人造成严重损失。如果行为人利用发送电子邮件或者在电子公告

栏上发布消息等方式披露他人商业秘密，由于电子邮件服务器服务失败而导致邮件未能成功发送，或者提供电子公告栏的服务器发生故障，商业秘密尚未被他人知悉，这种情况该如何处理？作者认为，侵犯商业秘密罪是结果犯，只有造成重大损失或者其他严重后果的，才能构成侵犯商业秘密罪既遂。行为人实施完侵犯商业秘密罪的行为，由于意志以外的因素未能得逞的，如果情节十分恶劣，具有严重社会危害性的，属于犯罪未遂，构成侵犯商业秘密罪（未遂）。

根据我国《刑法》，行为人明知是他人以不正当手段获取了商业秘密，而获取、使用、披露的，可能构成侵犯商业秘密罪。但是，如果行为人经合法途径获取了商业秘密，而后进行传播的，则可能不构成本罪。这是因为，商业秘密一旦在互联网络上披露，就可以被网上数以万计的用户获悉，从而不再具有“不为公众知悉”的保密性，也就不再是商业秘密。行为人实施以上行为的，由于对象不是侵犯商业秘密罪的犯罪对象，当然不能构成侵犯商业秘密罪。

3. 行为人非法侵入他人计算机信息系统，窃取商业秘密的，如何处理？

前面提到章、田二人非法侵入证券计算机信息系统窃取商业秘密案和原电视公司职员夏皮罗利用他以前掌握的密码，非法侵入原单位的计算机信息系统并窃取商业秘密案中，对于前者，如果行为人非法侵入的是国家事务、国防建设、尖端科学技术领域的计算机信息系统，如行为人非法侵入中国人民银行的计算机信息系统，窃取商业秘密，并给权利人造成重大损失或者其他严重后果的，构成非法侵入计算机信息系统罪和侵犯商业秘密罪的牵连犯，以侵犯商业秘密罪定罪处罚；如果没有造成重大损失或者其他严重后果，以非法侵入计算机信息系统罪定罪处罚。对于后者，行为人虽然在技术上仍然保留进入访问目标计算机信息系统的权限，然而这一权限仅仅是因为安全管理的疏漏而存在，根据

劳动合同和其他法律不得具有和继续行使，行为人使用相关技术密码或者其他技术秘密，进入计算机信息系统的行为，属于非法侵入计算机信息系统的行为，进而实施窃取商业秘密的，依照前者的处理方法进行处理。

第五节 电子商务领域的诈骗犯罪

一、电子商务领域诈骗犯罪的发展现状

随着互联网络技术及应用的发展，网上购物人数和金额与日俱增。全球至少有 1.2 亿人进行过网上购物，1999 年美国节日购物潮中网上购物额高达 70 亿美元，是 1998 年节日期间网上购物额的两倍多。有观察家预言，网上年消费额将从 1999 年的 150 亿美元猛升至 2003 年的 780 亿美元①。同时，电子商务交易的商品日益丰富、交易方式日趋多样。如商业网站的网上拍卖活动为商品销售开辟了广泛的市场，也为用户获取物美价廉的商品提供了新的机会；网上大学如雨后春笋般迅速出现，为求学者提供远程教育的机会，自己也获得丰厚的回报；金融证券行业参与电子商务，通过网络接纳客户、办理各种业务，不仅扩大了客户市场、增加业务处理能力，而且大幅度降低了交易成本、优化了服务质量。

庞大的电子商务市场蕴含着巨大的经济利益，吸引大量客户涌入，其中不少是盲目的随大流者，这是电子商务领域诈骗犯罪产生的重要条件和原因。以网上拍卖为例，美国网上拍卖市场增长迅速，市场研究公司 Forrester Research 估计，2000 年美国网上拍卖生意额会由两年前的 14 亿美元，上升至 61 亿美元，估计

① 《世界各国应联合对付互联网诈骗》，《法制日报》，2000 年 7 月 23 日。

到两年后将会超过 120 亿美元，增幅达一倍。但是，网上拍卖诈骗问题亦随之而来，美国联邦贸易委员会 1999 年接到 10 700 宗有关网上拍卖的投诉，是 1997 年的 100 倍，联邦贸易委员会副主席保罗说，超过一半有关互联网的投诉是网上拍卖诈骗。eBay 商业网站是美国著名的大商业网站，2000 年首季该网站发生的诈骗个案就超过 2 100 多宗①。其他种类的电子商务诈骗犯罪如网上证券销售诈骗、网上大学诈骗、网上基金会诈骗等也十分猖獗，而且这些诈骗犯罪行为与传统形式的诈骗犯罪截然不同，具有新的犯罪形式和特点。目前，电子商务领域诈骗主要表现为以下几种行为方式：

1. 网上拍卖诈骗

目前许多商业网站提供商品拍卖服务，网络用户进入该网站，登记交易身份后，就可以参加网上商品拍卖。由于网上拍卖的商品往往比市面商店里的商品要便宜，因而吸引了大量网络用户参与。但是，由于目前尚没有网上个人身份认证管理，网络用户为参加拍卖而登记的交易身份可能是编造的虚假身份，行为人使用这种假身份，低价拍卖商品，而一旦收到买主的汇款或者信用卡划拨来的资金后，就消失得无影无踪。而要根据行为人留下的交易身份根本找不到本人，行为人注册另外一个交易身份又可以堂而皇之地再次进行网上拍卖诈骗活动。目前，网上拍卖诈骗是电子商务领域诈骗犯罪的主要犯罪形式，这方面的案件有很多，如发生在雅宝网站上的拍卖诈骗案。2000 年 6 月雅宝拍卖网客户服务中心收到了一封不同寻常的电子邮件，山东泰安的王某反映，他在网上通过竞价的方式购买了一部 Nokia8810 手机，汇款给卖主之后，就和这位名叫“kiss590069”的物主失去了联系。雅宝客户服务中心根据王先生提供的线索查找发现，网名为

① 《eBay 首季出现 2100 起网上交易诈骗案》，《联合早报》，2000 年 5 月 23 日。

“kiss590069”的物主所有注册信息的真实性都值得怀疑。经进一步核实，该人同时有4台手机正在网上拍卖，参与竞标的人相当多，物主的留言很有吸引力，物品的起拍价格均低于市场价1 500～2 000元。雅宝客户服务中心找到了曾与“kiss590069”物主进行过交易接触的肖某、白某等其他几位用户，这几位用户的交易情况也与王先生的情况基本相同：将钱汇给物主之后就与其失去了联系，手机不开、呼机不回，钱付了出去，货却没有收到①。

2. 网上大学诈骗

网上大学远程教育是近年来发展起来的一种新的教育形式，由于其具有建设、营运成本低，学费低廉等优点，发展十分迅速，成为一种极有发展潜力的新教育产业。但是，有些网上大学不注重教育质量，只关心收缴学费的数量，甚至假冒合法营运或者名牌大学，诈骗他人钱财。例如美国堪萨斯州的司法部长最近下令关闭了一所被控向人们提供假学位的网上大学，堪萨斯州的司法部长Carla Stovall日前向Leslie Edwin Snell提起诉讼，指控其发布虚假广告，声称在线Monticello大学能够提供堪萨斯州和其他州的官方机构承认的学位证书。大约200个人为了取得大学和研究生学位，分别向Snell支付了2 000～8 000美元不等的费用，而实际上Monticello大学未经任何官方机构批准②。

3. 冒充电子商务交易方诈骗他人财物

电子商务中商务活动的有关信函，都是通过互联网络以电子数据的形式进行传输和交换，这些商业秘密信息如果不慎泄露，可能被犯罪人利用来假冒电子商务交易方，诈骗他人财物。例如发生在余姚的网上骗取国外汇款案。1998年11月，姚某发现自

① 《雅宝协助警方侦破首例网络诈骗案》，http://www.ccidnet.com/，2000年7月13日。

② 《美一在线大学行骗被关闭》，《计算机世界》，1999年9月9日。

己的电子信箱中有荷兰一公司发给泰丰公司的信，信中提到支付货款 1 万美元事宜。姚某决定占有此笔货款。此后两天他通知荷兰方面更改收款银行账号，并提供了自己分公司的银行账号。12 月 21 日，荷兰方面即按姚某提供的账号汇入了 5 130 美元①。

4. 网站诈骗国际电信资费

电信用户在使用国际电信通信时，有一部分电信资费归国外的电信公司或者个人所有，有些行为人为谋求非法利益，在网站上设置“陷阱”诈骗他人财物。例如长春市民句某的女儿上 163 信息网 138 分钟，却花费了 1 956 元钱。句某找到市电信局询问，工作人员说这种情况是网民掉进了国外一些商业公司精心设置的“互联网陷阱”。据介绍，国外有一些商业公司精心设计恶意网站通过游戏、软件诱惑网民，这些游戏、软件中往往隐藏了陷阱指令，会隐蔽地断开用户通信线路，并拨通国际长途电话，使网民在不知不觉中已经用国际长途在远程拨号上网。国外的恶意网站可通过这种“网络陷阱”，引诱用户上网，并从中挣取部分国际话费②。

5. 建立网上基金会，诈骗他人财物

非法投资会、基金会诈骗钱财的案例屡有发生，这种行为借助电子商务的合法外衣，能够更加隐蔽地骗取更多人的财物。例如，1996 年美国华盛顿州贝灵汉的“幸运联盟”公司采取“金字塔”骗术，在互联网络上刊登广告进行诈骗，共骗取了 600 多万美金。幸运联盟利用人们想发财的心态，成立了一个投资会，保证加入者获得巨额投资回报，这一骗局使得数以千计的投资者纷纷投下资金，数额从 250～1 750 美元不等。该公司向会员宣

① 李朝军：《互联网上骗来国外汇款　余姚一用户将错就错美梦一场》，《检察日报》，1999 年 2 月 24 日。

② 《上网 138 分钟花掉 1956 元　网民需警惕“网络陷阱”》，《生活日报》，2000 年 3 月 20 日。

布，能吸引他人入会的会员的“利润”每月将达到 5 000 美元以上，并向会员提供建议及宣传材料，让他们在互联网络上设立网址，以吸引新的会员，新入会的会员经过最初的努力可以赚到一些钱，但最后大多数会员只落得两手空空①。

6. 网上销售证券诈骗

网上证券投资是证券业务发展的新方向，由于其便捷、成本低廉，受广大投资者欢迎，然而有些犯罪人则利用这种证券投资新形式诈骗钱财。1999 年英国调查人员披露了一个通过互联网进行投资诈骗的案件。诈骗分子首先虚构一个不存在的股票，并为这种虚构的股票建立网站，该网站不断更新信息，制造股票发展良好的假象，然后，诈骗分子向网络用户寄送资料，要求他们以“特别”低的价格购买股份，并将投资者引到假股票信息网站。当投资者希望退出时，诈骗分子就告诉投资者不能抽回投资。据警方估计，本案诈骗金额已达数十亿港币。

7. 利用中奖信息诈骗他人财物

以中大奖为诱饵诈骗广大被害人的财物，是一种比较传统的诈骗方法，这种诈骗手法也被利用到互联网络上，并且具有了新的形式和特点。2000 年 7 月，开罗的一位青年女教师马赫尔收到一个电子邮件，被告知澳大利亚举行的一个国际抽奖活动中，她中了头奖，奖金为 900 万美元，在邮件的最后，发信人告诉她立即向某个账号汇款 60 美元，以便他把那 900 万美元巨奖给她汇去。马赫尔是开罗苏伯拉区一所中学的普通青年教师，不认识任何澳大利亚人，既没亲戚，也没朋友或网友，更没参加什么抽奖活动，怎么会得奖呢？实际上，这个特大喜讯只是一个网上骗局而已，如果她往邮件上所说的那个账号汇去 60 美元的话，那将是“肉包子打狗”，那 900 万美元一个子儿也得不到！无独有偶，埃及天文研究中心航天研究部主任雅各布也收到一个邮件，

① 胡泳、范海燕：《网络为王》，海南出版社 1997 年版，第 298 页。

祝贺他已被评为 20 世纪最伟大的科学家之一，某个著名国际学会将给他颁发大奖。邮件最后一行注着：请往某个银行账号汇去 150 美元获奖证书费和 150 美元奖章费。令人称奇的是，其后一个星期，雅各布的助手也收到了内容几乎完全相同的邮件。雅各布和他的助手估计是在 1992 年去美国参加一个国际研讨会时，会议主办者索要了他们的简历和通讯地址，行骗者因此知道了他俩的电子邮件地址①。

面对日益严重的电子商务领域诈骗犯罪，世界各国纷纷采取法律手段进行打击，美国联邦贸易委员会、司法部、邮政检查机构及全国司法部长协会连同其他政府部门积极展开对网络拍卖诈骗活动的侦查和起诉。同时，打击电子商务领域诈骗犯罪的国际协作也迅速发展起来，美国联邦贸易委员会策划了一次针对“迅速致富”诈骗的搜寻浏览，28 个国家的 150 个组织参加了这次最大的国际执法活动，主要目标是打击以互联网为依托的连锁投机诈骗、贸易和投资机会诈骗以及欺骗性的当日买卖活动。联邦贸易委员会号召几十个国际组织，包括挪威、巴西、澳大利亚、香港、日本的消费者权益保护机构及国际消费者组织，连同美国许多联邦机构、49 个州级和地方消费者保护组织都参加了这次搜寻活动。

二、诈骗罪的概念和犯罪构成

我国打击电子商务领域诈骗犯罪的刑事法律条文主要是《刑法》第 287 条、第 266 条。《刑法》第 287 条关于“利用计算机实施金融诈骗……或者其他犯罪的，依照本法有关规定定罪处罚”的规定和《关于维护互联网安全的决定》，是认定利用电子商务领域诈骗犯罪的法律前提，行为人在电子商务活动中实施诈骗犯罪的，依据我国《刑法》第 266 条诈骗罪定罪量刑。

① 蒋生元：《警惕网上诈骗》，《检察日报》，2000 年 7 月 26 日。

诈骗罪是指以非法占有为目的，采用虚构事实或者隐瞒事实真相的方法，骗取公私财物，具有法定数额或者其他法定情节的行为。本罪分为基本罪和派生的重罪、极重罪三个构成类型，它们的构成要件是：

（一）基本罪的构成要件

本罪的基本罪是由一般主体、直接故意、选择性危害行为、特殊犯罪结果、特殊犯罪对象、被害法益 6 个要件构成。

1．一般主体

本罪的主体是一般主体，即已满 16 周岁具有刑事责任能力的自然人。在《刑法》修改以前，由于诈骗罪罪名单一，有关司法解释曾经规定，对“以单位名义实施诈骗”，“诈骗所得归单位所有”的行为，实行单罚制，即只追究单位直接负责的主管人员和其他直接责任人员的刑事责任。修改后的《刑法》已将经济诈骗从诈骗罪中分解出去，另规定为若干新罪名，从而形成普通诈骗罪与特殊诈骗罪的竞合关系。本罪是普通诈骗罪。由于现行《刑法》对单位诈骗行为另有规定，所以本罪的主体不包括单位。

2．直接故意

本罪在主观方面表现为直接故意。直接故意的一般犯罪目的是明知自己实施诈骗行为会侵害他人财产权的严重后果，而希望这种危害结果发生的心理态度。间接故意和过失不构成本罪。本罪除了一般犯罪目的外，还有非法占有公私财物的特殊犯罪目的。

3．选择性危害行为

本罪在客观方面表现为诈骗行为。所谓诈骗行为，是指虚构事实或者隐瞒真相，使财物所有人或管理人信以为真，“自愿地”交出财物的行为。虚构事实和隐瞒真相，是本罪行为的两种并列选择行为形式，只要实施其中一种行为，便可构成本罪。所谓虚构事实，是指捏造全部或部分虚假的事实，骗取被害人的信任，

使其“自愿地”交出财物；所谓隐瞒真相，是指故意对被害人掩盖客观上存在的事实，使被害人受哄骗，产生错觉，“自愿地”交出财物。表面上看，被害人交出财物似乎是“自愿”的，其实这是由于行为人的欺骗行为所引起的，如果被害人了解事实真相，决不会将财物交给对方，所以“自愿地”交出财物并非被害人的真实意思表示。

本罪规定了两种选择性的行为方式，即虚构事实或隐瞒真相，但没有规定危害行为的具体方法，也就是说，可以使用各种行为方法实施本罪的犯罪行为。在电子商务领域，行为人大多利用电子商务计算机信息系统的应用功能，如商业网站的拍卖服务、电子公告栏服务等。

4．特殊犯罪结果

本罪的特殊犯罪结果是诈骗财物数额较大。至于何谓数额较大，最高人民法院于1996年12月16日《关于审理诈骗案件具体应用法律的若干问题的解释》中规定，个人诈骗公私财物2 000元以上的，属于“数额较大”。各省、自治区、直辖市高级人民法院可根据本地区经济发展状况，并考虑社会治安状况，在2 000～4 000元的幅度内，确定本地区执行“数额较大”的起点标准。这一司法解释虽然是在《刑法》修改前作出的，但在无新的有权解释时，仍可参照适用。

5．特殊犯罪对象

本罪的特殊犯罪对象是合法所有的公私财物。

6．被害法益

本罪侵犯的法益是公私财物的所有权。

（二）重罪的构成要件

本罪的重罪构成要件，是指在罪行符合基本罪构成要件的基础上，数额巨大或者有其他严重情节的行为。“数额巨大”和“其他严重情节”是构成重罪的选择要件，只要具备其中一项，重罪便可成立。根据前述司法解释，所谓“数额巨大”是指个人

诈骗公私财物 3 万元以上。各省、自治区、直辖市高级人民法院可根据本地区经济发展状况，并考虑社会治安状况，应在 3 万～5 万元的幅度内，确定本地区执行“数额巨大”的起点标准。在无新的有权解释时，仍可适用这一司法解释。至于何为“其他严重情节”，有待司法解释作出规定。在无新的有权解释时，根据刑法理论联系司法实践经验，作者认为，“其他严重情节”可界定为：诈骗数额在 15 000 万元以上，又具有下列情形之一的：(1) 诈骗集团的首要分子或者共同诈骗犯罪中情节严重的主犯；(2) 惯犯或者流窜作案危害严重的；(3) 诈骗法人、其他组织或者个人急需的生产资料，严重影响生产或者造成其他严重损失的；(4) 诈骗救灾、抢险、防汛、优抚、救济、医疗款物，造成严重后果的；(5) 挥霍诈骗的财物，致使诈骗的财物无法返还的；(6) 使用诈骗的财物进行违法犯罪活动的；(7) 曾因诈骗受过刑事处罚的；(8) 导致被害人死亡、精神失常或者其他严重后果的；(9) 具有其他严重情节的。

(三) 极重罪的构成要件

本罪的极重罪构成要件，是指在罪行符合基本罪构成要件的基础上，数额特别巨大或者有其他特别严重情节的行为。“数额特别巨大”和“其他特别严重情节”是构成极重罪的选择要件，只要具备其中一项，极重罪便可成立。根据前述司法解释，所谓“数额特别巨大”是指个人诈骗公私财物 20 万元以上。所谓“情节特别严重”是指诈骗数额在 10 万元以上，又具有前述重罪构成“其他严重情节”所列 9 项情形之一的行为。

根据《刑法》第 287 条和第 266 条规定，犯本罪基本罪的，处 3 年以下有期徒刑、拘役或者管制，并处或者单处罚金；犯重罪的，处 3 年以上 10 年以下有期徒刑，并处罚金；犯极重罪的，处 10 年以上有期徒刑或者无期徒刑，并处罚金或者没收财产。

三、电子商务领域诈骗罪的犯罪形态问题

1. 网上拍卖诈骗犯罪的既遂与犯罪未完成形态问题

在处理诈骗犯罪案件时，行为人诈骗的财物是否达到法定数额，是确定本罪罪与非罪、重罪或轻罪的重要标准。在传统的诈骗犯罪中，被害人失去财物的数额与行为人非法占有的财物数额总是相同的，即财物从被害人手中被诈骗走的同时转移到行为人手中，因此，认定诈骗财物的数额比较容易。然而，在电子商务时代，这二者可能不一致，以哪一个数额为标准，存在不同看法，有的认为应当以被害人失去控制的财物数额为准；有的认为以行为人实际控制的财物数额为准；有的认为应当以被害人失去控制而由行为人控制的财物数额为准。作者赞同后者观点，这是因为，诈骗罪属于侵犯财产的犯罪，后者的标准反映了侵犯财产权的实际情况。在这一观点的基础上来分析网上拍卖诈骗犯罪中的犯罪形态问题。

网上拍卖诈骗行为人为了便于获取财物后隐匿，往往不让被害人通过邮局汇款，较多的是给被害人留下银行账户，要求被害人电汇或者转账，而接收汇款的银行账号多是以假名、假地址设立，案件发生后根据行为人虚假的网上交易身份和银行账号都难以发现犯罪行为人。行为人实施网上诈骗，可能会出现以下几种情况：(1) 行为人实施网上拍卖诈骗，被害人向行为人账户汇款，如果行为人提取、转移了资金，或者对该账户资金进行了消费，表明行为人已经实际控制了该账户中的所有资金，即使行为人只动用了被害人汇来资金的一部分，都应该将进入行为人账户的全部资金数额认定为犯罪数额，并据以认定是否构成诈骗罪的基本罪、重罪或者极重罪。(2) 被害人汇出数额较大的资金，但由于银行工作事故没有转入行为人账户的，或者虽然资金已经进入行为人账户，但是在行为人能够实际提取、转移、消费之前，由于被害人等方面的原因，银行冻结该账户，而造成行为人不能

实际控制被害人资金的，构成犯罪未遂。(3) 行为人为实施网上拍卖诈骗，在商业网站注册虚假身份资料的，构成犯罪预备行为，由于这时行为人没有实际的实施行为，犯罪主观意图尚未完全表现，应该认定情节显著轻微危害不大的违法行为，不以犯罪论。但是，如果行为人已经在网上发出虚假拍卖商品信息，即使尚未有客户与之联系，如果其拍卖的“商品”底价已经达到“数额较大”的标准，同时行为人已经着手实施犯罪行为，应该以犯罪未遂论处。(4) 被害人汇出的资金进入行为人账户，在被害人发觉或者案情暴露以前，行为人自动将资金退回被害人的，表明行为人已经没有非法占有他人财物的故意，构成犯罪中止，应该认定为情节显著轻微危害不大的行为，不以犯罪论处。

最后，行为人获取他人财物后，给被害人的是型号不对或者品种不对的低劣商品，应该构成诈骗行为；如果被害人实际获得的商品与支付的钱款差价达到“数额较大”的标准，应该以诈骗罪论处。

2. 网上发送中奖信息诈骗他人财物问题

利用中奖信息的电子邮件诈骗他人财物的，能否构成诈骗罪？作者认为，利用中奖信息的电子邮件，蒙骗他人寄送所谓的“证书制作费”、“奖章工本费”，属于诈骗行为。这种行为能否构成诈骗罪，要看其是否齐备诈骗罪的全部犯罪构成要件，其中最关键的是犯罪数额是否达到“数额较大”的法定标准。对于收到电子邮件的某一个具体人而言，行为人能够诈骗的财物非常有限，如前面的案件中行为人索取的钱款不超过 200 美元，因此，行为人如果只向某个人发送电子邮件，诈骗一定的财物，往往因为犯罪数额得不到犯罪要求的标准，而不构成犯罪，只构成违法诈骗行为。但在实际生活中，这类行为一般不会只对某几个人实施，行为人往往有具体的行动计划，对不特定的较多人发送这类电子邮件，以欺骗其中一部分被害人寄送财物，因此，对于这类案件，应该进行全面调查，查明行为人犯罪所得的实际数额，如

果达到本罪规定的法定数额的，构成本罪的基本罪、重罪或者极重罪。行为人为实施诈骗发出大量电子邮件或者实施诈骗行为次数非常多的，表明行为人意图诈骗更多被害人的财物，其主观恶性更大，这一情节应该作为量刑从重的依据。

行为人为实施诈骗发出大量电子邮件或者实施诈骗行为次数非常多，意图诈骗他人数额较大或者巨大的财物，由于意志以外因素违法所得未达到法定数额的，应以诈骗罪未遂论处。

第六节　电子商务领域的非法行医罪

一、电子商务领域非法行医罪的发展现状

随着电子商务的发展，网络远程医疗服务悄然兴起并迅速发展。澳大利亚早在 1995 年就着手建立了“健康通讯网络”公司，目前这个网络医疗保健信息提供商为澳提供超过 70％的医院信息服务，它的在线教育数据库包含了世界上主要医学期刊中的信息①；德国也开设了医疗服务网站，全天候为老年人和伤残人服务；1999 年我国首家“网上医院”在深圳开通，患者只要把自己的疾病症状等写在网上或者直接发给自己选定的“网上专家诊室”，即可得到专家的诊断和治疗建议②；2000 年中日双方共同承担的中日信息化合作远程医疗系统在哈尔滨开通，哈尔滨市的第一中心医院、北京协和医院、辽宁省的金秋医院三所医院之间实现了真正意义上的远程网上医疗③。除了以上政府或者医院建

① 《网上医疗在澳悄然兴起》，《检察日报》，1999 年 3 月 7 日。

② 《深圳首家“网上医院”开张　患者耐心等待 48 小时内就有答复》，《电脑日报》，2000 年 7 月 30 日。

③ 杨晓慧：《远程网上可会诊　中日合作示范工程在一中心开通》，《今晚报》，2000 年 2 月 7 日。

立的网上医疗网站外，一些个人或企业建立和营运的网上医疗网站也逐渐发展起来，目前互联网上已有 15 000 多家医疗网站，访问这些医疗网站的用户人数越来越多。

通过互联网络的远程医疗是计算机、网络技术应用在医疗卫生领域的重要表现。在传统的诊治方式下，医师和病人必须会面才能进行诊断治疗，而使用远程医疗设备设施，医师、病人哪怕远隔千山万水也能进行诊断和治疗。网络远程医疗能够克服医疗技术地区发展不平衡的障碍，充分利用医疗人才和技术资源，及时抢救危险病人，使人们获得更完善的医疗保障，实现医疗服务的及时、个人化和个性化，深受广大就诊人的信任和欢迎。但是，由于就诊人无法直接验证医疗方的资格，网络远程医疗也可能被犯罪人用来实施非法行医，成为非法行医犯罪的一种新犯罪方法。电子商务领域非法行医犯罪与传统方式不同，主要表现为以下两种行为：

1. 设立网络站点非法开展医疗保健业务

在电子商务发展过程中，人们逐渐认识到网上医疗保健是一个庞大的市场，近年来医疗卫生网站迅速增加，如 Yiyee.com，newhealth.com.cn 等，同时，其他商业网站也纷纷增加医疗卫生服务项目，网络用户通过这些网站获得各种医疗信息和服务。我国网上医疗市场发展迅速，而国家相应的法律法规管理制度尚未跟上，在经济利益的驱使下，一些未取得执业医师资格和未经卫生行政部门注册行医的人员，也参与建立和营运网上医疗网站，他们利用患者为了省时、省事、省钱和急于求医治病、热衷接受个性化医疗的心理，冒充医学博士、教授和专家，在互联网上开展营利性医疗保健业务。

非法行医的方式有两种：(1) 信息咨询。在网站上提供具体疾病的症状、预防、保健信息，而这些信息的科学性、有效性往往得不到保障，就诊人根据这些信息进行自我保养预防，可能造成相反的效果。(2) 网上接诊。这些网上医疗网站安排未取得执

业医师资格和未经卫生行政部门注册行医的人员在网上坐诊，就诊人接入非法医疗保健网站后，填写个人病状的电子表格，或者直接向网站发送电子邮件，把个人的身体、心理症状告诉“医师”，接诊人根据这些症状信息判断就诊人是否患病和患了何种疾病，并给出诊断、治疗处方。由于就诊人自己对症状的发现和描述不可能完全科学，以及难以保证接诊人的医疗水平，这种接诊方式往往不能正确诊断就诊人的真实健康状况，对于一些比较危险的疾病，容易造成误诊，严重的会危及就诊人身体健康和生命安全。而且，这种网上医疗所开的处方难以落实接诊人的医疗责任，一旦发生损害就诊人的健康和生命安全的后果，就难以追究接诊人的责任。如 2000 年 7 月澳大利亚医学协会宣布，居住在澳大利亚新南威尔士州乡村的一对老年夫妻日前一起自杀，原因是一个互联网医疗网站的诊断使这对老年夫妻相信，妻子可能患有晚期癌症。但是，据澳大利亚医学协会一般治疗委员会主席 David Rivett 称，验尸结果显示，这位妇女根本就没有患癌症。他说：“这对夫妻不想彼此分离，就一起结束了自己的生命。但是，这是误诊。”David Rivett 表示，这起悲剧显示出通过互联网进行自我诊断和自行开处方的危险性。

行为人非法进行网上医疗获取商业利益有两种方式：一种是直接收取就诊人的钱财，具体收费方式既可以是通过网络服务提供商收取信息服务费，或者是“网络医师”和病人建立专门的个人医师服务合同，按照合同规定收取费用。另一种是前期免费提供网上医疗服务，以吸引网络用户访问网站，提升网上医疗网站的知名度和点击率，以后再利用网络广告、建立网上药店等方法赚取利润，因此，看似行为人免费提供医疗服务，实际上具有行医营利的目的。

2．网上医疗网站使用自查自诊智能医疗系统进行非法行医

医学科学的发展已经使相当多的疾病得到了充分、深入的研究，对某些疾病可以根据基本生理病理数据，查明人体健康状况

并提供规范化的治疗方案，医学研究的这些成果与计算机技术的有机结合，促使智能化电子医疗设备的产生。这种智能化的电子医疗设备通常是一种机电一体化的医疗设备，有的则是计算机“医疗专家系统”软件，其区别于一般电子医疗设备的地方，在于智能化程度很高，能够自动检测病人的身体、心理状况，经过设备内部的计算机逻辑分析判断，给出诊断结果，有的能选择相应的治病方案，控制其他部分的电子设备给病人治疗。以计算机医疗专家系统软件为例，行为人只需要提供自己的症状信息，该系统就可以给出就诊人是否患病和患何种疾病的诊断结果。这种医疗设备的智能化程度正在提高，能够处理的疾病种类也越来越多，具有广阔的市场前景。但是，这种医疗设备研究、生产必须依法进行，投入使用还须通过有关机关的鉴定和批准，操作者只能是具有行医资格的执业医师。

二、非法行医罪的概念和犯罪构成

我国打击电子商务领域非法行医犯罪的刑事法律条文主要是《刑法》第 287 条、第 336 条第 1 款。《刑法》第 287 条关于“利用计算机实施金融诈骗……或者其他犯罪的，依照本法有关规定定罪处罚”的规定和《关于维护互联网安全的决定》，是认定利用电子商务领域非法行医犯罪的法律前提，行为人在电子商务活动中实施非法行医犯罪的，依据我国《刑法》第 336 条第 1 款非法行医罪定罪量刑。

非法行医罪，是指未取得医生执业资格的人非法行医，情节严重或者造成其他法定后果的行为。本罪分为基本罪和派生的重罪、极重罪三个构成类型。

（一）基本罪的构成要件

本罪的基本罪是由一般主体、直接故意、单一危害行为、特殊犯罪前提、特殊犯罪对象、被害法益、酌定构成要件 7 个要件构成，具体内容和形式如下：

1．一般主体

本罪的主体是已满 16 周岁且具有刑事责任能力、未取得医生执业资格的人，其既可以是中国人，也可以是外国人。只要未取得医生执业资格而非法行医的，都可能成为本罪的主体。

2．直接故意

本罪在犯罪心态方面表现为直接故意，直接故意的一般犯罪目的是行为人明知自己没有取得医生执业资格，违反国家对医疗工作管理秩序，可能危害就诊人的健康权利和生命安全，而故意实施非法行医行为的心理态度。本罪除了一般犯罪目的外，还有牟利的特殊犯罪目的。以牟利为目的是构成本罪不可缺少的要件。但对非法行医所造成的危害结果，只能出于过失，即行为人不希望危害结果发生，也不是放任危害结果发生，否则，可能构成其他犯罪。

3．单一危害行为

本罪的危害行为表现为非法行医的行为。所谓非法行医，是指未取得医生执业证书，非法开展诊疗活动。非法行医的方式是多种多样的，有的自己挂牌行医，有的在药店坐堂看病，有的挂靠某个单位开业行医，有的冒充医生在医疗单位从业，有的在集市摆摊看病或在城乡游串行医，有的在互联网上建立医疗站点行医，有的利用智能化电子医疗设备非法行医等。无论以何种方式非法行医，均不影响本罪的成立。

4．特殊犯罪前提

《中华人民共和国执业医师法》第 13 条规定了国家实行医师执业注册制度，“未经医师注册取得执业证书，不得从事医师执业活动”。《互联网医疗卫生信息服务管理办法》规定，所有的卫生信息网站，只能提供医疗卫生咨询服务，不得从事网上诊断和治疗活动。利用互联网开展远程医疗会诊服务的，只能是具有医疗机构职业许可证的医疗机构。因此，本罪的特殊犯罪前提是，违反了《执业医师法》、《互联网医疗卫生信息服务管理办法》等

金；犯重罪的，处 3 年以上 10 年以下有期徒刑，并处罚金；犯极重罪的，处 10 年以上有期徒刑，并处罚金。

三、对几类典型犯罪行为的审判处理意见

1．不具有执业医师证书的人在网站发布疾病诊断治疗处方，该如何处理？

不具有执业医师证书的人在网站上发布某种疾病诊断治疗处方，如果行为人是该医疗网站的经营方，或者是医疗网站的雇员，其行为直接或者间接以营利为目的，即使行为人只就特定疾病开列处方而不接诊病人，都应该认定其构成非法行医行为。这是因为网站上发布的疾病诊断治疗的处方，被求医人获取后，求医人可能根据自己的症状判断是否构成处方上判断的某种疾病，甚至可能直接按处方购药或者治疗。由于就诊人往往难以准确判断自己是否具有某种症状，在心理因素的作用下，可能发生无病误认为有病，进而错误地用药治疗，造成危害就诊人的健康或生命安全的严重结果。如果造成这种结果，虽然这一结果不是由网上发布的处方直接造成的，但是与其有因果关系，应该认定行为人的非法行医行为情节严重，构成非法行医罪。不具有执业医师证书的人在网站上发布疾病诊断治疗处方，没有引起就诊人身体健康遭受损害结果的，属于情节显著轻微危害不大的行为，应该按照相应的医疗卫生行政管理法规进行处理。

2．不具有执业医师证书的人在网上接诊病人开列处方，引起就诊人身体健康遭受损害等严重后果的，如何处理？

不具有执业医师证书的人在网上接诊就诊人开列处方，如果其具有营利的目的，应该构成非法行医行为，行为人多次进行这类非法行医的，应该认定具有严重情节，构成非法行医罪。在目前网上医疗诊断设备不能保障准确检测就诊人症状的情况下，仅仅根据就诊人自己的陈述难以如实反映就诊人身体状况，行为人根据就诊人陈述诊断疾病开列处方，极有可能造成误诊。这一情

况行为人是能够预见到的。一旦就诊人根据网上医师的诊断处方进行治疗，发生损害就诊人身体健康的严重后果，或者造成就诊人死亡的，构成相应的非法行医罪重罪或极重罪。

第六章　电子商务关联犯罪

第一节　电子商务关联犯罪概述

电子商务关联犯罪是传统犯罪在电子商务发展中的衍生物，它与电子商务相关，但不发生在正常电子商务活动过程中。电子商务关联犯罪与电子商务犯罪的特征相似，如行为方式上表现为利用计算机信息系统特性，犯罪心态多表现为以牟利为目的，或者出于其他与经济利益相关的目的动机等；它与电子商务犯罪的区别在于，这类犯罪不发生在正常电子商务活动中，但是必须以电子商务应用为前提。

电子商务的发展创生了新形式的社会活动和新形式的财富，这些新社会活动和财富的出现及其对社会的影响，强烈冲击着现有的社会组织体系，包括法律体系。电子商务关联犯罪是伴随这些新事物产生而产生的新法律问题，深入研究电子商务关联犯罪，必须首先了解这些新生事物的基本情况：

（一）电子货币

电子货币是信息技术新发展和金融业激烈竞争的产物。一般认为，电子货币是电子结算系统中账户资金的电子记录，它不同于纸币、硬币，也不同于本票、汇票、支票等金融票证，是一种新的财富形式。

电子货币具有以下基本特点：

（1）控制管理的多主体性

电子货币同时为两个以上不同主体管理控制。多个主体依据一定的协议共同分享电子货币的使用权，从而实现对电子货币的共同控制，同时，任何一方都不是排他地完全控制电子货币。以信用卡这种典型的电子货币为例。首先，客户和金融机构要签署一定的协议，同时控制着信用卡账户中的资金，用户凭信用卡可以进行取款、转账、消费等；金融机构可以暂时使用用户账户中的资金进行投资，当发生约定或者法定事由时，金融机构可以冻结用户信用卡账户中的资金，禁止账户资金的使用。其次，发行信用卡的金融机构凭借控制金融电子化设备和协议条款上的优势（信用卡使用协议通常规定，由于信用卡用户过失造成的电子资金的损失由用户承担），比用户更能有效地控制电子资金，当用户管理信用卡和密码不善造成电子资金被他人转入其他账户时，将失去对被使用的电子资金的控制权，但这些电子资金还处在金融机构的控制下。

（2）无形性

电子货币表现为电子结算系统中的记录，其本质是表示财富数量的信息，承载这种信息的载体有形，而电子货币本身无形，因此，持有、携带、使用电子货币可以不依赖有形的物体。金融机构一般通过计算机系统验证账号密码信息来管理这些无形的电子货币。账户密码如同金融机构提供的钱箱和钥匙，掌握了电子资金账户密码就等于掌握了电子钱箱的钥匙。

（3）流通环境的特定性

电子货币只能在金融电子化系统中流通，脱离金融电子化系统，电子货币无法发挥货币的功效。随着金融电子化的推进和电子商务的广泛应用，电子货币的种类将越来越多，应用范围将越来越广，但所有这些电子货币的流动仍然只在金融电子化系统内。

由于电子货币具有不同于传统货币的特殊性，与电子货币相关的法律问题必然具有特殊性。

（二）网上营销

互联网络是一种方便快捷的新型信息交流途径，当它用于商业目的时，就开创了一种新的商业模式——网上营销。网上营销不仅包括为销售货物所进行的商务信息交换，还包括利用互联网络传送计算机数据类商品，这种全新的商业活动方式具有联系范围广、快捷及时、成本低廉等优点，不仅大量出现在正常电子商务交易活动中，也为非法交易所青睐，如网上销售违禁物品、网上推销淫秽或者其他有害信息等。

网上营销在行为方式、交易对象等方面与传统营销行为有较大差别，主要表现为：(1) 信息交换的网络化。交易方商务信息的交换通过互联网络完成，一般不留下有形的书面文件，即所谓的无纸化。(2) 交易对象特殊化。网上营销的交易对象除了传统的物品外，还包括计算机数据类商品，如计算机软件、数字化的音乐、图片、影像以及专业信息等。这类商品的特点是可以被无限次地复制，出售方销售的实际是计算机数据类商品的复制件而复制成本极低。此外，由于各国文化传统和法律制度的差异，各国规定了合法交易的不同范围，如我国禁止经营色情商业网站或者以色情信息牟利，而在日本和美国的一些州则视为合法商业行为。

目前互联网络上存在大量非法网上营销行为，给我国刑事法律体系带来了新的法律问题。

（三）电子代理人

电子代理人是美国《统一计算机信息交易法》中的概念，是指在没有人检查的情况下，独立采取某种措施，对某个电子信息或者履行作出反应的某个计算机程序或者其他手段①。在实际生活中，大量电子商务活动，如要约的提出、合同的签订履行等，

① 郑成思、薛红《国际上电子商务立法状况》，《科技与法律》，2000 年第 3 期。

都由这种电子代理人来执行，电子代理人的性质、行为特点、法律地位对相关法律问题有重要影响。

电子代理人是计算机程序或者机电一体化的设备设施，由交易主体事先设置好需要进行的目标行为及逻辑条件，交易对方按照要求进行预定的活动，如网上银行要求用户正确输入用户名和密码后，才能进行各种金融业务服务。电子代理人具有以下特点：

1. 电子代理人不是民法和刑法意义上的“人”。民事主体必须具有民事行为能力和民事责任能力，刑事主体包括自然人和单位，电子代理人是计算机程序或者是机电一体化设备设施，不具有责任能力，不能成为独立的民事关系主体或者刑事关系主体。

2. 电子代理人的“行为”由其权利人负责。电子代理人的行为逻辑反映了其权利人的意志，电子代理人的行为为其权利人希望或者默认，因此，电子代理人的行为所产生的后果当然应该由其权利人承担。由于开发者的疏忽或者意外因素导致的电子代理人行为“出轨”，造成其权利人意志以外的结果的，如果与交易对方没有责任分担约定，应由电子代理人的权利人承担意外结果产生的民事责任。

3. 电子代理人只能进行形式上的审查。电子代理人按照其权利人的设置审查交易对方提交的信息，这种审查只能是某方面的形式审查，例如网上转账系统只能判断用户输入的用户名和密码是否正确来判断是否是真实的用户。犯罪人冒用他人用户名、密码时，电子代理人会误认为真实的用户。随着现代信息技术的发展，电子代理人可以被设置更多的审查的条件，增加审查条件可以减少电子代理人错误处理的比例，但这以业务程序繁琐为代价。电子代理人形式审查后误认导致的后果，应当理解为其权利人能够认识到并容忍的结果，应该由其权利人承担责任。

（四）网络服务提供商的责任问题

网络服务提供商（ISP，Internet Service Provider）是指从事

互联网络服务的单位。按其提供的服务的种类，可以分为网络连接服务提供商（IAP，Internet Access Provider）和网络信息服务提供商（ICP，Internet Content Provider）。网络服务提供商的责任问题，就是他人利用互联网络实施违法犯罪时，网络服务提供商（包括 IAP 和 ICP）是否承担责任的问题。新加坡《电子商务法》规定，网络服务提供者不应因其无法控制的第三方的电子形式的信息而承担民事的或者刑事的责任。欧盟要求成员国不能给网络服务提供商施加一种一般性的监控义务，因为网络服务提供商没有能力保证通过其计算机信息系统的无数信息的合法性。欧盟法律还规定，网络服务提供商不因其传输或者存储的信息中含有违法信息而承担法律责任。美国《统一计算机信息交易法》规定计算机信息提供者对其提供的计算机信息负有担保的义务，即担保其提供的计算机信息不侵害第三方的权利，在许可期间被许可人的利益不会因为任何第三方对计算机信息主张权利而受到损害①。可见，各国对于互联网络服务提供商责任问题有不同的规定。作者认为，网络服务提供商是互联网络社会的重要组成部分，国家管理网络社会很大程度上必须通过网络服务提供商来完成，国家出于维护社会利益、国家利益的需要，有必要让网络服务提供商承担一定的责任；网络服务提供商在哪些方面应当承担责任以及承担责任的程度，必须考虑网络服务提供商在保障业务正常进行前提下的责任承担能力。由于 IAP 和 ICP 提供的网络服务不同，要求 IAP 承担检查、过滤浩如烟海、转瞬即逝的违法信息不具有现实可能性，因此，我国立法应规定网络连接服务提供商（IAP）不需为第三方的行为承担民事或刑事责任；网络信息服务提供商（ICP）应当承担担保责任；对明知或已被通知他人利用其计算机信息系统实施犯罪的，应当承担相应的刑事责

① 郑成思、薛红：《国际上电子商务立法状况》，《科技与法律》，2000 年第 3 期。

任。

电子商务关联犯罪包含多种具体犯罪，而且随着电子商务的发展将继续增加。这些犯罪带来的有些新法律问题可以在现行刑事法律体系内解决，而有些犯罪在适用法律时则面临困难甚至无法可依。本章将对电子商务关联犯罪中频繁发生、法律问题比较突出的两种犯罪进行研究。

第二节 电子商务领域的盗窃犯罪

一、电子商务领域盗窃犯罪的发展现状

计算机、网络等信息技术给现代社会以深刻的影响，在电信、金融等两个领域表现得更加突出。在电信业，不仅固定电话、移动电话、传呼和卫星通信等业务都实现了计算机、网络控制管理，新发展起来的互联网络业务完全建立在计算机和网络技术基础上。在金融业，计算机、网络技术推动了金融电子化进程，尤其突出的是信用卡等与电子资金相关业务迅速发展起来。目前我国信用卡服务范围已经由各家银行各自独立的城域范围发展到到全国范围内“金融联”系统，信用卡功能也越来越强，逐步实现了全国范围内的取款、消费、转账等功能，金融电子化加快了资金流动速度，通过电子资金过户系统，能够在极短的时间内完成跨地域的资金流动。另外，金融电子化还创生了各种各样的电子现金（e-cash）、电子钱包等电子化金融工具，并在社会上逐步推广和应用起来。

电子商务时代，电子资金、电子信息等新形式的财富产生并得到广泛的应用，上网浏览信息、购物等新的社会活动不断产生，并日益成为人们日常工作、生活中的一部分，与此相关的盗窃犯罪活动也随之衍生并日益严重起来。电子商务领域盗窃犯罪与传统的盗窃犯罪不同，主要表现为以下几种行为方式：

1. 利用技术手段非法获取他人电信号码并非法使用

根据被非法侵占的电信服务种类的不同，这类行为可分为非法获取使用固定电话电信号码和非法获取使用移动电话电信号码两种。

前者多表现为利用计算机、网络技术非法侵入控制通信服务的计算机信息系统窃取电信号码，然后使用该电信号码的行为。例如，1996 年美国一名黑客破解英国伦敦警察厅的计算机系统的入网密码，偷打国际长途电话，给英国警察当局造成了总额达 100 多万英镑的损失。

与前者不同，复制移动电话号码则是使用电子扫描仪和数字分析仪，乘被害人在使用移动电话通话时，截取通信信号，破解通信频率或者通信号码并使用的行为。在美国仅 1995 年盗用移动电话号码的犯罪就发案七十多万起，从而给电话公司造成的经济损失高达 6.5 亿美元①。

2. 盗用个人的电信账号和密码

随着电信企业安全防护意识和措施的加强，电信企业给网络用户的初始密码各不相同，在一定程度上减小了被盗用电信账号的可能性。但是，如果用户密码不慎被他人知道，或者用户的密码设置过于简单，则可能发生盗用电信服务的事件。例如南京郑某于 2000 年 1 月 28 日到电信局申请安装家庭电话，同时获赠一张 9989 电话卡，2 月 8 日他打了两个市内电话后，查询发现卡上竟已少了六十多元，两天后，再次查询，尽管家人没有再用此卡，可金额却又少了许多。相类似的投诉不仅涉及到 9989 电话卡，还有 300 电话卡②。

---

① 高凤仪：《美着力打击盗用移动电话号码犯罪活动》，《光明日报》，1996 年 6 月 19 日。

② 王文坚、李国葆：《电话卡为何频频被盗打》，《扬子晚报》，2000 年 3 月 22 日。

3. 盗用公用信息网络服务

这类行为有两种形式，一种是盗用合法网络用户电信服务，另一种是盗用电信企业电信服务。网络用户在使用互联网络前，必须向电信企业申请网络账号，用户凭借网络账号和密码进入互联网络，而在有些地区，用户申请到网络账号后使用统一的密码入网，再把这一密码改为个人所需的密码。由于一些网络用户对互联网络不熟悉，且缺乏足够的警惕性，给他人窃取密码并盗用网络造成可乘之机。如 1998 年 2 月，江苏省南京市的何某在办理互联网络开户后，由于听错账号密码，以致一直没有能够使用互联网络，当然也没有按电信部门的要求及时修改初始密码。有人得知何某的用户名后，使用电信部门的统一初始密码进入了信息互联网络，而后这一账号密码被透露给其他 13 人，使这些人故意非法使用他人账号密码，给何某带来五千九百余元的经济损失①。

盗用电信企业电信服务，通常是非法侵入电信企业的计算机管理信息系统，非法设立、使用电信账号享用电信服务。如 1998 年 8 月，上海市杨某利用计算机、网络技术非法侵入上海某信息网络，并在该信息服务网络上私自开设了 4 个非法网络用户账号，这些非法账号被查出时，有的使用记录长达二千多个小时。按照上海信息费每分钟 0.12 元计算，盗窃信息使用费共计 1.6 万余元。而且，杨某还把制作非法账号和密码的方法传授给他人，给该市的信息网络安全造成了极大威胁②。

4. 利用计算机盗窃金融机构的电子货币

盗窃电子货币的行为表现为，使用计算机技术修改金融计算

① 朱进：《南京查获一起因特网上盗窃案》，《光明日报》，1998 年 6 月 6 日。

② 《“黑客”攻击上海网，警方以“破坏计算机信息系统”的罪名逮捕嫌疑犯杨某》，《报刊文摘》，1998 年 9 月 17 日。

机管理系统中合法客户的存款账目，向其他账号转移资金来窃取金融机构的资金。例如前面提及的郝氏兄弟盗窃金融机构案。

5. 非法充值电信卡并使用

随着电信业务的扩展，凭卡消费日益为各种电信业务所采用，如移动电话的充值卡业务、固定电话的 IC 卡业务、200 卡、300 卡等。与此同时，非法充值电信卡犯罪也发展起来，他们回收用完的电信卡，利用技术手段非法充值后，或者自己使用，或者低价卖给他人，给电信企业造成巨额经济损失。

二、盗窃罪的概念和犯罪构成

我国打击电子商务领域盗窃犯罪的刑事法律条文主要是《刑法》第 287 条、第 264 条、第 265 条、第 196 条第 3 款、第 253 条第 2 款。《刑法》第 287 条关于“利用计算机实施……盗窃……或者其他犯罪的，依照本法有关规定定罪处罚”的规定和《关于维护互联网安全的决定》，是认定利用电子商务领域盗窃犯罪的法律前提，行为人在电子商务活动中实施盗窃犯罪的，依据我国《刑法》第 264 条、第 265 条、第 196 条第 3 款、第 253 条第 2 款规定定罪量刑。此外，《最高人民法院关于审理扰乱电信市场管理秩序案件具体应用法律若干问题的解释》第 7 条和第 8 条规定，“将电信卡非法充值后使用，造成电信资费损失数额较大的”和“盗用他人公共信息网络上网账号、密码上网，造成他人电信资费损失数额较大的”，以盗窃罪定罪量刑。

盗窃罪，是指以非法占有为目的，盗窃公私财物数额较大、多次盗窃，或者以牟利为目的盗接他人通信线路、复制他人电信号码，或者明知是盗接、复制的电信设备、设施而使用，具有法定数额或者法定情节的行为。本罪分为基本罪和派生的重罪、更重罪和最重罪四个构成类型。

（一）基本罪的构成要件

本罪的基本罪是一般主体、犯罪故意、选择性危害行为、特

殊犯罪后果、特殊犯罪对象和被害法益 6 个要件构成，具体内容和形式如下：

1. 一般主体

本罪的主体是一般主体，指年满 16 周岁具有刑事责任的自然人。

2. 犯罪故意

本罪在主观方面表现为直接故意。直接故意的一般犯罪目的是，明知自己在实施盗窃行为，会严重侵害他人财产权，而希望这种结果发生的心理态度。除了一般犯罪目的外，本罪还要求有非法占有公私财物的特殊犯罪目的，如果是盗接他人通信线路、复制他人电信号码或者明知是盗接、复制的电信设备、设施而使用的，必须以牟利为目的。

3. 选择性危害行为

本罪的危害行为表现为 6 种选择性行为方式：一是以非法占有为目的盗窃公私财物的行为；二是以非法占有为目的多次实施盗窃行为；三是以牟利为目的盗接他人通信线路、复制他人电信号码，或者明知是盗接、复制的电信设备、设施而使用的行为；四是盗窃信用卡并且使用的行为；五是将电信卡非法充值后使用；六是盗用他人公共信息网络上网账号、密码上网。这 6 个要件只要具备其中一项，都可能构成盗窃罪。上述 6 种选择性行为的共同特点都是“秘密窃取”。“秘密窃取”是盗窃行为的基本形式，也是本罪与其他侵犯财产罪相区别的主要特征。所谓秘密窃取，是指行为人必须采取自认为不被财物所有人或保管人知道的方法，将财物取走，至于客观上是否为被害人所知或觉察，不影响本罪的成立。如果在行窃时被人发觉进而公然夺取或使用暴力，盗窃行为就转化为抢夺行为或抢劫行为。秘密窃取的方法是多种多样的，通常表现为撬门破锁、翻墙入院、扒窃掏包、顺手牵羊等。在传统盗窃行为方式中，盗窃行为的实施将导致被窃财物在空间上发生位置移动，但在电子商务时代，可以在不取走原

物的情况下达到窃取经济利益的目的。如利用计算机等高科技设备，通过破解密码、篡改数据、下载信息、盗接通信线路、复制电信号码等手段，就能盗窃电子货币、有价计算机数据（如计算机软件）、电信服务。

4．特殊犯罪后果

本罪的特殊犯罪后果是盗窃公私财物“数额较大”。根据最高人民法院1998年3月10日发布的《关于审理盗窃案件具体应用法律若干问题的解释》的规定，所谓数额较大，是指个人盗窃公私财物价值人民币500～2 000元以上。各省、自治区、直辖市高级人民法院可根据本地区经济发展状况，并考虑社会治安状况，在这一数额幅度内确定本地区的具体数额标准，并报最高人民法院备案。“数额较大”是成立本罪的法定选择要件。如果盗窃数额不是较大，又不符合其他选择要件的，不能认为是犯罪。上述司法解释又规定：盗窃公私财物接近“数额较大”的起点，具有下列情形之一的，可以追究刑事责任：(1）以破坏性手段盗窃造成公私财产损失的；(2）盗窃残疾人、孤寡老人或者丧失劳动能力人的财物的；(3）造成严重后果或者具有其他恶劣情节的。

行为人没有盗窃数额较大财物，而有“多次盗窃”情节的，也可能构成本罪。根据上述司法解释，所谓多次盗窃，“是指一年内入户盗窃或者在公共场所扒窃三次以上的”行为。这一规定对“多次盗窃”作了三点限制：(1）次数上的限制。盗窃必须在三次以上才能算多次，三次以上包括本数在内。(2）时间上的限制。必须是在一年以内实施三次以上盗窃。(3）地点的限制。只限于入户盗窃和在公共场所扒窃。这里要指出的是，多次盗窃的前提是盗窃的数额没有达到“数额较大”的起点，由于行为人在一年内这个不算很长的时间内入户或在公共场所行窃三次以上，主观恶性较大，所以法律才将这种“反复危害行为”规定为犯罪。鉴于现行刑法已经取消了“惯窃”，因此，凡是多次盗窃数

额没有达到“数额较大”的起点，又不符合上述三个限制条件的，不能以犯罪论处。如果行为人“多次盗窃”，最后一次盗窃构成犯罪，其在一年以内的前几次盗窃数额累计达到“数额巨大或者有其他严重情节”、“数额特别巨大或者有其他特别严重情节”等条件的，应当分别认定为盗窃罪的重罪、更重罪或极重罪。

以牟利为目的盗接他人通信线路、复制他人电信号码或者明知是盗接、复制的电信设备、设施而使用的行为是本罪的选择性行为方式。成立本选择要件法律在主观方面有特别要求，即必须是法律规定的“以牟利为目的”或者“明知”。根据前述司法解释，所谓“以牟利为目的”，是指为了出售、出租、自用、转让等谋取经济利益的行为。如果行为人盗接他人通信线路、复制他人电信号码不是“以牟利为目的”，或者不知是盗接、复制的电信设备、设施而使用的，不能认为是犯罪。行为人在一年内多次实施本选择要件的行为，如果犯罪数额累计达到“数额巨大或者有其他严重情节”、“数额特别巨大或者有其他特别严重情节”的，应当分别认定为盗窃罪的重罪或更重罪。所谓“明知”，是指认识到所使用的电信设备、设施来源不正当。

5. 特殊犯罪对象

本罪的犯罪对象是公私财物，包括国有财产、劳动群众集体所有财产、公民个人所有财产、多种所有制经济成分混合组成的法人、非法人的社团的财物。作为本罪对象的财物，必须是具有一定经济价值且可为人力所控制、支配、转移、使用的财物，包括有形财物、无形财物和有价服务。根据《刑法》第196条第3款、第210条第1款和有关司法解释，本罪侵犯的对象主要有如下几种：(1)动产（包括金融资金、现款、物品等）、不动产上可与之分离的附属物（如房屋上的门窗）、文物等；(2)有价支付凭证、有价证券、有价票证、信用卡等；(3)电力、煤气、天然气等；(4)通信线路、电信号码、有价计算机数据等；(5)增

值税专用发票、可以用于骗取出口退税、抵扣税款的其他发票等等。不能为人力所控制、支配的财物，不能成为盗窃罪的对象。此外，盗窃枪支、弹药、爆炸物、国家秘密、商业秘密、公文、证件、印章、尸体等行为，因其侵犯的客体不同，刑法另规定为其他罪名，所以不能认定为本罪。

6. 被害法益

本罪侵犯的法益是公私财产所有权。

（二）重罪的构成要件

本罪的重罪构成要件，是指罪行在符合基本罪构成要件的基础上，“盗窃公私财物数额巨大或者有其他严重情节”的行为。盗窃“数额巨大”和“其他严重情节”，是构成重罪的两个选择要件，只要具备其中一项，重罪便可成立。“数额巨大”和“其他严重情节”，前述司法解释有明确规定。

（三）更重罪的构成要件

本罪的更重罪构成要件，是指罪行在符合基本罪构成要件的基础上，“盗窃公私财物数额特别巨大或者有其他特别严重情节”的行为。盗窃“数额特别巨大”和“其他特别严重情节”是构成重罪的两个选择要件，只要具备其中一个，更重罪便可成立。“数额特别巨大”和“其他特别严重情节”，前述司法解释有明确规定。

（四）最重罪的构成要件

本罪的最重罪构成要件，是指罪行在符合基本罪构成要件的基础上，有下列情形之一的行为：（1）盗窃金融机构，数额特别巨大；（2）盗窃珍贵文物，有严重情节的。根据前述司法解释，“盗窃金融机构”是指盗窃金融机构的经营资金（应当包括电子资金）、有价证券和客户的资金等，如储户的存款、债券、其他款物，企业的结算资金、股票，但不包括盗窃金融机构的办公用品、交通工具等财物的行为；“数额特别巨大”是指人民币在3万～10万元以上的。“盗窃珍贵文物，情节严重”，主要是指盗

窃国家一级文物后造成损毁、流失，无法追回；盗窃国家二级文物三件以上或者盗窃国家一级文物一件以上，并具有下列情形之一的行为：(1) 犯罪集团的首要分子或者共同犯罪中情节严重的主犯；(2) 流窜作案危害严重的；(3) 累犯；(4) 造成其他重大损失的。

根据我国《刑法》第 287 条、第 264 条、第 265 条、第 196 条第 3 款和《关于审理扰乱电信市场管理秩序案件具体应用法律若干问题的解释》的规定，犯本罪基本罪的，处 3 年以下有期徒刑或者管制，并处或者单处罚金；犯本罪重罪的，处 3 年以上 10 年以下有期徒刑，并处罚金；犯本罪更重罪的，处 10 年以上有期徒刑或者无期徒刑，并处罚金或者没收财产；犯本罪最重罪的，处无期徒刑或者死刑，并处没收财产。盗窃未遂，情节严重，如以数额巨大的财物为盗窃目标的，以盗窃罪（未遂）定罪量刑。

三、对几类典型犯罪行为的审判处理意见

（一）关于盗用合法用户的有价电信服务的问题

《刑法》第 264 条规定，以牟利为目的，盗接他人通信线路、复制他人电信号码或者明知是盗接、复制的电信设备、设施而使用的，以盗窃罪论处。但是，利用计算机技术盗窃其他有价电信服务能否构成本罪呢？对此法学界是有争论的。作者认为，以牟利为目的，盗接他人通信线路、复制他人电信号码或者明知是盗接、复制的电信设备、设施而使用的行为，从本质上看就是盗窃他人的有价电信服务。而利用计算机技术破解他人网络账号和密码并使用的，也属于非法获取他人付费电信服务的行为，应当属于《刑法》第 264 条规定的盗窃行为。《关于审理扰乱电信市场管理秩序案件具体应用法律若干问题的解释》第 8 条规定，“盗用他人公共信息网络上网账号、密码上网，造成他人电信资费损失数额较大的”，以盗窃罪定罪量刑，既然窃取他人付费的公用

信息网络电信服务以盗窃罪论处，那么其他有价电信服务如200卡、300卡电话服务等也应该属于盗窃罪的犯罪对象。

（二）关于盗窃经营单位的有价信息服务问题

前面提到上海杨某盗用电信服务案，作者认为此案应当以盗窃罪论处，理由如下：(1) 经营计算机信息服务的企业，要投入大量的资金建设网络、购买或租用场地、购置机器设备设施、开发信息软件、聘用专业人员进行管理和维护等，经营成本是相当高的，这些投入必须通过有偿服务而获取回报。如果盗窃信息服务不构成犯罪的话，将严重地影响我国信息产业的发展。(2) 电信服务是一种特殊的商品，这种商品的使用意味着一定设备资源被占有和损耗。杨某非法使用电信服务，导致电信企业的计算机信息系统及网络资源被无偿消耗，设备损耗增加，属于盗窃电信服务这种特殊商品的行为。(3) 信息经营企业对使用计算机信息服务有明确、公开的收费标准，并接受物价部门的监管。因此，“没有付费就上网”和无偿窃取有价信息的行为与盗窃商店商品行为没有本质上的区别。

（三）关于盗窃电子货币的问题

前面提到郝氏兄弟盗窃金融机构案。这一案件中包含两个问题：一个是电子资金能否成为盗窃罪的犯罪对象；另一个是这类案件中的犯罪既遂与未完成形态问题。

1. 电子资金能否成为盗窃罪的犯罪对象

有学者认为，传统的财产犯罪的犯罪对象一般是普通的实物和货币，包括动产和不动产，而计算机里的数字能否在刑法上认同为财产，尚无明文规定，这给处罚这类犯罪增加了（类推的）风险①。电子货币表现为电子结算系统中的计算机数据，计算机数据形式的电子资金能否成为盗窃罪的犯罪对象，成为学者们讨

① 赵秉志主编：《新千年刑法热点问题研究与适用》，中国检察出版社2001年版，第489～497页。

论的一个问题。

作者认为，电子货币是盗窃罪的一种特殊犯罪对象。这是因为：

（1）电子货币是金融电子化创造的新的财富形式，在电子商务应用中是主要的货币形式。

（2）任何犯罪都不是静止的，而是伴随社会的发展而发展的。盗窃罪犯罪对象的范围随着社会的发展不断扩大，由最初的普通实物和货币扩展到有价支付凭证、有价证券、有价票证、信用卡、电力、煤气、天然气、通信服务、电信号码、有价计算机数据。电子货币是社会信息化、金融电子化和电子商务发展的产物，电子资金成为盗窃罪的犯罪对象是这类犯罪发展的必然结果。

（3）电子货币不同于盗窃罪的其他普通犯罪对象，具有控制管理的多主体性、无形性和流通环境的特定性，因此，与其相关的法律问题和盗窃罪的普通犯罪对象有较大差别。正是由于这种特殊性，在司法实践和刑法理论上，不可用处理盗窃传统“财物”的思维方式来处理盗窃电子货币的问题，而应当从社会发展的实际情况出发，科学认定盗窃罪的犯罪对象。

2．犯罪既遂与未完成形态问题

对于这类窃取电子资金的行为，有人认为，盗窃电子货币，如果只是在电子资金过户系统中，将电子资金划拨到自己的账户上时，不构成盗窃行为，理由是实际的资金仍然处于银行的控制之下，只有行为人实际取走现金时，才构成犯罪。还有人认为应该按照失控加控制的标准来认定是否构成犯罪和犯罪的未完成形态，即盗窃电子货币的，如果被盗的电子资金已经脱离被害人账户，由于行为人意志以外的原因，未能进入行为人账户的，属于犯罪未遂；如果行为人账户中已经收到被盗资金的，构成既遂。

作者认为，以上两种观点都值得商榷。

（1）行为人通过电子资金过户系统，将他人的电子资金调拨

进自己的账户中，被害人账户上的资金相应减少，意味着这笔资金已经脱离被害人的控制。如果犯罪不被及时发现而将这笔资金冻结的话，行为人可能提取现金，或者在网络上消费如网上购物和其他交易，这种盗划他人电子资金的行为即使没有进一步使用或者转移，也已经具有严重的社会危害性，应当用刑罚手段予以惩治。此外，《关于审理盗窃案件具体应用法律若干问题的解释》第1条第2项规定，“盗窃未遂，情节严重，如以数额巨大的财物……为盗窃目标的，应当定罪处罚”，因此，将他人数额巨大的电子资金转入自己账户而未来得及使用、转移的行为，也构成犯罪，属于盗窃罪未遂。第一种观点把是否实际提取钱款作为能否构成犯罪的标准是错误的。

（2）电子资金过户系统是一种功能强大的金融电子化系统，既能使电子资金快速流动，也能实现电子资金的良好管理。如储户发觉资金被盗，经及时报警、挂失，可以对被盗资金流入的账户进行冻结，使犯罪人无法使用或者转移被盗资金，从而挽回损失、遏制犯罪。由于电子资金过户系统的电子资金处于金融企业和账户所有人的共同控制下，即使犯罪人将电子资金转进自己的账户，也不能认为犯罪人完全控制了资金。在这种情况下，由于犯罪人意志以外的因素，而未能进一步处置已经进入自己账户的资金的，应该以盗窃罪未遂论处。

（3）行为人将已经进入自己账户的被盗资金，作进一步转移、提取现金，或者在网上消费的，表明了行为人有非法占有他人财产的犯罪目的，并且已经实际控制了被盗资金，应该构成盗窃罪既遂。如果行为人在将他人资金转入自己账户后悔悟，在罪行暴露前自动将电子资金归还被害人的，表明行为人已经自动放弃犯罪并有效防止犯罪结果的发生，故应该以犯罪中止论处。这符合我国区别对待和鼓励悔罪的刑事政策。

（四）关于非法充值电信卡并使用的问题

非法充值电信卡并使用，造成电信资费损失数额较大的，以

盗窃罪定罪量刑。本罪是结果犯，只有行为人的行为造成电信资费损失数额较大的，才构成盗窃罪既遂。行为人非法充值电信卡并使用的，可以分为两种情形：其一是行为人非法充值电信卡并且自己使用的；其二是行为人非法充值电信卡，卖给他人使用的。对于前者，由于行为人非法充值电信卡并使用的行为，造成电信资费损失数额较大的，以盗窃罪定罪量刑；对于后者，非法充值电信卡的行为人和接受并使用电信卡的人构成共同犯罪，属于共同实行犯。如果造成电信资费损失较大的，非法充值电信卡的行为人和使用这种电信卡的行为人以盗窃罪共同犯罪定罪量刑。对于非法充值电信卡的行为人，如果行为人非法充值的电信卡资费数额巨大，即使没有使用造成较大电信资费损失，或者转手给他人使用而没有造成较大电信资费损失。对于这种情况，《关于审理盗窃案件具体应用法律若干问题的解释》第 1 条第2项规定，“盗窃未遂，情节严重，如以数额巨大的财物……为盗窃目标的，应当定罪处罚”，因此，应以盗窃罪（未遂）论处。

四、对电子商务领域盗窃罪的立法建议

《刑法》第 265 条规定，以牟利为目的，盗接他人通信线路、复制他人电信号码或者明知是盗接、复制的电信号码的电信设备、设施而使用的，依照本法第 264 条的规定定罪处罚。《关于审理扰乱电信市场管理秩序案件具体应用法律若干问题的解释》第 7 条规定，将电信卡非法充值后使用，造成电信资费损失数额较大的，依照刑法第 264 条的规定，以盗窃罪定罪处罚，第 8 条规定，盗用他人公共信息网络上网账号、密码上网，造成他人电信资费损失数额较大的，依照刑法第 264 条的规定，以盗窃罪定罪处罚。以上法律规定和司法解释是处理电信领域盗窃犯罪的法律根据。但是，司法实践中出现的新问题暴露出上述法律、司法解释的缺陷。

1. 虚设并使用电信号码的属于盗窃行为

对于杨某盗用电信服务案，司法界和理论界有多种意见，鉴于前述理由，作者认为应当以盗窃罪论处。但是，我国《刑法》第265条只规定了电信领域盗窃犯罪的三种行为方式，对虚设并使用电信号码的行为没有法律规定。而且，这种行为也不能纳入复制他人电信号码一类，因为“复制”是事先存在而再创造一个，虚设是非法地、从无到有地创造。因此，建议修改本条，增设虚设并使用电信号码为盗窃行为。

2.《关于审理扰乱电信市场管理秩序案件具体应用法律若干问题的解释》第7条规定了新的犯罪行为，超出了司法解释的权限

一种行为是否构成犯罪，必须由刑法等法律明确规定，法律没有明文规定为犯罪行为的，不得定罪处罚。司法解释是最高人民法院、最高人民检察院对司法工作中具体应用刑法规范所作的解释，不得越权规定新的犯罪行为。《关于审理扰乱电信市场管理秩序案件具体应用法律若干问题的解释》第7条和第8条规定了电信领域的两种犯罪行为处理办法。第8条规定的盗用他人公共信息网络上网账号、密码上网的行为，基本上符合《刑法》第265条规定的复制他人电信号码并使用的行为，而第7条规定非法充值电信卡并使用的行为按盗窃罪定罪处罚，则于法无据，有越权解释的嫌疑。第7条规定的将电信卡非法充值后使用的行为，是指增加电信卡电信资费数额，如修补用于打电话的磁卡、IC卡，使其电信资费数额超过实际数，或者将没有余额的电信卡修改成可以使用的电信卡等情况，并使用这些非法充值后的电信卡。这种行为不属于《刑法》第265条规定的任何一种行为方式，如果严格依照刑法，该行为不能按盗窃罪定罪处罚。实际上，非法充值电信卡并使用的行为应该属于盗窃罪，只是由于我国刑法立法的滞后才导致法律上的疏漏，但是，处理这一问题不能以司法解释代替刑事立法，建议修改《刑法》第265条，将非

法充值电信卡并使用的行为规定为盗窃罪。

3.《刑法》第253条第2款规定邮政工作人员私自开拆或者隐匿、毁弃邮件、电报而窃取财物的，以盗窃罪论处，那么电信企业工作人员私自开拆、隐匿、毁弃他人电子邮件，并窃取计算机数据类产品的，也应该以盗窃罪论处。

我国近年来，对邮电行业改革很大，首先将邮电行业分解为邮政和电信两个行业，进而对电信业作了进一步的分解，互联网络数据通信服务业迅速发展起来，其中电子邮件业务与普通邮政信函业务形成激烈的竞争。电子邮件业务不仅可以用于发送邮件，而且可以用于中小规模的计算机数据类商品的传送，其快捷、廉价是邮政业务所无法比拟的。但是，不排除电信服务企业工作人员利用工作便利，私自非法获取、隐匿、毁弃他人电子邮件及附属计算机文件的情况，如果附属的计算机文件是有价计算机数据类商品，还可能窃为己有。对于这种利用互联网络侵犯公民通信自由权利和财产权利的行为，如果按照《刑法》第252条以侵犯通信自由罪处罚，不能正确反映这种行为的实际情况。

《刑法》第253条规定，邮政工作人员私自开拆、隐匿、毁弃他人邮件而窃取财物的，按照盗窃罪定罪处罚。邮政、电信企业工作人员主体身份相似，客观方面危害行为相似，侵害的法益相同，既然前者情况可以按照盗窃罪定罪处罚，后者也应该以盗窃罪定罪处罚。建议将《刑法》第253条修改为：

“邮政、电信行业工作人员私自开拆、隐匿、毁弃他人邮件的，处2年以下有期徒刑或者拘役。

犯前款罪而窃取财物的，依照本法第264条的规定定罪，从重处罚。”

第三节　电子商务领域制作、贩卖、传播淫秽物品的犯罪

一、电子商务领域制作、贩卖、传播淫秽物品犯罪的发展现状

“色情”一词源于希腊文 Porne，意味着足以挑逗起顾客性欲的题材。国外有关色情作品的立法存在两个问题，一是判断色情的标准，一是色情作品是否对社会有害，各国对这两个问题的不同态度，导致这些国家立法和司法上的差异，例如丹麦允许出版和销售色情作品，而德国、奥地利和瑞士的态度比较谨慎，除儿童色情作品被严禁外，消费对象为成年人的色情作品一般不属于政府严禁的范围①。我国《刑法》规定了制作、贩卖、传播淫秽物品罪（刑法规定的淫秽物品包含色情作品），对于制作、贩卖、传播淫秽物品的，无论淫秽物品是否涉及儿童，以及消费者是否为成年人，都可能构成犯罪。在传统的色情作品相关犯罪中，色情作品表现为文字、绘画、相片和电影形式，进入 20 世纪 90 年代后，借助于计算机、网络和多媒体技术，色情作品以电子数据形式在互联网上迅速传播起来。互联网空间不同于陆地疆域，网上电子数据信息能迅速流转于世界各国，任何国家都难以有效控制。目前互联网已经成为色情服务行业最重要的“行销”平台之一，美国一项新的研究调查报告预测，在未来五年内色情网站的营业收入将会出现三倍以上的增长，比其他种类的互联网信息提供业增长率高出许多。Datamonitor 公司的研究调查报告显示，仅 1999 年一年，网民花费在成人网站上总计 9.7 亿

① 徐久生著：《德语国家的犯罪学研究》，中国法制出版社 1999 年版，第 316～320 页。

美元，5年内这个金额将增长到30亿美元①。巨额的网络淫秽信息交易背后，是给社会道德风尚和未成年人成长教育造成的恶劣影响。我国一项调查显示，在参与调查的3 000名大中学生中，曾光顾淫秽信息网站的占46%②，淫秽信息网站传播的内容多是畸形、变态的性行为，严重毒害青少年，容易导致青少年性犯罪的发生。

这些在互联网络上贩卖、传播的淫秽物品大多为色情图片和文字，有的还提供色情影像、动画和声音，提供这些色情物品的行为人大多是以收取信息服务费，或赚取广告资助费为目的。目前在互联网络上制作、复制、出版、贩卖、传播淫秽物品的犯罪主要有以下几种行为方式：

1. 设立色情淫秽信息网站，收取色情信息服务费

这类行为表现为建立色情淫秽信息网站，提供各种形式的色情淫秽信息，如色情淫秽图片、文字、声音、动画、影像等。在网络用户浏览部分免费提供色情信息后，网站要求用户注册加入色情网站成为会员，并要求使用信用卡等网上结算手段支付其他色情淫秽信息费用。由于我国《刑法》规定了制作、贩卖、传播淫秽物品的犯罪，禁止制作、查阅、复制和传播淫秽色情信息，所以淫秽色情信息商业网站往往不设在我国境内，多设在允许经营色情信息服务的国家或者地区，而且适应营业地所在国的法律，网站上的色情淫秽信息的类型也有所不同，在美国等国家，网上制作、复制、出版、贩卖、传播儿童色情淫秽物品的行为构成违法，而销售成年人色情淫秽信息则合法；在日本销售色情淫

① 《色情网站继续热销 五年内突破三十亿美金》，《电脑日报》，2000年5月29日。

② 《近半学生曾光顾色情网站：中国学生泡网吧情况堪忧》，http://www.hsm.com.cn/2000年7月26日。

秽信息甚至是儿童色情信息也不构成违法①。

2. 设立淫秽色情信息个人主页，借以发布他人的广告，赚取广告资助费

我国境内在互联网络上制作、复制、出版、贩卖、传播的淫秽色情物品犯罪，主要表现为设立淫秽色情信息个人主页。目前，新浪、雅虎等大大小小商业网站为吸引网络用户关注其网站，提供免费个人主页服务，一些国内外企业为扩大企业和产品的影响，对在个人主页上帮助其做广告的个人主页提供广告费资助，根据网络用户点击个人主页的次数支付广告费。为吸引更多的用户访问其个人主页赚取更多的广告费，一些行为人在个人主页上加入大量的淫秽色情图片、文字、声音、动画、影像等信息，或者嵌入指向淫秽色情信息或者境外淫秽色情网站的链接。例如 1999 年 4 月，一名为“性爱森林”的个人主页出现在云南公众多媒体通信网上，其中非法刊登了 22 篇国家明令禁止的淫秽读物。经云南警方调查，该主页系四川某机关职工杨某于 1998 年 10 月建立，刊登淫秽读物是为吸引网友前往访问该主页以赚取网络广告费，被查封前短短的两个月中，该主页累计访问人次达 11 万②。近年来我国个人主页的数量一直在快速增长，到目前为止，我国已经有 1 000 家网站提供个人主页服务，其中最大的网站有近 100 万的个人主页，传播淫秽内容的个人主页占有相当一部分，而且数量呈上升趋势。

3. 不以营利为目的，在互联网络传播淫秽物品

这类行为人不具有营利的目的，往往出于畸形的兴趣爱好，在互联网络上的公共交流区如电子公告栏、聊天室等处张贴淫秽

---

① 《日本：全球因特网上儿童色情的大本营》，《电脑日报》，2000 年 5 月 11 日。

② 《“性爱森林”想赚取网络广告费　云南警方依法查封》，《电脑日报》，1999 年 7 月 23 日。

色情信息。例如 1998 年 2 月，廖某在深圳视聆通网友沙龙栏目上公然散布内容极其庸俗下流的淫秽文章，大肆描述个人性爱好及性经验，还在文末发布性广告并留下传呼号码，影响很坏。经讯问，廖某交待他在澳大利亚留学期间认识了几位香港朋友，他们来深圳探望他时，提议制作一个色情淫秽的广告粘贴上网，看看会有什么反应。廖某当即表示同意，并亲自操作电脑，在深圳 online.net 网上的公告栏上发布。

二、制作、贩卖、传播淫秽物品犯罪的概念和犯罪构成

我国严禁在互联网络上制作、复制、出版、贩卖、传播淫秽物品（包括成人淫秽色情物品和儿童淫秽色情物品）。《计算机信息网络国际联网管理暂行规定》第 13 条规定，“从事国际联网业务的单位和个人……不得制作、查阅、复制和传播妨碍社会治安的信息和淫秽色情等信息”；我国《刑法》还将在互联网络上制作、复制、出版、贩卖、传播淫秽物品的行为规定为犯罪。我国打击电子商务领域制作、复制、出版、贩卖、传播淫秽物品犯罪的刑事法律条文主要是《刑法》第 287 条、第 363 条第 1 款、第 364 条第 1 款、第 366 条。《刑法》第 287 条关于“利用计算机实施……盗窃……或者其他犯罪的，依照本法有关规定定罪处罚”的规定和《关于维护互联网安全的决定》，是认定利用电子商务领域制作、复制、出版、贩卖、传播淫秽物品犯罪的法律前提，行为人在电子商务活动中实施制作、复制、出版、贩卖、传播淫秽物品犯罪的，依据我国《刑法》第 363 条第 1 款、第 364 条第 1 款、第 366 条规定定罪量刑。

（一）制作、复制、出版、贩卖、传播淫秽物品牟利罪的概念和犯罪构成

制作、复制、出版、贩卖、传播淫秽物品牟利罪，是指以牟利为目的，制作、复制、出版、贩卖、传播淫秽物品，具有法定情节的行为。本罪是选择性罪名，在司法实践中应当根据具体案

情，选择适用或并合适用。本罪分为基本罪和派生的重罪、极重罪三个构成类型，它们的构成要件分述如下：

1. 基本罪的构成要件

本罪的基本罪是由选择主体、直接故意、选择性危害行为、特殊犯罪对象、被害法益 5 个要件构成，具体内容和形式如下：

(1) 选择主体

本罪的主体是选择主体，可以是个人也可以是单位。个人是一般主体，指年满 16 周岁具有刑事责任能力的自然人；犯本罪的单位法律未作限定，即任何单位均可构成。

(2) 直接故意

本罪在主观方面表现为直接故意，其直接故意的一般犯罪目的为明知是淫秽物品而予以制作、复制、出版、贩卖、传播的心理态度。除了一般犯罪故意外，本罪还必须以牟利为目的。至于是否获利或获利多少，不影响本罪的成立。

(3) 选择性危害行为

本罪在客观方面表现为制作、复制、出版、贩卖、传播淫秽物品五种行为，行为人只要实施其中一种行为，便可构成犯罪。所谓制作，是指生产、录制、摄制、编写、绘制、印刷等行为。所谓复制，是指通过翻印、复印、复录等方式对已有的淫秽物品进行仿造的行为。所谓出版，是指出版单位以合法名义编辑、印刷、发行淫秽书刊和音像制品的行为。所谓贩卖，是指批发、零售、倒卖等销售淫秽物品的行为。所谓传播，是指通过播放、出版、出借、邮寄、携带和网络传输等方式，致使淫秽物品流传扩散的行为。以上五种行为都可以利用计算机技术实施。

(4) 特殊犯罪对象

本罪的犯罪对象是淫秽物品。所谓淫秽物品，是指具体描绘性行为或者露骨宣扬色情的淫秽性的书刊、影片、录像带、录音带、图片以及其他淫秽物品。

(5) 被害法益

本罪侵犯的法益是国家对文化市场的管理秩序和社会善良的道德风尚。

从《刑法》第 363 条第 1 款的规定来看，本罪的基本罪是行为犯，只要行为人实施了制作、复制、出版、贩卖、传播淫秽物品的行为，除情节显著轻微、危害不大的以外，都构成犯罪。以上规定对犯罪数额、情节和危害后果不做要求，似乎显得过于严酷，为了弥补立法上的这一疏漏，最高人民法院 1998 年 12 月 11 日《关于审理非法出版物刑事案件具体应用法律若干问题的解释》第 8 条第 1 款，在犯罪数额上作了具体规定。

2. 重罪的构成要件

重罪构成要件是指符合基本罪构成要件的基础上，情节严重的行为。这里的“情节严重”，上述司法解释作了明确规定。

3. 极重罪的构成要件

极重罪是指在符合基本罪构成要件的基础上，情节特别严重的行为。所谓情节特别严重，根据上述司法解释第 8 条第 3 款规定，是指制作、复制、出版、贩卖、传播淫秽物品的犯罪数量（数额）达到成立重罪犯罪数量（数额）的 5 倍以上。

根据《刑法》第 287 条、第 363 条和第 366 条规定，个人利用计算机犯制作、复制、出版、贩卖、传播淫秽物品牟利基本罪的，处 3 年以下有期徒刑、拘役或者管制，并处罚金；犯重罪的，处 3 年以上 10 年以下有期徒刑，并处罚金；犯极重罪的，处 10 年以下有期徒刑或者无期徒刑，并处罚金或者没收财产。单位利用计算机犯本罪的，对单位判处罚金，并对直接负责的主管人员和其他责任人员，依照个人犯本罪的规定处罚。

（二）传播淫秽物品罪的概念和构成

传播淫秽物品罪，是指不以牟利为目的而传播淫秽物品，情节严重的行为。本罪是独立的构成类型，由选择主体、犯罪故意、单一危害行为、特殊犯罪对象、被害法益、酌定构成要件 6 个构成要件组成，其具体内容和形式分述如下：

1．选择主体

本罪的主体是选择主体，即个人和单位均可构成。实施本罪的个人是已满16周岁且具有刑事责任能力的自然人，实施本罪的单位法律未作限定。

2．犯罪故意

本罪在主观方面表现为故意，但不具有牟利的目的。至于行为人出于什么动机和其他目的，均不影响本罪的成立。

3．单一危害行为

本罪在客观上表现为传播淫秽的书刊、影片、图片、音像制品或者其他淫秽物品的行为。所谓传播，主要指出借、播放、展示、赠送、散发、交换、讲解等行为，但这种行为必须是针对公众实施或者公共场所实施。法律对传播的方法、手段未作限制。因而传播行为既可以公开实施，也可以是秘密进行。

4．特殊犯罪对象

本罪的犯罪对象是淫秽物品。

5．被害法益

本罪侵犯的法益是社会治安管理秩序和良好的社会风尚。

6．酌定构成要件

本罪除了符合上述构成要件外，还必须是“情节严重”的行为。所谓情节严重，根据上述司法解释第10条第1款规定，是指向他人传播淫秽的书刊、影片、影碟、图片等出版物达300～600人次以上或者造成恶劣社会影响的。

根据《刑法》第287条、第364条第1款和第4款、第366条规定，个人利用计算机犯传播淫秽物品罪的，处2年以下有期徒刑、拘役或者管制；单位利用计算机犯本罪的，对单位判处罚金，并对直接负责的主管人员和其他责任人员，依照个人犯本罪的规定处罚。向不满18周岁的未成年人传播淫秽物品的，从重处罚。

三、对几类典型犯罪行为的审判处理意见

（一）淫秽信息网站传播淫秽信息的问题

淫秽信息网站传播淫秽信息的方式，与传统的犯罪形式不同。除了采取向用户发送附有淫秽信息的电子邮件外，大多数淫秽信息网站通过互联网向访问者直接传送淫秽信息：网站经营者购置网络服务器，或者租用他人的网络服务器，建立淫秽信息网站，并在网站的计算机信息系统中放置淫秽信息文件。访问者访问淫秽信息网站、点击相关链接后，网站将链接的图片、声音或者影像文件发往访问者的计算机，发出的数据文件经由多个网络连接服务提供商的通信网络进入访问者的计算机，访问者的计算机启动相应的程序，将图片、声音或者影像展现出来。可见，这种传播方式不是网站单方的主动提供，而是由访问者发出请求，网站响应请求、提供信息的被动传播。这里涉及两个问题，一是将淫秽信息传输给访问者的网络连接服务提供商（以下简称网络服务商）是否承担帮助传播淫秽信息的刑事责任？二是淫秽信息网站的计算机系统发送淫秽信息，能否视为行为人传播淫秽信息的行为？

1. 网络服务商是否承担帮助传播淫秽信息的刑事责任

网络服务商是指提供互联网接入服务等网络通信服务的单位。互联网由众多计算机系统和通信网络组成，淫秽信息网站发出淫秽信息，必须通过通信网络才能抵达访问者的计算机。网络服务商完全能够认识到互联网上存在大量的淫秽信息网站，这些网站发出的淫秽信息需要通过通信网络传输，他们虽不希望但放任了淫秽信息在自己的通信网络中传输，因此，可以认为网络服务商主观上存在间接故意帮助传播淫秽信息的心态，客观上具有帮助传输的行为，符合我国刑法理论中片面帮助犯的特征。网络服务商是否承担帮助传播淫秽信息的刑事责任呢？作者认为，虽然网络服务商的行为符合帮助犯的条件，但不应承担法律责任。

这是因为：首先，在互联网中每时每刻都有亿兆的数据在流动，如果要求网络服务商对这些数据进行鉴别、控制，必然要牺牲网络服务的质量，甚至无法符合公众网络服务的要求。法律不要求行为人承担无法履行的责任，当然不应要求网络服务商承担鉴别、控制淫秽信息的责任。其次，法律作为社会上层建筑，应当有利于生产力的发展，如果要求网络服务商承担以上责任，必将阻碍网络服务的开展，进而阻碍以网络服务为基础的所有信息行业的发展，如电子商务、信息服务业等。最后，网络服务业几近于电话服务业，犯罪人借助电话实施犯罪行为，而法律不要求电话公司承担法律责任，那么，对网络服务商传输淫秽信息的行为同样不应追究法律责任。此外，从国际上的立法来看，目前制定了网络服务相关立法的国家如美国、欧盟、日本等国，都不要求网络服务商承担一般性的监控传输信息的义务①。我国加入WTO后，正致力于信息网络立法与国际接轨，在网络服务商的法律责任问题上，也应采纳国际上广泛接纳的立法原则。

2．淫秽信息网站的计算机系统发送淫秽信息，能否视为行为人传播淫秽信息的行为

淫秽信息网站设立后，网站的运作几乎完全由计算机管理控制，包括响应访问者的请求、向访问者的计算机发送淫秽信息等各种操作，完全由网站的计算机系统自动完成。计算机系统的动作能否视为其权利人的行为，直接影响到犯罪能否成立。作者认为，一般情况下，网站的计算机系统的动作应视为其权利人的行为，这是因为：首先，计算机控制管理的淫秽信息网站，虽然能代替人的一部分脑力和体力劳动，但并没有产生自由意志，淫秽信息网站服务器的一举一动都是其权利人意志的体现，或者得到其权利人认可，而且，正是权利人事先做出努力，才使网站具有

① 郑成思、薛红：《国际上电子商务立法状况》，《科技与法律》，2000年第3期。

以上自动运作功能，计算机系统的举动是权利人先行行为合乎因果关系的自然延伸，应当视为其权利人的行为。其次，虽然淫秽信息网站被动传播方式与传统形式不同，但它包含了主动传播动作，因此，这种传播方式仍属于故意传播淫秽信息的行为。再次，计算机系统既不是民法意义上的人，也不是刑法意义上的人，如果不把以上举动当作权利人的行为，那是谁实施了传播淫秽信息的行为呢？当然，如果网站经营者或者其他权利人不知情，技术人员私自放置淫秽信息并使其传播的，不是网站权利人而是技术人员实施了传播淫秽信息的行为。总之，设立淫秽信息网站传播淫秽信息的，构成故意传播淫秽信息的行为。

淫秽信息网站提供淫秽信息中，部分要求访问者付费，也有部分是免费的，但是这些免费淫秽信息是用来吸引访问者，促使其决心购买付费淫秽信息，因此，网站提供免费淫秽信息，同样有营利目的。如果网站向他人传播淫秽信息的次数达到法定数量的，构成传播淫秽物品牟利罪。

在淫秽信息网站问题上，各国立法不完全相同，大多数国家禁止传播儿童色情信息和向未成年人传播色情信息。我国刑法禁止传播包括儿童色情在内的各种淫秽信息，考虑到淫秽信息对未成年人成长的严重危害，《刑法》第 364 条规定，对向未满 18 周岁的未成年人传播淫秽物品的，以传播淫秽物品罪从重处罚。那么，淫秽信息网站是否不向未成年人传播淫秽信息呢？有部分淫秽信息网站在首页上放置警告文字和进入或者退出的选择链接。警告信息告诉访问者：该网站含有描述性的图片和内容，访问者如未年满 18 周岁，依据当地法律可能构成违法犯罪，访问者如果点击进入网站，表明自己熟悉当地法律，认可自己访问该网站的行为合法。网站的这种举动能否阻却向未成年人传播淫秽信息的责任呢？作者认为，从这类警告信息的性质来看，属于网站与访问者的约定，访问者如果点击进入链接，表明接受网站在警告中提出的要求，如放弃访问者的某些个人权利。但是，无论访问

者放弃了什么样的个人权利，都不能否定网站向他人传播淫秽信息的事实，也不能通过约定将向他人传播淫秽信息的行为“私了”，因为传播淫秽信息行为妨害的是社会管理秩序和社会道德风尚，而不仅仅是对某个人的危害，因此，淫秽信息网站设立警告的信息。不能阻却其向未成年人传播淫秽信息的责任，但是，这种警告可能对一部分未成年人起警惕作用，促使其放弃访问淫秽信息网站，与不设警告的淫秽信息网站相比，社会危害性要小一些，因此，可以把设立警告信息作为一个从轻处罚的情节。此外，我国《刑法》第 363 条规定的传播淫秽物品牟利罪，没有把对向未成年人传播淫秽物品作为从重处罚的情节，而《刑法》第 364 条规定的传播淫秽物品罪则有这样的规定。作者认为，以营利为目的传播淫秽物品，如果传播的对象是未成年人的，不仅危害社会管理秩序和社会道德风尚，还毒害了未成年人的成长，应当予以从重处罚，建议在《刑法》第 363 条增加一款，“向不满 18 周岁的未成年人贩卖、传播淫秽物品的，从重处罚。”

由于我国禁止淫秽信息的传播，付费淫秽信息的网站大多不设在我国境内，这些淫秽信息网站为了规避法律，往往在允许经营淫秽信息的国家或者地区设立网站计算机信息系统，利用互联网的广泛连通性，向世界各地传播淫秽信息。根据我国《刑法》第 6 条规定，犯罪的行为地或者结果地有一项发生在我国境内的，认为是在我国领域内犯罪，适用我国刑法，付费淫秽信息网站向我国境内传播淫秽信息的，可能构成传播淫秽物品牟利罪。但是，按照犯罪人所在国法律，行为人的这种行为可能属于合法行为，行为人如果不进入我国境内，要实现刑法的管辖十分困难。这是互联网应用给各国法律制度、文化传统带来的冲击，需要通过国际协商合作逐步解决。

（二）利用个人主页传播淫秽信息的问题

我国境内以营利为目的传播淫秽信息的，主要表现为利用个人主页传播淫秽信息。利用个人主页传播淫秽信息犯罪涉及两个

法律问题，网络服务器：一个是个人主页制作者将淫秽信息上载到商业网站的网络服务器，是否构成传播淫秽信息的行为。一个是商业网站客观上传播了淫秽信息，是否应承担法律责任。

1．个人主页制作者将淫秽信息上载到商业网站的网络服务器，是否构成传播淫秽信息的行为

制作、贩卖、传播淫秽物品罪侵犯的客体是社会主义道德风尚和国家文化市场管理制度，这类犯罪的传播行为是指将淫秽信息在社会上广为散播的行为①。这就是说，向特定个人转移淫秽物品的行为，不构成本罪的犯罪行为。在前述行为过程中，行为人只有转移淫秽信息至特定商业网站网络服务器的行为，没有向不特定的、多人传播淫秽信息，行为人的这种行为是否构成传播淫秽信息行为呢？作者认为，行为人如果向公共场所转移淫秽物品，例如在人来人往的车站广告栏上招贴淫秽图片的，仍然属于传播淫秽物品的行为，因为公共场所的淫秽图片可以被不特定的多人观看到。因此，如果认定行为人传播淫秽信息的目的地是公共场所，则可能构成传播淫秽物品的行为，反之则否。商业网站的计算机系统是否属于公共场所呢？这要区别对待，商业网站计算机存储设备的大部分区域只对特定人开放，这部分区域不能作为公共场所；而个人主页区域的信息，虽然它处于特定权利人的控制范围内，但由于即使是一般网络用户都能够访问、获取，因而应属于公共区域或者公共场所。因此，行为人向商业网站转移淫秽信息的行为构成传播淫秽信息的行为。此外，行为人制作带有淫秽信息的个人主页，其目的是吸引网民访问，赚取广告资助费，因此，应当认为行为人主观上具有传播淫秽信息的故意，并有营利目的。如果同时具备了传播淫秽物品牟利罪的其他要件，可能构成传播淫秽物品牟利罪。

① 高铭暄、马克昌主编：《刑法学》，北京大学出版社、高等教育出版社 2000 年版，第 604～607 页。

2．商业网站客观上传播了淫秽信息，是否应承担法律责任

商业网站属于互联网信息服务提供者（以下简称信息提供者），依照我国《互联网信息服务管理办法》规定，信息提供者应当向上网用户提供良好的服务，并保证所提供的信息内容合法，不得传播包括淫秽信息在内的九类信息，如发现其网站传输的信息明显属于九类信息之一的，应当立即停止传输，保存有关记录，并向国家有关机关报告。可见，法律没有免除商业网站传播不合法信息的法律责任，并且规定，在知晓存在不合法信息的情况下商业网站有停止传输的义务。因此，商业网站明知自己的计算机信息系统中存在淫秽信息的，必须立即停止传输，否则构成故意传播淫秽信息的行为。虽然传播他人制作的淫秽信息，不会给自己带来直接经济利益，但是，淫秽信息的传播扩大了该网站的影响，客观上有利于商业网站的经营利益，故意放纵淫秽信息传播的目的也正是追求这种非法利益，因此，应当认为其存在营利目的。如果同时满足其他构成要件的，可能构成传播淫秽物品牟利罪，还要追究网站经营人员或者直接责任人员的刑事责任。但是，如果商业网站已经履行对网站上信息的检查义务，但因技术能力有限，没有发觉存在淫秽信息而导致淫秽信息传播的，由于商业网站主观上不存在传播淫秽信息的故意，不能构成传播淫秽物品罪或者传播淫秽物品牟利罪。

如果行为人在个人主页上，不直接安置淫秽信息文件，而是通过超链接指向其他淫秽信息网站（如指向国外合法经营的淫秽信息网站）或者淫秽信息的，如何处理？有学者认为，“明知是淫秽网站（网页），而建立指向淫秽网页的超链接应认为使淫秽物品得以传播的行为，即传播淫秽物品的行为”①。在分析这种行为之前，必须首先了解何为超链接？超链接是一种特殊的计算

① 赵秉志主编：《新千年刑法热点问题研究与适用》，中国检察出版社 2001 年版，第 456～463 页。

机指令序列，这种指令序列由用户的浏览器程序编译后，将标志信息显示在网页上（这种标志信息被称为锚），用户点击标志信息，将触发没有被显示的链接信息，其内容是本网站或者其他网站上信息的网络地址，用户的浏览器程序将按这一网络地址请求链接中的目标信息。可见，超链接的作用不在于表现目标信息，而是引导用户去寻找目标信息。行为人如果只在网页上设置转向其他网络服务器的超链接，而没有设置淫秽色情信息的，由于行为人没有控制淫秽信息文件，更谈不上传播淫秽信息，不构成传播淫秽物品的行为，而属于帮助他人传播淫秽信息。这里可以分为两种情况：（1）如果超链接指向的是营利性的淫秽网站（网页）（以下简称被指向方），由于这种链接存在于他人的网页中，而且，这种链接的作用效果与一般的下载请求没有区别，因此，可以认为被指向方对他人帮助其传播淫秽信息的行为没有认识。而建立链接者则对被指向方及自己的行为有确切的认识，其行为符合我国刑法理论中的片面帮助犯的构成要件，应按传播淫秽物品牟利罪的从犯论处。被指向方可能构成传播淫秽物品牟利罪，但不与主动方构成共同犯罪。（2）如果链接指向的是非营利性色情信息网站（网页），网站传播淫秽色情信息情节严重的，可能构成传播淫秽物品罪，但不与建立链接者构成共同犯罪。建立链接者的行为符合我国刑法理论中的间接正犯的特征，如果满足其他构成要件的，可以构成传播淫秽物品牟利罪。

第七章　危害电子商务计算机信息系统安全的犯罪

第一节　危害电子商务计算机信息系统安全犯罪概述

电子商务活动的物质技术基础是计算机系统及其网络通信设备设施，电子商务活动的正常进行依赖于这些设备设施的正常安全运作，如果它们遭到破坏或者干扰，必然影响电子商务活动的正常进行，甚至导致电子商务活动的失败。因此，研究危害电子商务计算机信息系统安全的犯罪以及审判实践中的疑难问题，对准确打击犯罪，保护我国电子商务正常发展具有重要意义。

在分析危害电子商务计算机信息系统安全的犯罪之前，有必要明确计算机信息系统和计算机信息系统安全性的概念。计算机的定义有多种，《新韦氏词典》的定义是“一种能存储、检索和处理资料的、可编制程序的电子装置”。《汉语大词典》的定义是“能进行数学运算的机器，有的用机械装置制成，如手摇计算机；有的用电子元件制成，如电子计算机”。一般认为，现代意义上的计算机是指电子计算机，由硬件系统和软件系统组成，是一个软硬件协调工作的有机的统一整体，这一整体也被称之为计算机系统。《中华人民共和国计算机信息系统安全保护条例》第 2 条规定，计算机信息系统“是指由计算机及其相关的配套设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采

集、加工、存储、传输、检索等处理的人机系统”。电子商务计算机信息系统是指能实现一定的电子商务应用功能，具有相应的信息存储、处理、传输能力，由计算机及其相关配套设备、设施（含网络）构成的人机系统。

计算机信息系统安全是计算机科学的重要研究方向之一。计算机信息系统安全的定义有多种，国际标准化委员会的定义是“为数据处理系统建立和采取的技术的和管理的安全保护，保护计算机硬件、软件、数据不因偶然的或恶意的原因而遭到破坏、更改、显露”。我国公安部计算机管理监察司的定义是“计算机资产安全，即计算机信息系统资源和信息资源不受自然的和人为的有害因素的威胁和危害”。有的学者将计算机信息系统安全分为四个层次①：(1) 实体安全——指系统设备及相关设施运行正常，系统服务适时。(2) 软件安全——指软件完整。(3) 数据安全——指系统拥有的和产生的数据或信息完整、有效，使用合法，不被破坏或泄露。(4) 运行安全——系统资源和信息资源使用合法。综合以上观点，作者认为，计算机信息系统安全应当包括计算机信息系统功能的正常发挥和计算机资产安全。具体而言，所谓计算机信息系统功能的正常发挥，是指计算机信息系统的各种功能能够按照设计要求正常发挥，不受自然的或者人为的因素的影响或丧失，如计算机访问控制功能能够阻止非授权人员访问计算机信息系统中的各种资源，电子商务销售计算机信息系统能够自动完成货物的销售和信用卡支付等功能。所谓计算机资产安全，是指计算机硬件系统或称计算机实体资源不被损坏而失去其应有的功能和计算机信息资源包括计算机程序和计算机数据不被非授权的删除、修改、增加。因此，电子商务计算机信息系统安全可以认为包括三个部分，其一是计算机信息系统能够按照

① 殷伟、张莉：《手把手教您计算机安全技术》，电子工业出版社1997年版，第28页。

设计要求正常运作，各种电子商务应用功能正常发挥；其二是计算机信息系统的实体系统不受损害，各设备设施电气性能正常；其三是各计算机程序和计算机数据不被非授权的修改、增加和删除，处于完整、保密状态。

危害电子商务计算机信息系统安全犯罪的直接危害对象，是电子商务计算机信息系统以上三部分的安全，它们与危害电子商务秩序的犯罪不同。在主观方面，除了有危害计算机信息系统安全的目的动机外，一般没有其他目的动机如盗窃财物、泄愤报复、贪污等，而后者通常不会危害计算机信息系统安全，反而希望系统能够正常工作，以利于实现盗窃财物、窃密、贪污、金融诈骗等目的；在客观方面表现为对计算机信息系统安全的破坏行为，后果一般表现为计算机信息系统不能正常工作，系统硬件系统或者软件系统遭到损坏或者破坏，而后者一般不会危害电子商务计算机信息系统安全，而是利用系统功能实现一定的目的。

危害电子商务计算机系统安全的犯罪可以依据不同标准进行分类。根据犯罪行为直接危害对象分类，可以分为危害计算机信息系统功能的犯罪、危害计算机信息系统实体资源的犯罪和危害计算机信息系统信息资源的犯罪；根据目前较常见的犯罪形式分类，可以分为非法侵入特定计算机信息系统的犯罪、施放有害计算机程序的犯罪、破坏计算机信息系统功能的犯罪、破坏计算机信息系统数据或者应用程序的犯罪。行为人实施危害电子商务计算机信息系统安全犯罪的，依据我国《刑法》第 285 条、第 286 条定罪量刑。

我国《刑法》第 285 条、第 286 条规定了危害计算机信息系统的犯罪行为，司法解释将其规定为非法侵入计算机信息系统罪和破坏计算机信息系统罪两种犯罪。《刑法》第 286 条三个条款规定之罪，究竟是一个罪名还是分成三个独立的罪名，理论界存在不同的看法。有些学者认为，这一条文规定之罪是一个罪名即

“破坏计算机信息系统罪”①，有些学者主张是三个罪名，即（1）破坏计算机信息系统功能罪；（2）破坏计算机信息系统数据、应用程序罪；（3）制作、传播计算机病毒等破坏性程序罪②。后者认为，《刑法》第 286 条三个条款规定的犯罪行为在犯罪对象、犯罪方法和犯罪前提等方面各不相同，应当成立三个罪名。作者同意后一种观点，认为关于罪名的确定，应当“根据犯罪构成来确定罪名，才能使罪名达到法定性、准确性等要求，罪名的内涵符合犯罪构成是罪名科学性最基本的表现”③。《刑法》第 286 条三个条款规定具有上述不同之处，其犯罪构成要件各不相同，由于该条没有采取“具有下列行为之一”或“具有下列情形之一”的表达方式，所辖三款的规定不是一个罪名下的选择性构成要件，将它们定为一个罪名确属不妥。另外，从法条的各款的罪状与法定刑的配置上看，《刑法》第 286 条与第 209 条、第 345 条等条文，在结构形式和立法技术上大同小异，既然后二者可以分别确定为独立的若干罪名，对《刑法》第 286 条三个条款规定的罪行，为什么不可以确定为 3 个罪名？此外，破坏计算机信息系统的行为十分复杂，将它们分为三个罪名来研究和论述，能够更为深刻、具体地揭示这三种罪行的特征，明确它们之间的界限，有利于准确定罪量刑。因此，本章对《刑法》第 286 条规定的犯罪行为按三个独立的罪名，即破坏计算机信息系统功能罪、破坏计算机信息系统应用程序或数据罪、施放破坏性计算机程序罪，

① 赵秉志主编：《新刑法教程》，中国人民大学出版社 1997 年版，第 671～673 页；吴振兴主编：《刑法新立罪的理论与实务》（下卷），吉林大学出版社 1998 年版，第 19～22 页。

② 周振想、张军主编：《中国新刑法释论与罪案》（下），中国方正出版社 1997 年版，第 1203～1210 页；陶驷驹主编：《中国新刑法通论》，群众出版社 1997 年版，第 818～821 页；赵秉志、于志刚：《试论计算机犯罪》，《刑法论丛》（第 1 卷），法律出版社，第 57～58 页。

③ 赵廷光：《论犯罪构成与罪名确定》，《法学》，1999 年第 5 期。

进行分析研究。

第二节　非法侵入特定计算机信息系统罪

自计算机投入应用伊始，非法侵入计算机信息系统的犯罪就接踵而来，随着计算机、网络的广泛应用，这种犯罪愈演愈烈，20 世纪末电子商务逐渐发展起来，承载着财富的电子商务计算机信息系统更是这种犯罪指向的重点。2001 年美国计算机安全协会和美国联邦调查局共同进行了一项调查，调查报告显示，有 85％的美国企业和政府机构的电脑在 2000 年遭受到非法入侵。关于被害频度，回答达到“10 起以上”的企业/政府机构为 58％①。在我国，这种犯罪也十分严重，中国互联网络发展状况统计报告（2001/7）显示，在一年内计算机被非法入侵的占 47.1％，另有 9.9％的人不知道是否被非法侵入过。电子商务领域非法侵入计算机信息系统的犯罪是电子商务安全迅速发展的巨大威胁。

一、非法侵入特定计算机信息系统罪的概念与犯罪构成

为保护我国计算机信息系统安全，特别是国家事务、国防建设和尖端科学技术领域等特定的计算机信息系统安全，我国先后制定了若干的规章、法规和法律，但没有将非法侵入特定计算机信息系统的行为规定为犯罪。1997 年刑法修订时，新增加了一个法条，即《刑法》第 285 条，规定非法侵入特定计算机信息系统的行为构成犯罪。行为人非法侵入特定的电子商务计算机信息系统的，依据我国《刑法》第 285 条和《关于维护互联网安全的决定》定罪量刑。

---

① 《85％美国企业和政府机构曾遭非法入侵》，http://tech.sina.com.cn/，2001 年 8 月 1 日。

非法侵入特定计算机信息系统罪是指，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行为。本罪是行为犯，只有一个构成类型，由一般主体、犯罪故意、特定犯罪前提、单一危害行为、特定犯罪对象和被害法益 6 个构成要件构成，具体内容和形式如下：

1. 一般主体

本罪的主体是一般主体，即年满 16 周岁，具有刑事责任能力的自然人。

从犯罪主体的能力来看，本罪的主体至少具有基本的计算机知识和计算机操作能力，有些甚至是计算机、网络技术方面的“高手”。由于近年来计算机应用发展十分迅速，年轻人对计算机技术十分感兴趣，对象征着“超人”能力的黑客技术尤甚，加之年轻人社会阅历浅薄，国家在该方面的法制教育没有跟上，相当一部分年轻人热衷于成为秘密闯入他人计算机信息系统的“黑客”。因此，从犯罪主体的年龄来看，黑客年轻化倾向越来越突出①。

由于我国计算机信息系统安全防护意识和安全防护技术比较落后，有些安全性能比较薄弱的计算机信息系统可能被他们成功侵入，其中就可能有国家事务、国防建设和尖端科学技术领域的计算机信息系统。但是，本罪不属于《刑法》第 17 条规定的八类犯罪，因此，即使行为人侵入国家最高保密级别的计算机信息系统，如果其尚未满 16 周岁，都不能构成本罪。

单位能否成为本罪主体？学术界存在不同的观点。有的学者认为，单位可以成为本罪的主体，理由是《中华人民共和国计算机信息系统安全保护条例》第 7 条规定，“任何组织或者个人，不得利用计算机信息系统从事危害国家利益、集体利益和公民合

① 《黑客年轻化倾向越来越突出》，http：//www.chinaeb.com.cn/，2000 年 4 月 28 日。

法利益的活动，不得危害计算机信息系统的安全”，其行为主体是“任何组织和个人”，当然包括单位，因此单位可以成为本罪的主体①。多数学者认为，本罪主体只能由自然人构成②，理由是《刑法》第 30 条规定，“公司、企业、事业单位、机关、团体实施的危害社会的行为，法律规定为单位犯罪的，应当负法律责任。”根据该条规定，只有法律明文规定单位可以构成犯罪的，单位才能成为该罪的主体。《刑法》没有规定单位可以构成本罪犯罪主体，因此在认定本罪时，不能把单位作为本罪的犯罪主体。作者赞同后者观点，认为《中华人民共和国计算机信息系统安全保护条例》是行政法规，不是刑事法律法规，单位可以构成非法侵入计算机信息系统行政违法行为的主体，而不能构成本罪的主体。

但是，在现实生活中完全可能出现单位指派职员非法侵入以上特定的三类计算机信息系统的行为，如某些网络安全公司为向政府某机构推销安全产品，未经该机构允许，指派公司职员非法侵入国家事务计算机信息系统，以证明其计算机信息系统安全性能落后，必须更新安全设备设施。对于此类情况，依据我国刑法规定，只处罚实施行为的人和指使其行为的人，不处罚单位。随着社会信息化的发展，计算机信息系统在国家事务、国防建设和尖端科学技术领域的应用将会越来越广泛，单位实施非法侵入以上三类计算机信息系统的情况可能会大量增加，我国可以借鉴法国关于该罪的立法经验(《法国刑法典》第 323 条)，将单位纳入本罪的犯罪主体。

境外人员实施本罪规定的行为该如何处罚？计算机网络把世界各地的计算机信息系统连接在一起，行为人可以在境外操作计

① 姚茂文：《计算机犯罪及实践问题》，《人民检察》，1997 年第 7 期。

② 高铭暄、马克昌主编：《刑法学》（下编），中国法制出版社 1998 年版，第 958 页。

算机，突破境内计算机的安全防护措施，未经授权调用境内计算机信息系统中的资源，由于计算机网络的特性，行为人的行为和结果几乎同时发生，而结果和行为可能分处远隔万里的两地。对于这种情况，根据我国《刑法》第 6 条第 3 款和第 1 款规定，“犯罪的行为或者结果有一项发生在中华人民共和国领域内的，就认为是在中华人民共和国领域内犯罪”，“凡在中华人民共和国领域内犯罪的，除法律有特别规定的以外，都适用本法”，因此，境外的中国公民和外国人实施本罪规定的行为的，都应当依法追究刑事责任。境外的中国公民实施本罪，侵犯他国国家事务、国防建设、尖端科学技术领域的计算机信息系统的，可以适用我国刑法，但是由于本罪最高法定刑不超过 3 年，可以不追究。

2. 犯罪故意

本罪在心态方面表现为故意，而且必须是直接故意，即明知是国家事务、国防建设、尖端科学技术领域的计算机信息系统，自己的行为属于非法侵入行为，而仍然侵入的心理态度。由于以上三类特定的计算机信息系统均有较强的安全防护措施，行为人在非授权的条件下，往往要花费大量的时间，进行长时间的努力，才能发觉计算机信息系统安全漏洞，或者强行突破安全防护措施侵入系统，而即使是他人告知非法侵入方法，行为人也必须遵循该方法主动实施，因此间接故意不可能实施本罪。

过失能否构成本罪？有学者认为过失也可以构成本罪，理由是为了从法律上保护国家计算机信息系统不受侵害，特别是考虑到计算机信息系统被破坏后将造成的重大损失，因而，对过失犯罪也应当定罪处罚，并认为由于计算机犯罪主观认定的复杂性，如果不设立过失犯罪，任何人都可将自己侵入计算机信息系统的行为归为疏忽大意所致，导致对计算机信息系统安全保护不力①。作者不同意这种观点，过失行为不可能实施非法侵入以上

① 姚茂文：《计算机犯罪及实践问题》，《人民检察》，1997 年第 7 期。

三类特定计算机信息系统。以上三个领域的计算机信息系统由于用途特殊，一般都装备了较强的安全防护技术措施。行为人如果明知是以上三类特定计算机信息系统，不经努力是不可能非法侵入系统的。另据《刑法》第 15 条规定，过失犯罪不仅必须以发生危害结果为前提，而且“法律有规定的才负刑事责任”，《刑法》第 285 条没有规定过失犯罪，因此，过失不构成本罪。

需要指出的是，行为人如果完全不知道是以上三类特定计算机信息系统，例如行为人从其他途径非法得到以上三类特定计算机信息系统的用户密码，而并不知道这些计算机信息系统的性质，实施非法侵入这些系统的行为，其行为应当按照《中华人民共和国计算机信息系统安全保护条例》进行处罚，而不构成本罪。如果行为人侵入后发觉计算机信息系统的性质而不退出的，行为人的不退出行为默认了其非法侵入以上三类特定计算机信息系统的行为，属于刑法理论上的事后故意，应视为在主观方面具有直接故意的心态。

行为人的犯罪目的可能有多种，如突破这些计算机信息系统安全防护体系、了解系统的功能、偷阅系统中的有关信息资料，或者是帮助发现这类计算机信息系统的安全漏洞等，但是不能有其他犯罪目的，如窃取秘密资料、破坏计算机信息系统、盗窃财物、金融诈骗等，如果有后者所述的犯罪目的，则不构成本罪，而可能构成其他犯罪。行为人的动机也可能有多种，如对这类计算机信息系统的安全系统抱有好奇心理和探知狂癖、挑剔这类系统的安全漏洞借以显示炫耀自己的计算机能力，或者是搞恶作剧戏谑，甚至是纯粹追求刺激，即所谓的“黑客”动机，行为人如果有其他动机如泄愤，则可能构成其他犯罪而非本罪。

3. 特定犯罪前提

本罪的特定犯罪前提是违反国家规定。这里的国家规定，不仅包括相关的国家法律、法规，还包括相关的行政规章制度、命令等。具体而言，主要指《保守国家秘密法》、《军队通用计算机

系统使用安全要求》、《计算机信息系统安全保护条例》、《计算机信息网络国际联网管理暂行规定》、《互联网络域名注册暂行管理办法》和《互联网络域名注册实施细则》、《计算机信息网络国际联网管理暂行规定实施办法》、《计算机信息网络国际联网安全保护管理办法》、《计算机信息系统保密管理暂行规定》、《金融机构计算机信息系统安全保护工作暂行规定》、《国际互联网出入信道管理办法》、《计算机信息系统国际联网保密管理规定》等。行为人如果没有违反有关国家规定，则不构成本罪。

4. 单一危害行为

本罪的单一危害行为表现为，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行为。以上三类特殊领域计算机信息系统由于其重要性，一般都有相当强的防护措施防止非授权访问行为，包括拒绝非合法用户访问所有的系统资源和限制合法用户调取其权限范围外的其他系统资源。这里的“侵入”一词，本身含有未经授权而调取需授权才能获得的系统资源的意义，它包含两种行为方式：一种是非合法用户未经授权而调取计算机信息系统资源的行为；一种是合法用户利用各种手段，超越其被授予的权限，调取需要更高权限的系统资源的行为。关于授权的主体，有人认为是国家有关主管部门①。作者认为授权主体应该根据具体情况而定，有的安全级别较高的国防建设计算机信息系统需要国家有关主管部门授权，直接管理营运的部门无权向他人授权或者提升其权限，有的国家事务计算机信息系统的授权权力直接由计算机信息系统管理营运部门行使。

行为人侵入的具体方法有多种，主要表现为以下几种：(1)冒用合法用户身份侵入。行为人冒用合法用户的用户名和密码通过计算机信息系统安全检测进入系统，行为人所使用的合法用户

① 高铭暄、赵秉志主编：《刑法论丛》（第 2 卷），法律出版社 1999 年版，第 600 页。

的密码，既可能是秘密窃取的，也可能是通过其他途径非法得到的，还可能是合法用户非法给其使用的。(2) 乘机而入。行为人利用合法用户访问计算机信息系统时的线路连通状态，或者乘合法用户离开而未退出系统的疏忽进入系统。(3) 利用计算机安全技术破解计算机信息系统安全措施而侵入。计算机信息系统安全措施的安全保障是相对的，行为人经过努力能够突破或者绕过安全防护体系进入系统，其具体方式有两种：一种是利用密码破解技术搜索系统进入口令，利用解密技术破解系统中的口令加密文件，或者截获破译计算机信息系统通信线路中的密码信息等方法强行突破系统安全防护；一种是利用系统安全防护本身存在的缺陷和漏洞，绕过系统安全防护，例如前文提到的利用 TCP/IP 协议的缺陷攻击系统防火墙，将使系统安全防护形同虚设。(4) 利用系统“天窗”侵入。计算机信息系统在开发时，为便利调试的需要往往留有隐蔽的“天窗”，或者系统软硬件开发者出于其他目的，秘密设置“天窗”，这些“天窗”成为系统安全的严重隐患，行为人如果发觉这种秘密通道，可能用来侵入系统。例如美国底特律的几位汽车工程师发现了佛罗里达商用分时服务系统中的一个活动天窗，他们通过这个活动天窗进入计算机信息系统，查到了公司总裁的密码口令，并使用这一口令从系统中获取了具有重要商业价值的计算机文件。

行为人侵入以上三类特定计算机信息系统后，是否还必须进行其他后续行为？有学者认为，行为人破译系统密码，进入系统的总目录，但单纯从进入总目录到进入子目录阶段，其行为并没有社会危害性，对国家事务、国防建设、尖端科学技术的保密性也没有丝毫侵犯，因此，本罪规定的侵入行为必须伴有浏览行为且仅限于浏览①。作者不同意这种观点，国家事务、国防建设、

① 刘广三：《论计算机犯罪》，中国人民大学出版社 1999 年版，第 171 页。

尖端科学技术领域计算机信息系统是特别重要的计算机信息系统，刑法才把非法侵入这些系统的行为规定为犯罪，即使行为人侵入系统后不进行任何其他后续行为，也已经破坏了计算机信息系统的安全体系，侵犯了计算机信息系统的安全，其犯罪行为已经完成，至于其继续进行其他窃密、窃取财物、破坏计算机资源的行为，则还可能构成其他犯罪。而且，我国刑法没有规定行为人侵入以上系统后，还必须进行浏览等行为才能构成犯罪，因此，是否有后续的浏览、拷贝系统信息等行为不是构成本罪必需的危害行为。

5. 特定犯罪对象

本罪的特定犯罪对象是国家事务、国防建设、尖端科学技术领域计算机信息系统。《计算机信息系统安全保护条例》第 4 条规定，“计算机信息系统的安全保护工作，重点是维护国家事务、经济建设、国防建设、尖端科学技术等重要领域的计算机信息系统的安全”，而以上三类特定计算机信息系统是重中之重，国家利用刑法手段予以保护。同时，行为人只有违反国家规定，侵入以上三类特定计算机信息系统才可能构成犯罪，而侵入其他计算机信息系统，如经济建设领域计算机信息系统则不会构成本罪。《刑法》第 285 条规定，受刑法保护的是国家事务、国防建设和尖端科学技术这三类领域的计算机信息系统，但是以上三类特定计算机信息系统的具体范围和认定标准却没有法律规定，有学者认为，主要是看该系统所采集、加工、存储、传输、检索的信息属于何种性质，具体的技术性规定应由国家相关部门发布规章加以规定①。作者基本同意这种观点，在目前没有相关法律法规、司法解释予以明确规定的情况下，在司法实践中应该认为，凡是为国家事务、国防建设、尖端科学技术领域服务的，以及这些领域部门拥有的计算机信息系统属于以上三类特定计算机信息

① 姚茂文：《计算机犯罪及实践问题》，《人民检察》，1997 年第 7 期。

系统。《刑法》第 285 条保护的电子商务计算机信息系统，主要是从事电子商务宏观调控和直接管理的国家机关的计算机信息系统，如中国人民银行、税务机关、工商管理机关等国家机关的计算机信息系统，以及为这些部门服务的计算机信息系统。

6. 被害法益

本罪侵犯的法益是复合的，包括国家对计算机信息系统安全管理秩序、国家的保密制度和国家事务、国防建设、尖端科学技术领域的正常活动。行为人非法侵入以上三类特定计算机信息系统，破坏了国家对计算机信息系统安全管理制度，同时，由于以上三类特定计算机信息系统往往存储、处理、传输国家秘密信息，直接关系到国家秘密的保护和这些重要部门的正常活动，因此，本罪危害行为还使国家秘密和国家相关重要部门的正常活动处于现实危险状况，行为人非法侵入以上三类的特定计算机信息系统，还对电子商务管理活动的正常进行构成现实的威胁。有些学者认为，“本罪所侵犯的客体是国家重要领域的计算机信息系统的安全”，并认为“惩罚此类入侵行为的关键之处在于，其非法侵入计算机信息系统的行为已使国家事务秘密、国防建设秘密和尖端科学技术秘密等受保护的秘密超出了限定的授权接触范围”①。这种观点明显忽略了刑法对以上三类特定计算机信息系统正常运作和相关部门正常活动的保护。

以上 6 个要件是非法侵入特定计算机信息系统罪的构成模型，缺少其中任何一个构成要件，均不能成立本罪。

根据《刑法》第 285 条的规定，犯非法侵入特定计算机信息系统罪的，处 3 年以下有期徒刑或者拘役。在刑罚适用时，应该考虑具体情况，在法定刑的范围内从重或者从轻处罚：(1) 行为

① 赵秉志、于志刚：《论非法侵入计算机信息系统罪》，《法学研究》1999 年第 2 期；刘广三：《计算机犯罪论》，中国人民大学出版社 1999 年版，第 164 页。

人犯非法侵入特定计算机信息系统罪，如果被侵入的国家事务、国防建设、尖端科学技术领域的计算机信息系统特别重要，行为人的社会危害性特别严重的，应当从重处罚，反之，如果被侵入的是重要程度相对较低，影响范围相对较小的计算机信息系统，造成的社会危害相对较轻的，可以从轻处罚。(2) 行为人多次侵入或者侵入多个以上三类特定计算机信息系统的，应当从重处罚；行为人初次侵入，并且侵入后自动退出系统的，可以从轻处罚。

二、认定非法侵入特定计算机信息系统罪应该注意的问题

1. 本罪与非罪的界限

区别本罪与非罪，关键要注意三个方面：首先，行为人必须明知是国家事务、国防建设、尖端科学技术领域的计算机信息系统，而有意实施侵入的心态，如果行为人不知道是以上三类计算机信息系统的，即使客观上非法侵入了以上三类计算机信息系统，也不能构成本罪，而应当依据相应的行政法规进行处罚。其次，行为人侵害的犯罪对象必须是以上三类特定计算机信息系统，才能构成本罪，行为人非法侵入的计算机信息系统不属于以上三类的，只能依据相应的行政法规进行处罚，不构成本罪。再次，行为人的危害行为是违反国家规定侵入以上三类特定计算机信息系统的行为，其根本特征是获得了其无权获得的这些计算机信息系统的资源控制权，因此，计算机信息系统的合法用户的非授权侵入行为也可能构成本罪。

2. 本罪与利用计算机实施的其他犯罪的界限

《刑法》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，依照刑法有关规定定罪处罚。本罪与利用计算机实施的其他犯罪，虽然都是利用计算机信息技术实施的犯罪，但是，它们存在明显的区别，主要表现在：(1) 犯罪目的不同。利用计算机实施其他犯罪的，一

般有相应的犯罪目的，如非法获取财物、窃取国家秘密等，而本罪多以破解计算机信息系统安全防护为目的。(2) 客观方面的表现不同。利用计算机实施其他犯罪的，在进入计算机信息系统后，往往实施完成犯罪目的所必需的其他犯罪行为，如复制秘密信息、修改电子资金账户等，而本罪侵入计算机信息系统后，不再有其他犯罪行为。(3) 犯罪对象不同。本罪的犯罪对象仅限于国家事务、国防建设、尖端科学技术领域的计算机信息系统，而利用计算机实施其他犯罪的，其犯罪对象则不限于以上三类计算机信息系统。

3. 本罪的犯罪形态问题

本罪是否为行为犯，具有哪些未完成犯罪形态？学者们有不同的观点。有学者认为，本罪是行为犯，只要查证行为人有侵入信息系统的事实，即构成犯罪既遂①。有学者也认为本罪是行为犯，并且认为本罪的犯罪形态只有犯罪预备、犯罪中止和犯罪既遂三种形态，而没有犯罪未遂，判断犯罪预备与犯罪既遂界限的标准应当是行为人的侵入行为是否突破或者绕过系统的安全机制②。还有学者认为，本罪不是行为犯，本罪存在犯罪未遂，已经“侵入”计算机信息系统的，应当视为犯罪既遂，而“侵而未入”的，则显然应当认为是犯罪未遂。

作者认为，本罪是行为犯。行为犯可以分为两类，一类是举止犯（亦称即成犯），指行为人只要着手实施刑法分则规定的构成要件的行为，就成立犯罪既遂；另一类是过程犯，指行为人实施并完成刑法分则所规定的构成要件的行为，才成立犯罪既遂③。对于行为犯的即成犯而言，只有犯罪的既遂形态，而不存

① 胡国平：《关于四种计算机犯罪的认定》，《法律科学》，1997 年第 4 期。

② 姚茂文：《计算机犯罪及实践问题》，《人民检察》，1997 年第 7 期。

③ 姜伟：《犯罪形态通论》，法律出版社 1994 年版，第 116 页。

在预备犯、未遂犯和中止犯这三种犯罪的未完成形态；而对于行为犯的过程犯而言，只有当构成要件的危害行为实行终了，犯罪才告完成，从行为人着手实行构成要件的行为到行为实施终了，其间通常有一个较为复杂的动作过程，在此过程中行为人可能自动放弃犯罪，也可能因行为人意志以外的原因未能得逞，从而存在犯罪未遂和犯罪中止，至于是否存在预备犯，要根据预备行为的性质及其对刑法保护法益的危害来确定，不能一概而论。本罪属于行为犯的过程犯，当行为人完成构成要件的侵入行为，才能构成犯罪既遂。

关于本罪有哪些未完成形态，作者认为，行为人试图侵入计算机信息系统，被系统安全措施拒之门外，而自动放弃继续侵入努力的，属情节显著轻微、危害不大的行为，不能认为是犯罪，故本罪不存在中止犯；行为人侵入计算机信息系统是危害行为直接接触犯罪对象并进行攻击的过程，这就是着手实行犯罪，如果行为人在着手攻击之前准备工具、制造条件，如购买设备，学习安全技术等，由于这种行为缺乏现实的针对性，离具体的犯罪对象较远，对直接客体尚未构成现实的威胁，更是情节显著轻微、危害不大的行为，也不构成犯罪，因此，本罪不存在预备犯；如果行为人着手侵入计算机信息系统，有可能侵入系统而在实现侵入之前被发觉抓获的，或者其物质技术条件尚不足以破解计算机信息系统安全措施，行为人却主观上认为可以实现侵入的，在实施侵入行为过程中被发觉抓获的，其行为对计算机信息系统安全构成了直接的、现实的威胁，之所以未能完成犯罪是由于行为人意志以外的因素造成的，因此应当构成犯罪未遂，即本罪存在未遂犯。

4．一罪和数罪问题

行为人违反国家规定，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，如果有其他后续行为的，应当视其具体情况，区别对待处理：(1) 行为人违反国家规定，侵入以上

三类特定计算机信息系统后，产生了新的犯罪故意，进行其他犯罪行为的，如盗窃国家秘密、破坏计算机信息系统等，构成非法侵入计算机信息系统罪和各相应的其他罪，按照数罪并罚的原则进行处罚。(2) 行为人出于破坏计算机信息系统、盗窃国家秘密等目的，违反国家规定侵入以上三类特定计算机信息系统的，构成非法侵入计算机信息系统罪和各相应的其他罪的牵连犯，从一重罪定罪处罚。

三、对非法侵入特定计算机信息系统罪的立法建议

我国《刑法》第 285 条规定，“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”，构成非法侵入计算机信息系统罪，该法条在以下两个方面需要完善：

1.“国家事务、国防建设、尖端科学技术领域计算机信息系统”的概念、范围不明确。《刑法》第 285 条规定的犯罪对象是国家事务、国防建设、尖端科学技术领域的计算机信息系统，即用途为国家事务、国防建设、尖端科学技术领域的计算机信息系统，当然包括中央政府、省、市、县、乡（镇）政府机构用于公务的计算机信息系统。本罪的立法本意是对特别重要的计算机信息系统予以特殊的法律保护，用刑法手段打击非法侵入这类特别重要的计算机信息系统的行为，但是，仅仅根据用途划分是否属于这类特别重要的计算机信息系统，并不十分准确。例如随着社会信息化和政府上网工程的发展，乡（镇）政府一级的国家机关也可能应用计算机信息系统，管理日常行政事务，如乡（镇）一级的公安派出所利用计算机信息系统统计辖区内居民的基本情况，行为人非法侵入该单位的计算机信息系统的，毫无疑问，属于非法侵入国家事务的计算机信息系统的行为，构成犯罪，应当定罪量刑。然而行为人如果非法侵入中国工商银行总行存储密钥的核心计算机信息系统，由于犯罪对象不属于国家事务、国防建设、尖端科学技术领域的计算机信息系统，虽然对国家金融安全

构成严重威胁，但也不构成犯罪，只能依据相关行政法规进行行政处罚。依照常识，乡（镇）一级公安派出所用于资料统计的计算机信息系统，无论如何都不如中国工商银行总行的核心计算机信息系统更重要，侵犯后者的计算机信息系统的社会危害性明显更大。此外，还有电力、煤气、电信等企业的控制计算机信息系统，也要比乡（镇）一级公安派出所的计算机信息系统更重要，如果遭到破坏可能对公共安全构成严重威胁，非法侵入这些计算机信息系统的社会危害性更大。犯罪是具有严重社会危害性的行为，侵犯乡（镇）一级公安派出所的计算机信息系统属于社会危害性严重的行为，而侵犯更重要的非法律指定的计算机信息系统却不构成犯罪，这明显与立法本意和刑法基本原则相违背，因此，应该对本罪的犯罪对象进行修改。

如上所述，除了国家事务、国防建设、尖端科学技术领域的计算机信息系统外，其他领域如金融、电信、电力、燃气、水利、航空、铁路等的计算机信息系统中，有一部分也特别重要，侵犯这些计算机信息系统具有严重的社会危害性，刑法应该予以保护。此外，目前我国危害计算机信息系统安全的行为十分严重，加大刑法打击力度对遏制这类犯罪具有积极作用。建议将本罪侵犯的犯罪对象扩展到所有重要的计算机信息系统，同时规定较宽的法定刑幅度，法官可根据侵犯对象重要性等犯罪情节的差别，从重或者从轻处罚。

2．增设单位犯罪

本罪没有规定单位犯罪，但是实际生活中，有些网络安全公司为显示自己的破解计算机信息系统安全防护能力，推销其安全产品，可能未经许可，非法侵入他人计算机信息系统，甚至是特别重要的计算机信息系统，或者为不正当竞争目的，非法侵入对手的计算机信息系统，暴露竞争对手安全系统的漏洞。这类行为不是自然人的个人行为，而是单位行为，应当追究单位的刑事责任。建议本罪增设单位犯罪。

综合以上两点，建议将《刑法》第285条修改为：违反国家规定，侵入重要计算机信息系统的，处3年以下有期徒刑、拘役或者管制，单位犯前款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照前款的规定处罚。

第三节　破坏计算机信息系统功能罪

一、破坏计算机信息系统功能罪的概念与犯罪构成

破坏计算机信息系统功能罪，是指违反国家规定，对他人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，具有法定后果的行为。本罪是复合的构成类型，分为基本罪和派生的重罪两个构成类型，具有相应的两个法定刑档次。

（一）基本罪构成要件

本罪的基本罪是结果犯，由一般主体、犯罪故意、单一危害行为、特定犯罪前提、特定犯罪对象、特定犯罪结果、被害法益7个构成要件组成，具体内容和形式如下：

1. 一般主体

本罪的主体是一般主体，即年满16周岁具有刑事责任能力的自然人。未满16周岁的自然人实施本罪规定行为的，不构成本罪。关于本罪主体，有学者认为由于行为人通常具有高超的计算机技能，是从事计算机技术职业的专业人员，因此本罪主体是特殊主体①。作者认为，由于计算机应用的普及，操作使用计算机已经不再是计算机专业人员的特长，越来越多的非专业人员能够熟练使用计算机，并且操作计算机的技术越来越高超，这是计

① 刘广三、陈开琦、胡继光：《计算机犯罪的有关法律问题》，《法学》，1996年第8期。

算机技术和应用发展的必然结果。此外，刑法上的特殊主体的特定身份包括法定身份和自然身份两种，具有计算机技能的人不属于其中任何一种，我国刑法分则对本罪也没有要求行为人具有特殊身份，因此，认为本罪主体是特殊主体的观点站不住脚。

关于境外人员是否能够成为本罪主体。如本章上一节所述，中国人和外国人在境外实施本罪规定行为，破坏我国境内的计算机信息系统功能的，应该依照我国刑法追究刑事责任。中国人在境外实施本罪规定的行为，破坏他国计算机信息系统功能的，根据《刑法》第 7 条规定，“中华人民共和国公民在中华人民共和国境外犯本法规定之罪的，适用本法，但是按本法规定的最高刑为 3 年以下有期徒刑的，可以不予追究”，本罪基本罪的最高刑为 5 年有期徒刑，重罪的最高刑为 15 年有期徒刑，因此，应该依照我国刑法规定追究刑事责任。

2. 犯罪故意

本罪在犯罪心态上表现为故意，即明知自己的行为可能造成计算机信息系统不能正常运作的危害后果，希望或者放任这种危害后果的心理态度。过失不构成本罪。在实践中，此种犯罪多表现为直接故意，其一般犯罪目的是：明知自己的行为可能造成计算机信息系统不能正常运作的危害后果，希望这种结果发生的心理态度。除了这种一般犯罪目的外，通常还有毁灭罪证、报复、敲诈勒索、恐吓他人等犯罪目的。行为人有无其他特殊犯罪目的不影响本罪成立，但如果有其他犯罪目的，可能同时构成其他犯罪。行为人的犯罪动机可能有多种，如泄愤、恶作剧戏谑他人、向他人展示自己的高超计算机技能等，犯罪动机如何，不影响本罪的成立。

3. 单一危害行为

本罪是单一危害行为，即破坏计算机信息系统功能的行为，它有四种选择性行为方式，即删除、修改、增加、干扰计算机信息系统功能的行为，只要行为人实施其中任何一种行为，都构成

本罪的破坏行为，行为人同时实施两种以上行为的，仍然只构成一罪，而不实行数罪并罚。

所谓删除，是指使计算机信息系统功能的全部或者部分丧失。删除计算机信息系统功能的方式有多种，大体可以分为物理删除方式和使用计算机命令程序删除方式两种。前者有物理损坏计算机硬盘、网络设备设施等方法，如使用高能电磁武器损坏计算机设备，俄罗斯最近研制出一种“电子炸弹”，它完全无声，体积不大，可威力无比。瑞典军方对这种可以装在公文包中的微型“电子炸弹”进行的试验证明，其巨大的破坏力，能使周围的任何计算机在顷刻间遭到致命损害。这种“电子炸弹”能发射一种短微波脉冲，其能量最高达 100 亿瓦，这种高能量脉冲能将任何计算机中的细小电路开关“熔断”，进而使整个系统瘫痪。其有效作用范围约 50 米，“较大的炸弹”的破坏范围可达几百米。它可用来对付任何种类的计算机，不管是装在战斗机上的计算机、信息中心的计算机、银行的计算机还是发电厂的计算机①。后者方法与计算机的种类型号和使用的操作系统平台有关，由于计算机可以分为巨型计算机、大型计算机、中型计算机、小型计算机和 IBM PC 微型计算机等种类，系统操作平台也有 UNIX 操作系统、MACTOISH 操作系统、DOS 操作系统、WINDOWS 系列操作系统、WINDOWS NT 操作系统和一些大企业自行开发的操作系统等，不同型号的计算机和不同的操作系统软件的计算机信息系统的删除程序命令各不相同，不可能一一枚举，以微型计算机常用的 WINDOWS95 系统为例，删除计算机信息系统功能的命令程序有 FORMAT（格式化）命令、DELETE（删除）命令等。

有学者把破坏计算机信息系统功能的方法分为两类，一类是

① 《俄罗斯研制出“电子炸弹”瞬间破坏计算机系统》，《电脑日报》，1999 年 5 月 5 日。

有形破坏或者称硬破坏，指通过爆炸、砸毁等手段破坏计算机设备及其功能，一类是无形破坏或者称软破坏，指利用计算机操作方法进行非针对硬件的信息及程序的破坏，而且认为新刑法规定的破坏方法“删除、修改、增加、干扰”是指软破坏方法，而硬破坏方法没有为刑法明确规定①。作者认为，这里的“删除、修改、增加、干扰”不是计算机科学上的技术术语，而只是表明对计算机信息系统功能的影响方式，是使其功能永久性丧失、变动、增添，以及非永久性地损害系统功能而妨碍功能的正常发挥等四种方式。计算机信息系统是一个软硬件协调工作的有机整体，侵害计算机软硬件的行为都可能影响系统功能，如秘密将网卡拔出然后虚插在接口槽上，将造成计算机信息系统网络通信功能的丧失，因此，只要能够实现这四种影响方式，无论是硬破坏或是软破坏方法，都应该属于刑法规定的四种方式下的具体方法。将破坏计算机信息系统功能的方法仅限于软破坏方法，仅限于对程序和信息的破坏，缩小了《刑法》第 286 条对计算机信息系统功能的保护，不利于有效打击破坏计算机信息系统功能犯罪。

所谓修改，是指改动计算机信息系统功能的行为，具体的方法有多种，既可能是改动计算机程序和相关数据，也可能是对计算机设备设施进行物理变动，如调节硬件设备设施的设置，或者更改计算机程序的参数使计算机信息系统功能发生改变。

所谓增加，是指向计算机信息系统中增添以前没有的功能，如为邮件服务器系统增加自动回信功能等。

所谓干扰，是指采取删除、修改、增加等方法之外的，非永久性变动计算机信息系统功能的行为，具体方法有多种，目前比较典型的主要有“电子邮件炸弹”和拒绝服务两种。

---

① 于志刚：《计算机犯罪研究》，中国检察出版社 1999 年版，第 124 页。

“电子邮件炸弹”是指行为人利用特殊的电子邮件程序，在短时间内自动向被害人的电子邮件邮箱发送大量的、数据量庞大的无意义或者乱码邮件，网络用户容量有限的电子邮件信箱很容易被这些垃圾邮件充满，无法正常接收邮件。对于一些收费电子邮件服务而言，还可能给电子邮件用户造成巨大的经济损失。“电子邮件炸弹”的另一个危害是大量增加了网络上传输的电子邮件，有时甚至使电子邮件服务器资源耗尽而瘫痪。1999 年的“梅利莎”病毒和 2000 年的“爱虫”病毒的传播导致了大量电子邮件等待发送，致使许多计算机信息系统的电子邮件服务器功能丧失。

“拒绝服务”原指在公用电话网中，当没有可用线路或对方正在接听电话时，向呼叫用户发送忙音的一种网络状况。在这里是指由于计算机信息系统收到大量的、恶意请求服务，系统资源被这些无意义的服务请求消耗完而无法为正常用户服务的情况。具体而言，行为人使用拒绝服务程序，向目标计算机信息系统发送服务请求，系统接收到请求后开始响应，这时拒绝服务程序断开请求，而发送下一个新的请求，这种拒绝服务程序能够在短时间内发送数量巨大的恶意请求，甚至可以借用多台计算机信息系统发送这类请求，逐步将目标计算机信息系统的资源耗尽，以降低目标计算机信息系统的工作效率甚至使其瘫痪。在 2000 年初美国发生的黑客大规模攻击商业网站事件中，美国斯坦福大学海洋研究所内的大约 50 台电脑曾被黑客用于攻击雅虎等大型网站，加利福尼亚大学圣巴巴拉分校电脑也被用来袭击 CNN 网站。由于美国大学校园里的科研电脑比比皆是，常常无人看管，黑客用“欺骗”手段指令许多电脑同时访问某个网站，导致该网站瘫痪，如雅虎网站受攻击时，一度每秒钟要处理来访电脑发出的 1 000

兆位的信息量，相当于 1.04 亿人同时拨打某个公司的电话号码①。

4. 特定犯罪前提

本罪的特定犯罪前提是违反国家规定，这里的国家规定，不仅包括相关的国家法律、法规，还包括相关的行政规章制度、命令等。具体而言，主要指《军队通用计算机系统使用安全要求》、《计算机信息系统安全保护条例》、《计算机信息网络国际联网管理暂行规定》、《计算机信息网络国际联网管理暂行规定实施办法》、《计算机信息网络国际联网安全保护管理办法》、《计算机信息系统保密管理暂行规定》、《金融机构计算机信息系统安全保护工作暂行规定》、《国际互联网出入信道管理办法》、《计算机信息系统国际联网保密管理规定》等。行为人如果没有违反有关国家规定，则不构成本罪。

5. 特定犯罪对象

本罪的犯罪对象是他人的计算机信息系统功能。所谓功能，是指“事物或方法所发挥的有利的作用、效能”②。计算机信息系统功能是指计算机信息系统所具有的有利的作用或者效能，具体而言，是指计算机信息系统“按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理”的有利作用和效能。电子商务计算机信息系统功能根据具体从事业务活动的不同而不同，有的包括订货功能、货流配送管理功能、电子资金转账功能等，有的包括电子商务商户交易审计功能，税务征缴功能等。计算机信息系统功能不是一个有形的实物，而是计算机硬件系统、计算机程序、计算机数据和操作人员协调工作所具有的一种能力或者服务。破坏这种功能、能力、功效的途径既可以是破

① 《斯坦福大学 50 台电脑被黑客利用》，http://www.ccidnet.com.cn/，2000 年 2 月 15 日。

② 《现代汉语词典》，商务印书馆 1996 年版，第 438 页。

坏计算机程序和信息数据，也可以是破坏计算机硬件设备设施，还可以是大量虚增业务处理量，干扰计算机信息系统功能的正常发挥。

6. 特定犯罪结果

本罪是结果犯，只有因为行为人破坏计算机信息系统功能的行为，造成计算机信息系统不能正常运行，后果严重的，才能构成本罪基本罪的既遂。构成本罪，行为人的行为与计算机信息系统不能正常运行必须具有因果关系。这里的计算机信息系统“不能正常运行”，既包括不能运行，也包括运行不正常。何为“后果严重”，法律没有规定，有待司法解释予以明确，但是从刑法理论联系司法实践来看，主要包括以下情形：(1) 致使计算机信息系统功能全部或者大部遭到永久性破坏；(2) 修复被破坏的计算机信息系统功能消耗的人力、物力、财力较大，耗时较长；(3) 严重影响工作、生产、经营的正常进行，给被害单位和个人造成较大的经济损失等。

7. 被害法益

本罪的被害法益是复合的，包括计算机信息系统安全保护管理秩序、计算机信息系统所有人的合法权利和被害人正常的工作、生产经营秩序。

（二）重罪构成要件

本罪的重罪是结果加重犯，指罪行在符合基本罪构成要件的基础上，后果特别严重的行为。至于何谓后果特别严重，有待司法解释作出规定，从刑法理论联系司法实践来看，主要是指：(1) 破坏国家事务、国防建设、尖端科学技术领域的计算机信息系统功能，致使其不能正常运作，后果严重的；(2) 破坏较广泛范围内的或较多的计算机信息系统功能的全部或者部分的；(3) 为修复被破坏的计算机信息系统功能耗资巨大、耗时长久；(4) 对单位工作、生产经营活动影响特别严重，给被害单位或者个人造成巨大经济损失的。

二、认定破坏计算机信息系统功能罪应该注意的问题

1. 本罪与非罪的界限

区别本罪与非罪，关键要注意两个方面：首先，行为人主观上是否出于故意。在计算机使用过程中，不能完全避免因误操作破坏计算机信息系统功能的情况，对于这种过失行为破坏计算机信息系统功能的，即使造成严重后果，我国刑法也不以犯罪论处。因此，查明行为人主观上是否有犯罪故意是认定犯罪的关键。其次，是否因行为人的行为造成计算机信息系统不能正常运作，并有严重后果。如果行为人的行为与计算机信息系统不能正常运行没有因果关系，即使计算机信息系统不能正常运行导致严重后果，也不能追究行为人的刑事责任，不构成本罪既遂。

2. 本罪与他罪的界限

本罪与非法侵入特定计算机信息系统罪的界限。两罪虽然都是侵犯计算机信息系统安全的行为，但二者之间存在明显界限：(1) 犯罪心态不同。前者犯罪心态既可能是直接故意，也可能是间接故意，后者只能是直接故意。(2) 危害行为不同。前者是以四种行为方式破坏计算机信息系统功能的行为，后者是未经授权侵入计算机信息系统的行为。(3) 犯罪对象不同。前者的犯罪对象可以是所有类型的计算机信息系统，而后者仅限于国家事务、国防建设、尖端科学技术领域的计算机信息系统。(4) 对危害结果的要求不同。前者是结果犯，要求行为人的行为造成计算机信息系统不能正常运作，并产生严重后果，而后者是行为犯，只要行为人实施了侵入行为，就构成犯罪既遂，不要求有另外的危害结果。(5) 犯罪构成类型不同。前者有基本罪和重罪两个构成类型，基本罪的法定最高刑为 5 年有期徒刑，重罪的法定最高刑为 15 年有期徒刑，后者是单一构成类型，法定最高刑为 3 年有期徒刑。

3. 本罪的未完成犯罪形态问题

关于本罪的未完成犯罪形态，有学者认为，行为人虽然实施了破坏计算机信息系统的行为，但没有发生严重的后果，就不能认为是犯罪①。作者认为，行为人破坏非重要的计算机信息系统的功能，或者破坏重要领域计算机信息系统的非重要的功能，没有引起严重后果的，属于情节显著轻微、危害不大的行为，不能认为是犯罪；我国刑法对国家事务、国防建设、尖端科学技术领域的计算机信息系统安全予以特殊保护，行为人非法侵入以上三类计算机信息系统的即被认为是具有严重社会危害性的行为，如果行为人破坏国家事务、国防建设、尖端科学技术领域计算机信息系统的重要系统功能，由于行为人意志以外的因素，如破坏行为被及时发现和制止危害后果的发生，没有造成严重后果的，不能认为属于情节显著轻微、危害不大的行为，应当构成为本罪的未遂犯；如果行为人破坏以上三类计算机信息系统功能，在严重危害结果发生前自动放弃犯罪或者自动有效制止严重危害结果发生，应按中止犯处理。行为人准备破坏计算机信息系统功能的条件，而尚未着手实施危害行为的，由于对计算机信息系统功能尚未构成直接的现实的威胁和危害，属于情节显著轻微、危害不大的行为，不构成犯罪，因此本罪无预备犯。

4．一罪与数罪问题

（1）本罪与非法侵入计算机信息系统罪。本罪的危害行为是破坏计算机信息系统功能，不一定要求有违反国家规定侵入计算机信息系统的行为，如计算机信息系统管理人员出于报复的目的，破坏计算机信息系统功能。行为人以破坏计算机信息系统功能为目的，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，并破坏计算机信息系统功能后果严重的，构成非法侵入计算机信息系统罪和破坏计算机信息系统功能罪，按处罚牵

① 周道鸾、张军主编：《中国新刑法释论与罪案》（下），中国方正出版社 1997 年版，第 612 页。

连犯的原则，从一重罪处罚；行为人侵入以上三类特定计算机信息系统后，产生了破坏计算机信息系统功能的故意，并实施破坏行为，后果严重的，构成非法侵入计算机信息系统罪和破坏计算机信息系统功能罪，进行数罪并罚。

（2）本罪与破坏公用电信设施罪。电信企业、互联网络信息提供企业（ICP）建立在计算机、网络技术基础上，计算机信息系统在这些行业应用程度很高，是这些企业提供公用电信服务的关键设备设施，行为人破坏这种计算机信息系统功能，造成计算机信息系统不能正常运行，后果严重并且危害公共安全的，同时构成破坏公用电信设施重罪和破坏计算机信息系统功能基本罪，这种情况属于法规竞合，应该按照从一重罪定罪处罚，即以破坏公用电信设施罪定罪处罚；如果尚未危害公共安全的，虽然造成严重后果，只构成破坏计算机信息系统功能罪。

（3）本罪与故意毁坏财物罪。计算机资产是信息时代的一种重要财富，计算机硬件设备设施在法律意义上属于财产为人们所公认，而计算机里存储的信息资源和计算机信息系统功能往往不被认为是财产的一种。实际上，一些重要计算机信息系统的信息资源和功能的价值要远远超过计算机硬件设备设施的价值，它们一旦遭到破坏造成的损失要超过硬件设备设施的价值。利用物理破坏手段破坏计算机信息系统，导致计算机信息系统功能被破坏，后果严重的，应该如何处理？有学者认为可以按照故意毁坏财产罪处理①。作者认为，对于这类行为不能一概而论，应区别对待，对于行为人故意毁坏计算机硬件设备设施，而没有破坏计算机信息系统功能的目的的，根据计算机硬件设备设施的损失情况和因计算机信息系统功能和信息资源所遭到的破坏程度，以故意毁坏财产罪论处；对于行为人为破坏计算机信息系统功能，而

① 于志刚：《计算机犯罪研究》，中国检察出版社 1999 年版，第 124 页。

采用物理破坏计算机信息系统的手段实施破坏，后果严重的，应该以破坏计算机信息系统功能罪定罪处罚。

（4）本罪与破坏生产经营罪。行为人出于泄愤报复等个人目的，破坏用于生产经营的计算机信息系统功能，如电子商务计算机信息系统功能，后果严重的，构成破坏生产经营罪和破坏计算机信息系统功能罪的法条竞合，择一重罪定罪处罚；如果没有造成严重后果的，则构成破坏生产经营罪。

（5）本罪与为毁灭罪证等目的破坏计算机信息系统功能的犯罪。行为人实施其他犯罪如窃取电子资金，在计算机信息系统中留下了作案的痕迹和罪证，为毁灭罪证而实施破坏计算机信息系统功能，造成严重后果的，应如何处理？例如四川省某市银行计算机操作员谢某，伙同他人侵入金融计算机系统，诈骗人民币87万元，作案后谢某又将该计算机信息系统功能加以修改、删除，企图抹去作案痕迹，造成计算机信息系统不能正常运行，后果十分严重。对于谢某的行为，有学者认为，应该按照诈骗罪和破坏计算机信息系统功能罪进行并罚①。作者赞同这种观点。

根据《刑法》第286条第1款规定，犯本罪基本罪的，处5年以下有期徒刑或者拘役；犯重罪的，处5年以上有期徒刑。在对基本罪和重罪适用刑罚时，还应考虑犯罪的其他情节，在法定刑范围内予以从轻或者从重，这些情节包括：被破坏的计算机信息系统及其功能的重要性程度；因破坏计算机信息系统功能而导致后果的严重程度，社会影响恶劣程度；行为人主观恶性程度，以及影响量刑轻重其他方面的情节。

① 高铭暄、赵秉志主编：《刑法论丛》（第1卷），法律出版社1998年版，第79页。

第四节 破坏计算机信息系统数据或应用程序罪

一、破坏计算机信息系统数据或应用程序罪的概念与犯罪构成

破坏计算机信息系统数据或应用程序罪，是指违反国家规定，对计算机信息系统中存储、处理或者传输的数据或应用程序进行删除、修改、增加操作，造成法定后果的行为。

《刑法》第 286 条第 2 款规定，实施以上行为，后果严重的，依照该条第 1 款的规定处罚。《刑法》第 286 条第 2 款规定的是单一的构成类型，还是复合的构成类型？有学者认为，破坏计算机信息系统数据、应用程序，不但会引起“后果严重”的情形，而且还可能引起“后果特别严重的”情形，既然存在破坏“后果特别严重”的情形，如果不加重其法定刑就令人难以理解。因此，对于《刑法》第 286 条第 2 款规定之罪，只有扩大解释为涵盖“后果特别严重”，才符合立法本意。毋庸讳言，本款在文字表述上是存在严重缺陷的，正确的表述应当是：“违反国家规定，对计算机信息系统中存储、处理或传输的数据或应用程序进行删除、修改、增加的操作，后果严重或后果特别严重的，依照前款的规定处罚。”① 作者同意这种观点，并认为《刑法》第 286 条三个条款规定的三种犯罪，其刑罚立法模式应该是完全相同的，如果理解为仅本条第 1 款有重罪，而其余两个条款规定的犯罪无重罪，与立法原意不符，在司法实践中必然导致轻纵犯罪。

基于以上理由，本罪应该是复合构成类型，分为基本罪和派

① 赵廷光、朱华池、皮勇：《计算机犯罪的定罪量刑》，人民法院出版社 2000 年版，第 205 页。

生的重罪两个构成类型，相应的具有两个法定刑档次。

（一）基本罪构成要件

本罪的基本罪是结果犯，由一般主体、犯罪故意、单一危害行为、特定犯罪前提、特定犯罪结果、特定犯罪对象、被害法益7个构成要件组成，其具体内容和形式分述如下：

1．一般主体

本罪的主体是一般主体，即年满16周岁具有刑事责任能力的自然人。未满16周岁的自然人实施本罪规定行为的，不构成本罪。本罪无单位犯罪。境外中国公民和外国人实施本罪行为，破坏我国计算机信息系统的，适用我国刑法，构成本罪。

2．犯罪故意

本罪在犯罪心态上表现为故意，即明知自己在实施删除、修改、增加计算机信息系统数据、应用程序的行为，可能造成严重的危害后果，希望或者放任这种危害后果发生的心理态度。过失不构成本罪。在实践中，较多表现为直接故意。其犯罪目的、动机如何，不影响本罪的成立。

3．单一危害行为

本罪是单一危害行为，表现对计算机信息系统数据、应用程序进行破坏性操作的行为，该行为可以有三种选择性行为方式，即删除、修改、增加操作，只要行为人实施其中任何一种行为方式，都构成本罪的破坏性操作行为，行为人同时实施两种以上行为方式的，仍然只构成一罪，而不实行数罪并罚。本罪的“删除、修改、增加”不同于破坏计算机信息系统功能罪的“删除、修改、增加”，本罪的以上行为方式仅限于“删除、修改、增加的操作”，即调用计算机命令、应用程序，对计算机信息系统数据、应用程序进行删除、修改、增加，而不能使用物理性破坏方法来破坏计算机信息系统数据、应用程序。同时，这里的“删除、修改、增加”不能理解为计算机科学里的删除命令、修改命令和增加命令，而是对作为犯罪目标的计算机信息系统数据、应

用程序的影响方式。

所谓删除，是指使计算机信息系统数据、应用程序的全部或者一部分丧失。删除的具体方法根据计算机信息系统所使用的计算机设备型号和计算机操作系统的不同而不同，并且对于每一类计算机信息系统都可能有多种删除方法，既可以直接调用操作系统命令予以删除，如 WINDOWS 系统中的 FORMAT（格式化命令）和 DELETE（删除命令），也可以利用各种有删除计算机数据、应用程序功能的应用程序进行删除。

所谓修改，是指对计算机信息系统数据、应用程序原状进行改动的行为，既可能是改动其中一部分，也可能使其完全改变；既可能只改动计算机数据或者应用程序其中任何一种，也可能使两种都改动；既可能是改动计算机数据、应用程序的内容或者数据形式，也可能使两者都改动。行为人对计算机数据、应用程序进行加密处理，使计算机数据、应用程序文件由明文变成密文，虽然只是改变了数据形式，数据所反映的信息内容没有改变，但使这些计算机数据、应用程序不能正常使用，也应该属于修改方法的一种。例如某计算机集团一位项目主管人员，擅自把公司的档案全部加密，致使该公司只好又用半年多的时间重新研究设计。

所谓增加，是指向计算机信息系统中增添原先没有的计算机数据、应用程序。向计算机信息系统增加计算机数据、应用程序，造成的影响可能有多种，如大量的垃圾数据占据计算机硬盘，消耗计算机信息系统的存储空间，使计算机信息系统的正常数据得不到存储空间，或者增加的控制数据改变了相关功能程序的正常处理、传输、存储。增加应用程序既可能占用计算机信息系统的资源，使计算机信息系统正常处理能力受到影响，也可能进行不利于计算机信息系统所有人权利的处理。

有学者认为，破坏计算机信息系统数据和应用程序的方法，除了“删除、修改、增加”之外，还有损坏（就部分而言）、毁

灭（就整体而言）、瓦解（致使数据或应用程序处于混乱状态）、隐匿等方法，计算机病毒和其他破坏性程序也是本罪的常用手段①。有的学者对此进行了反驳，认为本罪的犯罪方法是法定的，因而根据罪刑法定主义原则，只有使用上述“删除、修改、增加”三种行为方式才能以本罪论处，因而使用其他犯罪方法的，要么不构成本罪，要么在实质上属于这三种犯罪方法之一②。还有学者认为，“删除、修改、增加”是本罪危害行为的表现形式，通常称为行为方式，表现为这三种形式的危害行为，可以采取各种不同的方法实施，刑法对某些具体犯罪要求以特定的方法实施，对某些犯罪的实施则不加以限定。《刑法》第 286 条第 2 款只限定了犯罪的行为方式，而对犯罪的具体方法没有限制，这就是说，不论以何种方法实施这三种形式的行为，都不影响本罪的成立。至于第一种观点所说的对数据和应用程序的“损坏”、“毁灭”、“瓦解”，应视危害后果；“隐匿”应该视为一种修改方法或者删除方法；“计算机病毒或其他破坏性程序”，则是制作、传播计算机病毒等破坏性程序罪的行为对象，利用它们破坏计算机数据和应用程序，实际上是以“传播”的行为方式实施这种犯罪，破坏计算机信息系统中的数据和应用程序则是该罪的危害后果，因此，不能将利用“计算机病毒或者其他破坏性程序”视为本罪的一种犯罪手段③。作者认为，《刑法》第 286 条第 2 款只规定了本罪的三种行为方式，非以上三种行为方式的行为不能构成本罪，但是没有限定具体的犯罪方法，具体犯罪方法可能

① 胡国平：《关于四种计算机犯罪的认定》，《法律科学》，1997 年第 4 期；陈兴实、付东阳：《计算机、计算机犯罪、计算机犯罪的对策》，中国检察出版社 1998 年版，第 83 页。

② 高铭暄、赵秉志主编：《刑法论丛》（第 1 卷），法律出版社 1998 年版，第 77～82 页。

③ 赵廷光、朱华池、皮勇著：《计算机犯罪的定罪量刑》，人民法院出版社 2000 年版，第 202 页。

有多种。计算机病毒和其他破坏性程序，从其性质来看，也属于应用程序，行为人向目标计算机信息系统中施放这类应用程序，是向计算机信息系统增加应用程序的行为，如果造成严重后果，构成本罪，同时，向计算机信息系统施放计算机病毒等破坏性程序的行为，构成施放破坏性计算机程序罪，这种情况属于刑法理论中的法规竞合，适用施放破坏性计算机程序罪的条款规定定罪量刑，而排斥本罪条款的适用。

4．特定犯罪前提

本罪的特定犯罪前提是违反国家规定。这里的国家规定，主要指《军队通用计算机系统使用安全要求》、《计算机信息系统安全保护条例》、《计算机信息网络国际联网管理暂行规定》、《计算机信息网络国际联网管理暂行规定实施办法》、《计算机信息网络国际联网安全保护管理办法》、《计算机信息系统保密管理暂行规定》、《金融机构计算机信息系统安全保护工作暂行规定》、《国际互联网出入信道管理办法》、《计算机信息系统国际联网保密管理规定》等。如果行为人没有违反有关国家规定，则不构成本罪。

5．特定犯罪结果

本罪是结果犯。行为人破坏计算机信息系统中存储、处理或者传输的数据和应用程序，造成严重后果的，才能构成本罪基本罪的既遂。构成本罪，行为人的行为与严重后果必须具有因果关系。这里的“后果严重”，不应该包括因为造成计算机信息系统功能被破坏，计算机信息系统不能正常运行而导致的严重后果，即要排除破坏计算机信息系统功能罪的特殊犯罪后果，否则构成破坏计算机信息系统功能罪而非本罪。“后果严重”的具体内容，法律没有规定，有待司法解释予以明确，但是从刑法理论联系司法实践来看，主要包括以下情形：(1) 造成被害人巨大的经济损失的；(2) 被害人工作、生产经营受到严重影响；(3) 造成恶劣的社会影响等。

6．特定犯罪对象

本罪的犯罪对象是计算机信息系统中存储、处理或者传输的数据和应用程序。数据这一概念，有一个发展的过程，在计算机发明和应用早期，仅指计算机数值和字符，随着计算机技术和应用的发展，数据的概念不断扩展，广义的数据指计算机及计算机网络中的所有数字化的信息，不仅包括数值和字符，还包括文字、图像、声音、影像的数字化信号。计算机程序实际上是由 1 和 0 这样的比特位符号组成，也属于广义上数据的范畴。狭义上的数据仅指非计算机程序的数字化信息，本罪的数据概念是指狭义上的数据。

所谓计算机程序，根据《计算机软件保护条例》第 3 条规定，是指“为了得到某种结果而可以由计算机等具有信息处理能力的装置执行的代码化指令序列，或者可被自动转化成代码化指令序列的符号化指令序列或者符号化语句序列。计算机程序包括源程序和目标程序。同一程序的源文本和目标文本应当视为同一作品。”计算机程序相对于计算机数据而言，范围十分广泛，既包括操作系统程序，也包括其他的应用程序。所谓应用程序，是指操作系统程序以外的，为特定的目的而设计、编写的具有某种特定用途的计算机程序。

本罪的数据和应用程序必须是“计算机信息系统中存储、处理或者传输的数据和应用程序”，不能由计算机信息系统进行存储、处理或者传输的，与计算机信息系统分离的存储器中的数据和应用程序不属于本罪的犯罪对象，如作为备份而另外存放的光盘、磁盘、磁带、磁鼓等存储器中的数据和应用程序。需要特别指出的是，与计算机信息系统连接的只读光盘驱动设备中的数据和应用程序，不是本罪的犯罪对象，因为虽然它们可以由计算机处理和传输，但是，由于只读光盘中的数据和应用程序不可被修改，它们不能被行为人删除、修改或者增加。

有学者认为，虽然《刑法》第 286 条第 2 款表述的犯罪对象是“计算机信息系统中存储、处理和传输的数据和应用程序”，

但是，本罪的犯罪对象应当是选择性的，即可以是数据，也可以是应用程序，只要破坏其中一种，便可构成本罪，不应要求两者都同时破坏。《刑法》第 286 条第 2 款中的“数据和应用程序”一语，应当限制解释为“数据”或者“应用程序”，否则，就会放纵那些只破坏数据而没破坏应用程序，或者只破坏应用程序而没破坏数据，并且后果严重的行为，这显然与立法本意相悖，建议修改刑法时予以纠正。

7. 被害法益

本罪的被害法益是复合的，包括计算机信息系统安全保护管理秩序、计算机信息系统所有人的合法权利和被害人正常的工作、生产经营秩序。

（二）重罪构成要件

本罪的重罪是结果加重犯，指罪行在符合基本罪构成要件的基础上，后果特别严重的行为。至于何谓后果特别严重，有待司法解释作出规定，但从刑法理论联系司法实践来分析，主要是指：(1) 破坏国家事务、国防建设、尖端科学技术领域的计算机信息系统数据和应用程序，后果严重的；(2) 破坏较广泛范围内的或者较多的计算机信息系统数据和应用程序的全部或者一部分的；(3) 造成被害人特别巨大的经济损失；(4) 对被害人工作、生产经营活动影响特别严重；(5) 造成特别恶劣的社会影响等。

二、认定破坏计算机信息系统数据或应用程序罪应该注意的问题

1. 本罪与非罪的界限

区别本罪与非罪，关键要注意两个方面：首先，行为人主观上是否出于故意。在计算机使用过程中，不能完全避免因误操作而错误删除、修改或者删除计算机信息系统数据和应用程序的情况，过失造成严重后果的，不以犯罪论处。其次，看行为人的行为是否破坏了计算机信息系统数据或应用程序，并造成严重后

果。如果行为人的行为与严重后果没有因果关系，或者造成的后果不严重，都不能追究行为人的刑事责任，不构成本罪既遂。

2．本罪与他罪的界限

（1）本罪与非法侵入特定计算机信息系统罪的界限

两罪虽然都是侵犯计算机信息系统安全的行为，但二者之间存在明显界限：①犯罪心态不同。前者犯罪心态既可能是直接故意，也可能是间接故意，后者只能是直接故意。②危害行为不同。前者是以三种行为方式破坏计算机信息系统数据、应用程序的行为，后者是未经授权侵入计算机信息系统的行为。③犯罪对象不同。前者的犯罪对象可以是所有类型的计算机信息系统，而后者仅限于国家事务、国防建设、尖端科学技术领域的计算机信息系统。④对危害结果的要求不同。前者是结果犯，行为人的破坏计算机信息系统数据、应用程序的行为造成严重后果，而后者是行为犯，只要行为人实现了侵入行为，就构成犯罪既遂，不要求有另外的危害结果。⑤被害法益不同。前者是计算机信息系统安全保护管理秩序、计算机信息系统所有人的合法权利和被害人正常的工作、生产经营秩序，而后者是国家对计算机信息系统安全管理秩序、国家的保密制度和国家事务、国防建设、尖端科学技术领域的正常活动。⑥犯罪构成类型不同。前者有基本罪和重罪两个构成类型，基本罪的法定最高刑为 5 年有期徒刑，重罪的法定最高刑为 15 年有期徒刑，后者是单一构成类型，法定最高刑为 3 年有期徒刑。

（2）本罪与破坏计算机信息系统功能罪的界限

本罪与破坏计算机信息系统功能罪的界限在于：①危害行为不同。本罪的危害行为只有三种行为方式，并且只能采取操作计算机命令或者应用程序的方式，实现删除、修改或者增加；后者的危害行为可以有删除、修改、增加和干扰四种行为方式，并且不限于计算机操作的方法，可以采取物理破坏计算机硬件设备的方法。②犯罪对象不同。本罪的犯罪对象是计算机信息系统数据

或应用程序，后者是计算机信息系统功能。③犯罪后果不同。后者的犯罪后果是造成计算机信息系统不能正常运行，并有严重后果；本罪的犯罪后果是除后者犯罪后果外的其他严重后果。④本罪保护的重点是计算机信息系统中的数据和应用程序，后者保护的重点是计算机信息系统功能的正常发挥。

3．本罪的未完成犯罪形态问题

行为人破坏计算机信息系统数据、应用程序，没有造成严重后果，并且没有其他严重情节的，属于情节显著轻微危害不大的行为，不能认为是犯罪。由于我国刑法对国家事务、国防建设、尖端科学技术领域的计算机信息系统安全予以特殊保护，行为人非法侵入以上三类计算机信息系统的即被认为是具有严重社会危害性的行为，如果行为人破坏国家事务、国防建设、尖端科学技术领域计算机信息系统的重要数据、应用程序，由于行为人意志以外的因素，如破坏行为被及时发现和制止危害后果的发生，没有造成严重后果的，不能认为属于情节显著轻微、危害不大的行为，应当构成本罪的未遂犯。如果行为人破坏以上三类计算机信息系统的数据或者应用程序，在严重危害结果发生前，自动放弃犯罪、有效制止法定危害结果发生的，应按中止犯处理。行为人准备破坏计算机信息系统的条件，而尚未着手实施危害行为的，由于对计算机信息系统尚未构成现实的威胁，属于情节显著轻微危害不大的行为，不构成犯罪，因此本罪无预备犯。

4．一罪与数罪问题

行为人以破坏计算机信息系统数据、应用程序为目的，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，并破坏计算机信息系统数据、应用程序，后果严重的，构成非法侵入计算机信息系统罪和破坏计算机信息系统功能罪的牵连犯，按从一重罪原则处罚。行为人侵入以上三类特定计算机信息系统后，产生了破坏计算机信息系统数据、应用程序的故意，进行破坏行为，造成严重后果的，构成非法侵入计算机信息系统罪和破

坏计算机信息系统数据或应用程序罪，进行数罪并罚。

根据《刑法》第 286 条第 2 款和第 1 款规定，犯本罪基本罪的，处 5 年以下有期徒刑或者拘役；犯重罪的，处 5 年以上有期徒刑。在对基本罪和重罪适用刑罚时，还应考虑犯罪的其他情节，在法定刑范围内予以从轻或者从重，这些情节包括：被破坏的计算机信息系统和数据、应用程序的重要性程度；因破坏计算机信息系统功能而导致后果的严重程度，社会影响恶劣程度；行为人主观恶性程度以及影响量刑轻重其他方面的情节。

第五节　施放破坏性计算机程序罪

一、施放破坏性计算机程序罪的概念与犯罪构成

施放破坏性计算机程序罪，是指故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，具有法定后果的行为。

基于与上一节破坏计算机信息系统数据或应用程序罪相同的理由，本罪应该是复合构成类型，分为基本罪和派生的重罪两个构成类型，具有相应的两个法定刑档次。

（一）基本罪构成要件

本罪的基本罪是结果犯，由一般主体、犯罪故意、单一危害行为、特殊犯罪结果、犯罪对象、被害法益 6 个构成要件组成，其具体内容和形式分述如下：

1. 一般主体

本罪的主体是一般主体，即年满 16 周岁具有刑事责任能力的自然人。与单纯传播计算机病毒等破坏性程序的行为人相比，能制作计算机病毒等破坏性程序的行为人技术水平较高，大多有一定的计算机编程技能，熟悉计算机病毒及其他破坏性程序的设计、工作原理。有学者认为，鉴于病毒等破坏性程序可能带来的

严重后果，已满 14 周岁未满 16 周岁的人也应成为本罪主体，对其犯罪行为承担相应的刑事责任；单位犯本罪的，应当首先追究单位的刑事责任①。作者认为，由于上文所述原因，未满 16 周岁的自然人实施本罪规定行为的，不构成本罪，本罪无单位犯罪。境外中国公民和外国人实施本罪行为破坏我国计算机信息系统的，适用我国刑法，构成本罪。

2. 犯罪故意

关于本罪的罪过形式，存在不同观点。(1) 制作计算机病毒等破坏性程序是否只能出于故意？有学者认为，传播计算机病毒等破坏性程序，既可能是故意，也可能存在过失或者意外事件，但是，对于制作这类程序而言，所有计算机病毒等破坏性程序均是故意行为的产物，换言之，制作破坏性程序的行为只能是出于故意，而不可能是出于过失或者属于意外事件。同时，这位学者又认为，“只要您在撰写程序时，不小心产生了一个 BUG，而这个 BUG 将导致计算机系统不正常运作，更糟糕的是您并不知情，于是您也制造了一个‘特洛伊木马’程序，像这种情况屡见不鲜”②。“特洛伊木马”程序是破坏性程序的一种，在“不知情”的情况下制造这种程序，主观上显然不是故意，可见，由于计算机程序编写的特点，行为人不出于故意也可以制造出计算机病毒等破坏性程序。(2) 过失传播计算机病毒等破坏性程序能否构成本罪？有学者认为，“鉴于计算机本身的特点和计算机病毒等破坏性程序可能带来的严重后果，应把设计者能够发现识别善意程序中的病毒而由于职务上的疏忽、懈怠而竟未识别出来，以致病毒等破坏性程序传染并造成严重后果的主观过错——过失，

① 刘广三：《计算机犯罪论》，中国人民大学出版社 1999 年版，第 189 页。

② 于志刚：《计算机犯罪研究》，中国检察出版社 1999 年版，第 147、158 页。

定为本罪的主观方面之一，从而在一定程度上避免病毒等破坏性程序的产生和传播，防止危害结果的发生”①。作者认为本罪无过失犯，这是因为如果将过失传播行为犯罪化，虽然在一定程度上可以促进人们加强安全管理意识，减少破坏性程序流向社会的机会，但这一措施过于严厉，可能阻碍计算机病毒的正常研究工作，而且，要达到以上效果完全可以通过加强行政管理来实现，采用刑法手段防止这类行为，实际效果并不大。

行为人故意、过失或者意外事故都可能导致破坏性程序的产生和传播，但构成本罪，在犯罪心态上只能为故意，即明知自己在实施制作、传播计算机病毒等破坏性程序的行为，可能影响计算机系统的正常运行，造成严重的危害后果，而希望或者放任这种危害后果的心理态度。过失和意外事故不构成本罪。犯罪目的、动机如何，不影响本罪的成立。

3．单一危害行为

《计算机信息系统安全保护条例》第 15 条规定，“对计算机病毒和危害社会公共安全的其他有害数据的防治工作，由公安部归口管理”，《计算机信息系统安全专用产品检测和销售许可证管理办法》第 15 条规定，“防治计算机病毒的安全专用产品须提交公安机关颁发的计算机病毒防治研究的备案证明”，因此，从事计算机病毒等破坏性程序研究防治的公司、企业、研究所等单位或者个人，必须获得公安机关颁发的计算机病毒防治研究的备案证明，未获公安部批准制作计算机病毒等破坏性程序的行为属于违法行为。《计算机信息系统安全保护条例》第 23 条规定，“故意输入计算机病毒以及其他有害数据危害计算机信息系统安全的”为应受行政处罚的违法行为。可见，擅自故意制作、传播计算机病毒等破坏性程序的行为属于违法行为。

---

① 刘广三：《计算机犯罪论》，中国人民大学出版社 1999 年版，第 190 页。

关于计算机病毒的概念和特点，在前面从计算机科学和犯罪学角度对其进行了研究。根据《计算机信息系统安全保护条例》第 28 条规定，我国刑法中的计算机病毒是指“编制或者在计算机程序中插入的破坏计算机功能或毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码”。其具有以下特征：(1) 计算机病毒是行为人编制或者插入其他计算机程序的计算机程序、计算机指令或者程序代码，其本身也是正常的计算机指令或者程序代码；(2) 计算机病毒的攻击对象是计算机功能或者计算机系统中的数据，包括各种计算机程序；(3) 计算机病毒危害计算机系统的正常运行；(4) 计算机病毒能够自我复制，进而传染破坏其他计算机信息系统。所谓破坏性程序，是指破坏计算机信息系统安全的计算机程序，计算机病毒以外的其他破坏性程序具有上述前三个特征。

本罪的危害行为是选择性行为，即故意制作、传播计算机病毒等破坏性程序的行为，行为人故意实施两种行为方式中的任何一种，都可以构成本罪，行为人同时实施两种行为即制作并传播计算机病毒等破坏性程序的，也以本罪论处，不构成数罪并罚。本罪的行为对象是计算机病毒等破坏性程序。

所谓制作，是指出于破坏计算机信息系统功能、数据或者应用程序的目的，在他人或单位（含本单位）的计算机上编制病毒等破坏性程序，影响该计算机信息系统正常运行的行为。这里的制作已经包含了“传播”行为。

关于本罪“制作”行为的概念，有学者提出不同观点，并举案例进行分析：某研究所研究人员张某，自信自己的计算机技术一流，因而对于市场上出现的各种杀毒软件不屑一顾，认为所有的杀毒软件都是骗人的，为了检验自己的看法，张某自己精心设计了一个计算机病毒，然后将市场上所有的杀毒软件全部买来进行杀毒实验，结果证明无法清除其所设计的病毒。不久，张某将此事忘记，也未向他人提起。数月后，张某自己的计算机硬盘出

现故障，张某和计算机供应商联系后更换了一个硬盘，却忘记了所退回的硬盘上还存有其所设计的计算机病毒，该硬盘经修理后卖给某省一个机关，该机关试用数月后，原存留于计算机内的病毒发作，并感染该机关内部联网的所有计算机，将计算机内部所存储的数据和应用程序全部清除，导致损失数百万元。由于该计算机病毒上留有张某的名字，公安机关据此将其抓获。该学者认为，张某对其所设计的计算机病毒的扩散，显然出于疏忽大意的过失，当然不构成犯罪，但是，“制作、传播计算机病毒等破坏性程序是一个选择性的罪名，只要行为人具备了制作或者传播两个行为之一，并且造成了影响计算机系统正常工作的严重后果的，即可构成犯罪，因而张某的传播行为虽然不构成犯罪，但是其故意制作计算机病毒的行为则显然已经构成了故意制作破坏性计算机程序罪，因而应当依法以本罪追究刑事责任”①。显然，该学者把在自己的计算机上制作计算机病毒等破坏性程序的行为纳入本罪危害行为的范围。还有学者认为，要造成危害后果，仅仅制作计算机病毒是不可能达到目的的，还必须将病毒输入计算机系统内部并扩散，才会造成直接对计算机系统的严重危害后果②。作者认为，这两种观点各有值得肯定的部分，同时又都忽略了“制作”行为对象的特殊性。行为人在他人的计算机信息系统上制作计算机病毒等破坏性程序，直接危害该计算机信息系统安全，这种行为当然属于本罪的危害行为。同时，如果行为人在自己的计算机上编写计算机病毒等破坏性程序，而不加以传播，不可能影响他人计算机信息系统正常运行，并产生严重后果，不能构成犯罪，而只是违反国家有关行政法规的违法行为。行为人

① 于志刚：《计算机犯罪研究》，中国检察出版社 1999 年版，第 149 页。

② 孙铁成：《计算机犯罪的罪名及其完善》，《中国法学》，1998 年第 1 期。

制作计算机病毒等破坏性程序不一定都属于本罪的危害行为，其制作的目的也不一定是为了传播出去造成危害。有学者认为“制作行为的最终目的是通过传播病毒来造成损害，所有制作行为中必然包括传播的行为，传播为制作这一主行为所吸收”①，这种观点是站不住脚的，该案例即是最好的反驳。该案中张某故意制作计算机病毒的行为是违法行为，应该依法进行行政处罚，其过失传播计算机病毒的行为不构成犯罪，造成的损失可以通过民事诉讼进行处理。

制作计算机病毒等破坏性程序有两种方式：(1) 创造新的计算机病毒等破坏性程序。所谓创造新的计算机病毒等破坏性程序，是指行为人利用某种计算机语言编制原先没有的计算机病毒等破坏性程序。(2) 改造已有的计算机病毒等破坏性程序。改造出来的计算机病毒等破坏性程序，被称为原来破坏性程序的变种。如 2000 年 5 月肆虐一时的“爱虫”病毒，在很短的时间就有多达 29 种变种“爱虫”，它们危害程度各不相同，其隐蔽性和恶性要远远超过原版“爱虫”病毒。改造计算机病毒等破坏性程序的另一种形式是，复合多种计算机病毒等破坏性程序，生成具有多种破坏性程序综合特性的新破坏性程序。不管行为人采取哪种方式制作破坏性程序，只要制作出来的计算机程序属于破坏性程序，其行为构成本罪的制作行为。

所谓传播，是指行为人故意将自己或他人制作的计算机病毒等破坏性程序，直接或者间接输入他人计算机信息系统，或者将携带计算机病毒等破坏性程序的计算机程序和数据文件及其载体，加以散发、销售，或者将计算机病毒等破坏性程序原代码予以公开的行为。一般而言，只有使他人计算机信息系统遭受破坏性程序直接危害或者现实威胁的传播行为，才能构成本罪的危害

① 刘广三：《计算机犯罪论》，中国人民大学出版社 1999 年版，第 187 页。

行为，因此，行为人向自己的计算机中输入破坏性程序，而非意图危害他人计算机信息系统的，不构成本罪的危害行为。但是，行为人明知自己计算机信息系统中的破坏性程序可能传播给他人的计算机信息系统（如利用共享网络资源或者利用软盘交换数据传播给他人计算机信息系统，希望或者放任这种危害结果发生），其向自己计算机输入破坏性程序的行为，实际上是间接向他人计算机传播破坏性程序，也构成本罪的危害行为。计算机程序包括源程序和目标程序，破坏性程序也是一种计算机程序，散发、销售、公开破坏性程序源程序和目标程序的行为，当然属于本罪的危害行为。传播计算机病毒等破坏性程序的具体方式有多种，主要有：(1) 通过软盘或者光盘向目标计算机信息系统传播；(2) 通过电子邮件向他人电子邮件邮箱中发送破坏性程序；(3) 通过电子公告栏散布或交换破坏性程序；(4) 通过病毒交换网交换破坏性程序，这类病毒交换网有 Vx-Net、NukEnet、维吉尼亚病毒研究所等；(5) 通过病毒分配网站传播、交换破坏性程序；(6) 通过病毒分配机器人和文件服务器中的自动文件分配程序传播破坏性程序；(7) 通过书籍刊载破坏性程序的代码进行传播；(8) 销售破坏性程序。

4. 犯罪对象

本罪的犯罪对象是他人的计算机系统，直接攻击对象是计算机信息系统功能、数据或者各种计算机程序。我国法律没有规定计算机系统的定义，这里的计算机系统应该与前文所述的“计算机信息系统”有相同的含义。

5. 特殊犯罪结果

本罪是结果犯。行为人的危害行为必须影响了计算机系统的正常运行，并且造成严重后果，两者缺一不可。其一，如果没有影响计算机系统的正常运行，即使因行为人的危害行为造成了严重后果，如行为人传播能够窃密的计算机程序，窃取他人重要商业秘密，给他人造成巨大经济损失，但是没有妨碍该计算机系统

的正常运行，不能构成本罪要求的犯罪结果。其二，如果因行为人的危害行为影响了计算机系统的正常运行，但是尚未造成严重后果，也不是本罪要求的特殊犯罪结果。其三，构成本罪的行为人的危害行为还必须与计算机系统的不能正常运行及严重后果具有因果关系。

关于本罪是否需要造成严重后果，学者间有不同观点。有人认为，《刑法》第 286 条没有必要将后果严重作为构成要件，只要实行了制作和传播计算机病毒的行为，就可以构成犯罪①。但有人对此持否定态度，认为以上观点将扩大打击面，是重刑主义的表现。同时，对于某一种程序是否具有破坏性及其破坏性程度的法律判断，只能是此种程序已经造成了社会危害，对尚未发生作用的破坏性程序进行危害性评价，司法成本过高，也缺乏司法介入的依据。另外，如果仅仅制作、传播即应当以犯罪论处，则造成严重后果的行为是否应当加重处罚呢？此种立法建议可能导致不必要的刑罚攀升②。作者认为，制作、传播某些传染性很强、破坏力很大的破坏性程序，可能导致很大范围内的计算机信息系统遭受破坏，其社会危害性要比针对特定计算机信息系统的破坏行为要大得多，对这种行为加重其刑罚，符合刑责相适应原则。同时，破坏性程序千差万别，并非所有的破坏性程序都有特别大的破坏力，有些破坏性程序有一定的破坏能力，但实际可能造成的危害非常有限。如 1999 年 7 月一种名为“野兔”的电脑病毒在新西兰问世，英国舆论界对其可能造成的危害大加渲染，各抗电脑病毒公司也纷纷以特急件的方式向用户寄送抗该病毒的

---

① 孙铁成：《计算机犯罪的罪名及其完善》，《中国法学》，1998 年第 1 期；刘广三：《计算机犯罪论》，中国人民大学出版社 1999 年版，第 188 页。

② 于志刚：《计算机犯罪研究》，中国检察出版社 1999 年版，第 163 页。

软件，并说该病毒已从新西兰传播到美国、南非和欧洲，可能是世界上传染范围最广的一种电脑病毒。然而英国的电脑用户紧张了一番后，却几乎没有电脑遭到它袭击。电脑专家对该电脑病毒的研究发现，原来这种病毒是一种编制水平很低的病毒，它还没来得及复制自己并传染给其他电脑就发作了，一旦发作它把电脑中的所有文件包括它自己就都删除了，因而几乎无法传染①。如果把故意制作、传播实际危害程度各异的破坏性程序的行为，都当作犯罪行为处理，将使刑罚与危害行为的行为人的法律责任不对等，违反了刑责相适应原则，扩大了刑法的打击面和不必要地加重了行为人的刑罚。根据行为人所造成后果的严重程度，判断行为人的行为是否具有严重的社会危害性及其程度，是对行为人正确适用刑罚的重要依据。

“后果严重”的具体内容，法律没有规定，有待司法解释予以明确，但是从刑法理论联系司法实践来看，主要包括以下情形：(1) 造成被害人巨大的经济损失的；(2) 被害人工作、生产经营受到严重影响；(3) 造成恶劣的社会影响；(4) 致使计算机信息系统功能部分或者全部丧失；(5) 破坏计算机信息系统数据或者应用程序数量大，对计算机信息系统正常运行影响严重等。

5. 被害法益

本罪的被害法益是复合的，包括计算机信息系统安全保护管理秩序、计算机信息系统所有人的合法权利和被害人正常的工作、生产经营秩序。

（二）重罪构成要件

本罪的重罪是结果加重犯，指罪行在符合基本罪构成要件的基础上，后果特别严重的行为。至于何谓后果特别严重，有待司法解释作出规定，但从刑法理论联系司法实践来看，主要是指：

---

① 《历史上最拙劣的病毒》，http：//www.enews.com.cn/，2000 年 6 月 20 日。

(1) 行为人制作、传播计算机病毒等破坏性程序，破坏国家事务、国防建设、尖端科学技术领域的计算机信息系统，后果严重的；(2) 破坏较广泛范围或者较多的计算机信息系统数据的；(3) 造成被害人特别巨大的经济损失的；(4)对被害人工作、生产经营活动影响特别严重的；(5)造成特别恶劣的社会影响的等。

二、认定施放破坏性计算机程序罪应该注意的问题

1. 本罪与非罪的界限

区别本罪与非罪，关键要注意四个方面：

(1) 行为人主观上是否出于故意？计算机编程员由于技术不熟练或者出于疏忽，编写出破坏计算机信息系统的计算机程序，如该计算机程序被运行时可能导致计算机信息系统瘫痪，或者毁坏数据和应用程序等。对于这种情况，由于行为人主观上没有犯罪故意，不构成犯罪，同时也不是违法行为，而只是编程业务中的事故。行为人没有认识到传播的是计算机病毒等破坏性程序，或者虽然认识到可能传播计算机病毒等破坏性程序，但由于疏忽大意或者过于自信而导致破坏性程序传播出去的，如行为人虽然知道自己使用的磁盘曾被传染了计算机病毒，在从其他计算机信息系统复制数据时，错误地使用了该磁盘；或者利用一般杀毒软件对该染毒磁盘杀毒而实际上尚未清除病毒，在使用该磁盘时，致使感染其他计算机信息系统的，属于主观上的疏忽大意或过于自信的过失，不构成本罪。

(2) 行为人故意制作或者传播的是否为计算机病毒等破坏性程序，作为行为对象的计算机程序是否为破坏性计算机病毒等破坏性程序，可以根据《计算机信息系统安全保护条例》第 28 条有关计算机病毒的规定进行认定，具有规定相应特征的计算机程序就是计算机病毒，否则不是计算机病毒。非计算机病毒的计算机程序是否破坏性程序，可以通过分析其对计算机信息系统的作用来认定，具有破坏作用的是破坏性程序，反之则否。认定计算

机程序是否具有破坏作用，可以由法院聘请计算机科学的专家进行。判断计算机程序是否为破坏性程序时，应当将编程技术故障与制作破坏性程序区分开，行为人编写的计算机程序由于兼容性等技术方面的原因，在运行时可能造成的系统死机、系统资源过度消耗等情况的，属于技术故障而非破坏作用，这种计算机程序不是破坏性程序。

（3）行为人的危害行为是否引起计算机信息系统不能正常运行，并且造成严重后果，若非同时引起以上两种后果，并且这两种后果与其危害行为具有因果关系，不能构成本罪既遂。

（4）行为人在自己所有或者自己有管理使用权的计算机信息系统上故意制作、传播破坏性程序，即使造成计算机信息系统不能正常运行和严重后果，不构成本罪，只有在他人所有的非授权的计算机信息系统制作破坏性程序，或者向其直接或间接传播破坏性程序，造成以上后果的，才构成本罪。

2．本罪与他罪的界限

（1）本罪与非法侵入特定计算机信息系统罪的界限

两罪虽然都是侵犯计算机信息系统安全的行为，但存在明显界限：①犯罪心态不同。前者犯罪心态既可以是直接故意，也可能是间接故意，后者只能是直接故意。②危害行为不同。前者是故意制作、传播破坏性程序的行为，后者是未经授权侵入计算机信息系统的行为。③犯罪对象不同。前者的犯罪对象可以是所有类型的计算机信息系统，而后者仅限于国家事务、国防建设、尖端科学技术领域的计算机信息系统。④对危害结果的要求不同。前者是结果犯，行为人的行为造成计算机信息系统不能正常运行，并有严重后果，而后者是行为犯，只要行为人实现了侵入行为，就构成犯罪既遂，不要求有另外的危害结果。⑤被害法益不同。前者是计算机信息系统安全保护管理秩序、计算机信息系统所有人的合法权利和被害人正常的工作、生产经营秩序，而后者是国家对计算机信息系统安全管理秩序、国家的保密制度和国家

事务、国防建设、尖端科学技术领域的正常活动。⑥犯罪构成类型不同。前者有基本罪和重罪两个构成类型，基本罪的法定最高刑为 5 年有期徒刑，重罪的法定最高刑为 15 年有期徒刑，后者是单一构成类型，法定最高刑为 3 年有期徒刑。

(2) 本罪与破坏计算机信息系统功能罪和破坏计算机信息系统数据或应用程序罪的界限

本罪与破坏计算机信息系统功能罪和破坏计算机信息系统数据或应用程序罪的界限在于：①危害行为不同。本罪的危害行为只有故意制作、传播破坏性程序两种行为方式；破坏计算机信息系统功能罪的危害行为可以有删除、修改、增加和干扰四种行为方式；破坏计算机信息系统数据或应用程序罪的危害行为有删除、修改、增加操作三种行为方式。②犯罪前提不同。本罪故意制作、传播破坏性程序的行为属于违法行为，无需再次评价是否“违反国家规定”；后两罪必须以“违反国家规定”为犯罪前提。后两罪中的删除、修改、增加、干扰等行为，必须是未经合法授权的行为才能构成相应犯罪的危害行为，经过合法授权的删除、修改、增加、干扰行为不是以上两罪的危害行为，如行为人经有关部门授权破坏某计算机信息系统，即使造成严重危害后果，也不能构成犯罪。③犯罪对象不同。本罪的犯罪对象是他人的计算机信息系统，包括计算机信息系统功能、数据和应用程序，破坏计算机信息系统功能罪只能是他人的计算机信息系统功能，破坏计算机信息系统数据或应用程序罪的犯罪对象是他人的计算机信息系统数据或者应用程序。④罪名结构不同。本罪和破坏计算机信息系统数据或应用程序罪是选择性罪名，而破坏计算机信息系统功能罪是单一罪名。

3. 本罪的未完成犯罪形态问题

关于本罪是否有未完成形态，有学者认为，计算机病毒等破坏性程序种类，潜伏性和可激活性是其特点，如果行为人在他人计算机信息系统中施放了具有破坏能力，足以造成严重后果的破

坏性程序，在其潜伏期间被用户发现，并采取清除、杀灭措施，使预期的危害后果没有发生，这属于已经完成犯罪行为，只是由于行为人意志以外的原因而未能得逞，属于犯罪未遂。如果行为人将计算机病毒等破坏性程序植入他人计算机信息系统后，在危害结果尚未发生前，自动将破坏性程序原代码提供给警方，将其潜伏方式和清除方式向社会公开，或者自动清除该破坏性程序而有效防止危害结果的发生，属于中止犯。如果行为人为制作、传播这种破坏性程序而准备工具、制造条件，由于尚未着手实施犯罪，对直接客体未能构成现实的威胁，属于情节显著轻微、危害不大的行为，不能认定为犯罪，故本罪不存在预备犯①。

4．一罪与数罪问题

行为人故意制作、传播破坏性程序，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，或者对计算机信息系统存储、处理、传输的数据和应用程序进行删除、修改、增加操作，后果严重的，应该如何处理？

有学者认为，行为人在“没有制作、传播”病毒等破坏性程序的前提下，如果只是“利用”它们对系统功能、数据或者应用程序进行破坏，可视为破坏计算机信息系统功能罪或者破坏计算机信息系统数据或应用程序罪的一种犯罪方法，后果严重的，应当分别认定为这两种犯罪②。有学者反对这种观点，认为：其一，既然《刑法》第 286 条第 3 款已将制作、传播计算机病毒等破坏性程序，影响计算机信息系统的正常运行，后果严重的行为，规定为独立的罪名，那么，在破坏计算机信息系统功能罪和破坏计算机信息系统数据或应用程序罪的行为方式中，自然也就

① 赵廷光、朱华池、皮勇：《计算机犯罪的定罪量刑》，人民法院出版社 2000 年版，第 219 页。

② 胡国平：《关于四种计算机犯罪的认定》，《法律科学》，1997 年第 4 期。

不在包括利用计算机病毒等破坏性程序这种行为方式。其二，“利用”病毒等破坏性程序，实施破坏计算机信息系统功能罪或破坏计算机信息系统数据或应用程序罪，本身就是“制作、传播”病毒等破坏性程序的行为，根本不存在只是“利用”而没有“制作、传播”病毒等破坏性程序的情形。其三，制作、传播计算机病毒等破坏性程序，致使计算机信息系统功能、数据或者应用程序遭受“破坏”，仅此就足以评价为“后果严重”，不需要其他“严重后果”。试想，如果排除了致使计算机信息系统功能、数据或者应用程序遭受“破坏”，制作、传播计算机病毒等破坏性程序罪所要求的“严重后果”和“后果特别严重”又从何谈起呢？至于造成其他严重后果，如破坏生产经营、危害公共安全，则超出了《刑法》第 286 条规定的范围。作者同意后者观点，认为以上两种情况属于刑法理论中的法规竞合，即施放计算机病毒等破坏性程序罪与破坏计算机信息系统功能罪的法规竞合；施放计算机病毒等破坏性程序罪与破坏计算机信息系统数据或应用程序罪的法规竞合。由于刑法把施放破坏性程序罪与其他两款并列规定出来，可见，前面两款规定的危害行为的方法中，不应再包括利用计算机病毒等破坏性程序进行破坏，因此，对于实施以上行为的，按施放破坏性程序罪定罪量刑。

根据《刑法》第 286 条第 3 款和第 1 款规定，犯本罪基本罪的，处 5 年以下有期徒刑或者拘役；犯重罪的，处 5 年以上有期徒刑。对基本罪和重罪适用刑罚时，还应考虑犯罪的其他情节，在法定刑范围内予以从轻或者从重，主要有以下方面：(1) 行为人故意制作并传播计算机病毒等破坏性程序，破坏计算机信息系统，影响计算机信息系统正常运行，后果严重的，表明在主观恶性方面，比只有单纯的制作或者传播的行为人更大，应该予以从重处罚。(2) 行为人制作、传播实际传染能力和破坏能力很强的计算机病毒等破坏性程序的，应该予以从重处罚，这是因为利用计算机病毒等破坏性程序破坏计算机信息系统的犯罪，影响的范

围可能极广，破坏性程序在潜伏期内不易被发觉，其危害后果实际情况不是一下子体现出来，而是逐渐得到反映，因此查证的危害后果要远远小于实际的危害后果。不对这类犯罪从重处罚，不能使犯罪人的刑与责相对等，正确追究其刑事责任。(3) 根据行为人的危害行为所破坏的计算机信息系统功能、数据或者应用程序的重要性程度，以及危害后果的严重程度，社会影响恶劣程度，确定是否从重或者从轻处罚。(4) 根据行为人的目的动机反映出来的主观恶性程度，确定是否从重或者从轻处罚。

第六节　完善《刑法》第 286 条的立法建议

《刑法》第 286 条规定了破坏计算机信息系统的若干种行为，并给这些犯罪行为配置了统一的法定刑，该法条在以下几个方面需要完善：

1. 根据我国刑法理论，某一行为是否构成犯罪以及构成何种犯罪，其惟一根据是该行为是否符合某一具体犯罪的犯罪构成。犯罪构成是一个完整、复杂的系统，不同的犯罪要么犯罪构成要件数量不同，要么犯罪构成要件数量相同而构成要件的种类不同，或者犯罪构成要件的数量、种类相同，但是构成要件的形式和具体内容不同，任何两个犯罪不存在完全相同的犯罪构成要件，否则就是一个犯罪。根据形式逻辑的逆否定理，只有刑法条文关于若干犯罪行为规定了相同的犯罪构成，它们才是一个犯罪。《刑法》第 286 条三个条款规定的三种犯罪行为，在危害行为、犯罪对象、犯罪后果等构成要件上各不相同，因此，它们不是一种犯罪，而是三种犯罪。另外，犯罪构成还是确定罪名的惟一根据，对于不同的犯罪应当规定不同的罪名，否则就不能起到区别不同犯罪的作用。最高人民法院《关于执行〈中华人民共和国刑法〉确定罪名的规定》将《刑法》第 286 条三种犯罪行为作为一种犯罪，规定为一个罪名，即破坏计算机信息系统罪是不正

确的，应当予以纠正。

2.《刑法》第 286 条第 2 款规定，“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”，构成犯罪。该款规定存在两个问题：

（1）该款规定的行为仅限于“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”。这里的操作行为，是指利用计算机信息系统命令，或者运行应用程序，以实现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的删除、修改或者增加。而利用非操作手段，如使用电磁干扰、强磁破坏等方法就不构成该款规定的犯罪行为。如使用电磁炸弹攻击计算机信息系统，能够一瞬间将计算机存储器中的所有数据和应用程序全部破坏。而该条款把犯罪方法仅限于操作计算机信息系统一类，排除同样利用计算机信息系统特性，达到相同的危害后果的其他非操作类的犯罪方法，这不能反映立法本意，而是放纵了利用后者方法实施破坏计算机数据和应用程序的行为，致使其逃脱法律的制裁。因此，应该对本款规定的犯罪方法进行修改，可以表述为“……进行删除、修改、增加，后果严重的……”应取消对犯罪方法的限制。

（2）本罪的犯罪对象是“计算机信息系统中存储、处理或者传输的数据和应用程序”。何为数据和应用程序，法律没有给出定义。从计算机科学角度理解，计算机信息系统中存储、处理或传输的数据是指所有数字化的符号，既包括作为处理原始材料和处理结果的信息资源，也包括各种应用程序和系统程序，而本款规定中所称的数据明显不包含应用程序，因此，法律应当给本款所使用的“数据”和“应用程序”两个功能予以明确的定义。建议在《刑法》第 286 条增加对数据和应用程序的定义条款，即“本法所称应用程序，是指具有某项应用功能的计算机程序。本法所称数据，是指除计算机程序外的可以由计算机处理的数字化

信息”。此外，本款规定的犯罪对象是“数据和应用程序”，行为人如果只破坏其中一项，都不符合该款对犯罪对象的要求，不能构成犯罪，从而导致对犯罪行为的放纵。建议修改本款规定，将“……数据和应用程序……”改为“……数据或者应用程序……”

3. 分析《刑法》第 286 条三个条款的规定，前二者是从行为对象角度进行规定，后者是以行为方式确定犯罪构成，而且三款的法定刑完全相同，这样，三款规定的犯罪构成和法定刑配置发生交叉。例如行为人制作、传播计算机破坏性程序，对计算机信息系统功能进行删除、修改、增加、干扰，以及对计算机信息系统中的数据或者应用程序进行删除、修改、增加操作的，可能同时符合三款的规定，依照任何一款都可以处相同的法定刑。这种状况与同一法条下不同条款适用不同情形的立法原则相悖，需要对该法条进行修改完善。

作者认为，《刑法》第 286 条对三款规定的三种犯罪行为规定了相同的法定刑，对于前两款规定的犯罪行为规定相同的法定刑是合适的，但是，给故意制作、传播计算机破坏性程序的行为也配置相同的法定刑，则没有正确反映这种犯罪行为的社会危害性，与将这种犯罪行为单列出来区别对待的立法本意不符。一般而言，利用计算机病毒等破坏性程序破坏计算机信息系统的，其危害对象不是特定的某一台或者几台，而是一定网络范围内的大量计算机信息系统，历次计算机病毒事件，如“蠕虫”病毒事件、“CIH”病毒事件、“梅利莎”病毒事件和“爱虫”病毒事件都波及行为人自己都无法预计的、数量极其巨大的计算机信息系统，造成的损失非常严重。在刑事诉讼中，要确切地计算这种犯罪行为所造成的严重后果是十分困难的，不仅因为受害的计算机信息系统范围极为广泛，而且因为计算机病毒具有潜伏的特点，可能案发时其危害作用尚未表现出来，但是肯定要发作并造成危害。因此，对故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行的，应该规定比前面两种行为更重的法定刑，

否则不能与这类犯罪更严重的社会危害性相适应，有悖刑责相适应原则。

此外，《刑法》第 286 条第 3 款规定的危害行为是故意制作、传播计算机病毒等破坏性程序的行为，有学者认为本罪的行为方式有三种，即制作、传播和制作并传播。作者认为，仅有制作计算机病毒等破坏性程序而没有传播的行为，这些破坏性程序是不可能对计算机信息系统造成危害的，换言之，能够给计算机信息系统造成危害必须有施放计算机病毒等破坏性程序的行为。因此，本罪的行为方式实际只有两种，即传播和制作并传播。

最后，本条第 3 款所称的“计算机病毒”，没有明确的法律定义。从计算机科学的角度理解，计算机病毒具有的基本特征是自我复制性或者称自动传染性，是否具有破坏性不是计算机病毒的基本特征，许多病毒如“圣诞树”病毒等，只给计算机用户开个玩笑，并不进行破坏，因此，有必要从刑法角度给“计算机病毒”下定义。建议本条增加如下内容：“本法所称计算机病毒，是指具有自动传染性和破坏性的计算机程序”。

综合以上三点，建议修改《刑法》第 286 条为：

违反国家规定，实施以下行为，造成计算机信息系统不能正常运行，后果严重的，处 5 年以下有期徒刑或者拘役；后果特别严重的，处 5 年以上有期徒刑：

（一）对计算机信息系统功能进行删除、修改、增加、干扰的；

（二）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；

故意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，处 3 年以上 7 年以下有期徒刑；后果特别严重的，处 7 年以上有期徒刑或者无期徒刑。故意制作并传播计算机病毒等破坏性程序的，从重处罚。

本法所称应用程序，是指具有某项应用功能的计算机程序。

本法所称数据，是指除计算机程序外的可以由计算机处理的数字化信息。

本法所称计算机病毒，是指具有自动传染性和破坏性的计算机程序。

第八章　电子商务安全对策建议

第一节　电子商务安全对策建议概述

电子商务是21世纪的新经济模式，是现代企业发展的趋势。在信息时代，企业如果不采用电子商务模式，在激烈的竞争中将难以与具备市场和经营优势的电子商务企业抗争，最终将被淘汰。在国际经济一体化的进程中，不积极发展电子商务的国家将逐渐失去综合国力的比较优势，最终危及国家的安全和发展。因此，大力发展电子商务应该是我国一项战略决策。电子商务安全是影响电子商务发展的重要因素，研究电子商务安全对策，对维护和促进我国电子商务发展具有重要意义。

关于电子商务安全对策，目前主要有两种倾向：一种观点认为，电子商务安全是一个技术问题，电子商务企业只要装备足够的安全设备设施，如反病毒软件、防火墙系统、数字加密系统、数字签名技术等，就能对抗电子商务领域犯罪，维护电子商务安全。这种观点为相当多的电子商务企业经营人员所认可。另一种观点认为，电子商务领域犯罪危及电子商务安全，法律是维护电子商务安全的有力保障，由于我国目前电子商务领域刑事立法尚不完善，致使法律不能有效打击电子商务领域犯罪，因此，要维护电子商务安全，国家应该迅速健全电子商务相关法律。

作者认为，以上两种观点各持一端，既有正确的一面，同时又失之偏颇。第一种观点看到了计算机安全技术对遏制电子商务

领域犯罪的积极作用，但过分夸大了这种作用：首先，电子商务安全技术和电子商务领域犯罪技术是一对发展的矛盾关系，两者谁都不能总是保持胜利者的位置，而是彼此消长，一段时间犯罪技术突破安全技术，一段时间安全技术能够有效遏制犯罪技术。而且，在整个矛盾关系中，犯罪技术始终处于积极进攻的有利位置，它们总是不断地寻找现有安全技术存在的漏洞，而电子商务安全技术不能确保电子商务安全不受犯罪的侵犯。其次，频繁地更换安全技术不仅使电子商务企业投入巨大，而且使电子商务过程繁琐复杂，降低了电子商务经营活动的效率。再次，反病毒软件、防火墙系统、数字加密系统、数字签名技术等安全技术在对抗单位外部人员实施的电子商务领域犯罪行为确实有效，然而对于单位内部人员利用企业技术秘密实施的犯罪却无能为力。第二种观点主张，利用法律手段威慑惩治电子商务领域犯罪行为人，强调运用国家、社会的力量维护电子商务安全。作者认为，刑罚作为犯罪实施后的惩罚措施，只能在一定程度上遏制犯罪，不足以彻底消除犯罪对社会的危害。因此，即使是完备的电子商务领域的刑事法律，也不能杜绝电子商务领域犯罪的发生和对电子商务安全的危害。电子商务领域犯罪是信息时代的一类特殊的犯罪，犯罪方法手段的高技术性是其重要特点，没有相应的安全技术防护和对抗，将难以发觉网络空间一闪而过的犯罪，更难以获取犯罪证据、发现犯罪人和追究其刑事责任。

作者认为，电子商务是全球范围内的世纪宏伟工程，要有效防治电子商务领域犯罪，保障电子商务安全，在制定对策时必须充分考虑电子商务领域犯罪的特点、我国电子商务发展现状和电子商务领域立法状况，从多个方面同时入手，多管齐下，相互协调配合，构建电子商务领域犯罪的综合控制体系，最大限度地保障电子商务安全。电子商务安全对策主要有以下四个方面：

1. 在技术方面，要完善电子商务安全技术防护，发展电子商务领域犯罪跟踪技术。

技术措施是与电子商务领域犯罪直接斗争的有力武器，没有先进的反犯罪技术，就没有与电子商务领域犯罪斗争的物质基础。电子商务安全技术措施，是计算机信息系统安全的坚固盾牌，只有根据电子商务领域犯罪发展的状况，不断更新改进安全措施，才能遏制电子商务领域犯罪的完成，减少犯罪造成的损失。电子商务领域犯罪大多发生在互联网络空间，犯罪行为过程往往表现为转瞬即逝的电脉冲波，只留下很少的电子数据记录，为有效追踪犯罪行为，获取有效的犯罪证据，必须发展电子商务领域犯罪追踪技术，否则，即使发现犯罪行为，也难以发现犯罪人，甚至发现犯罪人后也会因为缺乏有效的证据而无法提起有效的诉讼。

同时，电子商务安全技术措施的开发，必须配合其他几方面对策，才能收到事半功倍的效果。例如目前的防火墙技术一般是单纯地将非法侵入行为拒之门外，而不能记录不成功的非法侵入的历史，如攻击计算机信息系统的时间、次数、发起攻击的计算机的 IP 地址或者拨号上网的电话号码等。这些历史记录却是处罚违法犯罪行为的关键依据，直接影响对行为人行政处罚的轻重或者定罪量刑。因此，开发防火墙等安全技术时不仅要考虑计算机信息系统安全的要求，而且应与法律、管理及思想法制教育等对策相配合，为其他对策的实施提供物质技术支持。

2. 在管理方面，要建立健全有关电子商务活动的各项管理制度。

建立、健全各项电子商务管理秩序，不仅能够规范电子商务活动秩序，而且能够有效预防电子商务领域犯罪的发生，在犯罪发生后，还能起到协助刑事侦查的作用。如建立健全电子商务领域违法行为的行政处罚制度、电子商务交易管理制度、电子商务交易企业的电子身份证管理制度、自然人网域身份证管理制度、电子商务交易资信管理制度等。这些制度的实施将使互联网络不再是看不见的“黑洞空间”，网上实施的违法行为能够被记录下

来，从而使违法行为人不再逍遥法外，合法用户获得更高的信誉和保护。

3．在法律方面，要迅速完善我国电子商务领域刑事立法，包括相关的程序法和实体法，而且还要积极完善司法手段和措施，积累打击电子商务领域犯罪的经验。

20 世纪 90 年代以来，我国制定了一系列的关于计算机和网络的法律法规。1997 年修订刑法，增加了危害计算机信息系统犯罪的规定，但是，由于电子商务起步晚，发展速度快，现有的法律体系已经滞后于电子商务的发展，不能适应打击电子商务领域犯罪的需要，必须进行修改完善。在修改完善电子商务刑事立法时，不仅要修改已有的法律条文，还要增加新的法律法规，不仅要修改实体法，还要修改程序法。为避免对《刑法》、《刑事诉讼法》的频繁修改，建议制定电子商务安全法，立法模式可以采取先综合后单行的方式，即由全国人大制定电子商务安全法，对立法目的、原则、电子商务安全法的法律地位及主要的法律问题作统一的规定，然后根据实际情况制定单行条例，待条件成熟后对电子商务安全法进行修改。

此外，还必须积极完善司法手段和措施，积累司法经验，增加司法打击的有效性。

4．加强计算机信息网络环境秩序的思想与法制教育。

我国互联网络用户人数众多，而且发展非常迅速，仅靠技术防护、行政管理和法律手段难以应对数量巨大的违法犯罪行为。因此，应该加强计算机信息网络秩序的思想与法制教育，促使广大网络用户自我约束，自觉遵守信息网络秩序，把电子商务领域违法犯罪行为消灭在思想萌芽阶段。同时，这也有利于集中力量，有效打击严重犯罪行为。

本章主要就社会规范管理对策和法律对策进行深入研究。

第二节 加强对电子商务领域违法活动的社会规范管理

电子商务领域违法活动的社会规范管理，是指国家机关依照行政法律法规、规章制度，对电子商务领域发生的尚不构成犯罪的违法行为采取的行政管理措施。这种规范管理不同于前面所述的计算机安全管理，计算机安全管理是计算机信息系统所有人单位为维护计算机系统安全，而制定的在单位范围内执行的、约束单位内部工作人员的安全管理制度。电子商务领域违法活动的社会规范管理也不同于刑法处罚，其规范管理的对象是不构成犯罪的违法行为，这些行为虽然不如电子商务领域犯罪行为危害严重，但是这类行为数量很大，而且很容易转化为犯罪行为。国家机关加强对电子商务领域违法行为的社会规范管理，能够有效遏制电子商务领域犯罪的发生，对维护电子商务安全具有重要意义。

一、完善电子商务领域违法行为的行政处罚制度

（一）我国处理电子商务领域违法行为的行政处罚制度状况

从20世纪90年代初开始，我国就制定了一系列的保护计算机、网络安全的行政法律法规、规章制度，主要有：《军队通用计算机系统使用安全要求》、《计算机信息系统安全保护条例》、《计算机信息网络国际联网管理暂行规定》、《计算机信息网络国际联网管理暂行规定实施办法》、《计算机信息网络国际联网安全保护管理办法》、《计算机信息系统保密管理暂行规定》、《金融机构计算机信息系统安全保护工作暂行规定》、《国际互联网出入信道管理办法》、《计算机信息系统国际联网保密管理规定》、《互联网电子公告服务管理规定》等，这些法规、规章形成了维护信息网络安全，打击利用计算机、网络技术实施违法犯罪的行政法律

控制体系。

以上法律法规明确规定了以下违法行为，并制定了相应的行政处罚规定：(1) 利用国际联网危害国家安全、泄露国家秘密；(2) 利用国际联网侵犯国家的、社会的、集体利益和公民合法权益；(3) 利用国际联网制作、复制、查阅、传播 9 类有害信息；(4) 未经允许，进入计算机信息网络或者使用计算机信息网络资源；(5) 未经允许，对信息网络功能进行删除、修改或者增加的；(6) 未经允许，对数据和应用程序进行删除、修改或者增加的，故意制作、传播计算机病毒等破坏性程序的；(7) 其他危害计算机信息网络安全的；(8) 利用国际联网侵犯用户的通信自由和通信秘密的；(9) 运输、携带、邮寄计算机信息媒体进出境，不如实向海关申报的；(10) 未经许可出售计算机信息系统安全专用产品的。《计算机信息系统国际联网保密管理规定》还专门制定了 7 条禁止性或者限制性的规定，防止利用互联网络泄露国家秘密。

计算机信息系统、信息网络营运管理单位和个人是我国互联网络体系的主体，也是维护计算机信息系统安全和信息网络安全，遏制电子商务领域违法犯罪的基础。《计算机信息系统安全保护条例》和《计算机信息网络国际联网安全保护管理办法》等行政法规规定了在公安机关监督、检查和指导下的安全保护制度和安全管理制度。在信息网络安全保护方面，对上述单位下列行为予以行政处罚：(1) 违反计算机信息系统功能安全等级保护制度的；(2) 接到公安机关要求改进安全状况的通知后，限期内拒不改进的；(3) 其他危害计算机信息系统安全的；(4) 计算机机房不符合国家标准或者国家其他有关规定的，或者在计算机机房附近施工危害计算机信息系统安全的。

此外，还规定了从事国际联网业务的单位和个人的安全保护责任：(1) 从事国际联网业务的单位和个人应当接受公安机关的安全监督、检查和指导，如实向公安机关提供有关安全保护的信

息、资料及数据文件，协助公安机关查处通过国际联网的计算机信息网络的违法犯罪行为；(2) 国际出入口信道提供单位、互连单位的主管部门或者主管单位，应当依照法律和国家有关规定负责国际出入口信道、所属互联网络的安全保护管理工作；(3) 互连单位、接入单位及使用计算机信息网络国际联网的法人和其他组织应当负责本网络的安全保护管理工作，建立健全安全保护管理制度，落实安全保护技术措施，负责对本网络用户的安全教育和培训，保障本网络的运行安全和信息安全。

《计算机信息网络国际联网安全保护管理办法》规定了计算机信息系统和计算机信息网络营运管理单位和个人的安全管理制度和协助制度：

1. 对委托发布信息的单位和个人进行登记，并对所提供的信息内容按照《计算机信息网络国际联网安全保护管理办法》第5条进行审核。

2. 建立计算机信息网络电子公告系统的用户登记和信息管理制度。

3. 发现有《计算机信息网络国际联网安全保护管理办法》第4条、第5条、第6条、第7条所列情形之一的，应当保留有关原始记录，并在24小时内向当地公安机关报告。

4. 按照国家有关规定，删除本网络中含有本办法第5条内容的地址、目录或者关闭服务器。

5. 用户在接入单位办理入网手续时，应当填写用户备案表。

6. 互连单位、接入单位、使用计算机信息网络国际联网的法人或者其他组织在一定时间内的备案工作。

7. 涉及国家事务、经济建设、国防建设、尖端科学技术等重要领域的单位办理备案手续时，应当出具其行政主管部门的审批证明。

8. 使用公用账户的注册者应当加强对公用账户的管理，建立账号使用登记制度，用户账号不得转借、转让。

9.《互联网电子公告服务管理规定》第14条规定，“电子公告服务提供者应当记录在电子公告服务系统中发布的信息内容及其发布时间、互联网地址或者域名。记录备份应当保存60日，并在国家有关机关依法查询时，予以提供”。第15条规定，“互联网接入服务提供者应当记录上网用户的上网时间、用户账号、互联网地址或者域名、主叫电话号码等信息，记录备份应当保存60日，并在国家有关机关依法查询时，予以提供”。

（二）行政处罚制度的弊端与完善建议

由于计算机、网络技术及应用和电子商务发展非常迅速，现行的有关计算机信息系统和信息网络安全的行政法律法规已经滞后，不能适应打击电子商务领域违法犯罪的需要。主要表现在以下方面：

1.《计算机信息网络国际联网安全保护管理办法》第8条规定，“从事国际联网业务的单位和个人应当接收公安机关的安全监督、检查和指导，如实向公安机关提供有关安全保护的信息、资料及数据文件，协助公安机关查处通过国际联网的计算机信息网络的违法犯罪行为”，这规定了信息网络经营单位协助公安机关的制度。该办法第10条规定了“互连单位、接入单位及使用计算机信息网络国际联网的法人和其他组织……发现有本办法第4条、第5条、第6条、第7条所列情形之一的，应当保留有关原始记录，并在24小时内向当地公安机关报告”的制度，这对有效追诉违法犯罪行为具有积极作用。但是，该制度并不彻底，只要求信息网络经营单位记录已经发现的符合该管理办法第4条、第5条、第6条、第7条的信息，没有扩充到其他违法犯罪行为，客观上轻纵了其他违法犯罪行为。

2.《计算机信息网络国际联网安全保护管理办法》第10条规定，从事国际联网业务的单位和个人“对委托发布信息的单位和个人进行登记，并对所提供的信息内容按照本办法第5条进行审核；建立计算机信息网络电子公告系统的用户登记和信息管理

制度”。这种信息发布登记和信息内容审核制度实际上难以实行。首先，目前商业网站为了吸引网络用户访问使用，大多提供了免费信息发布服务，以任何方式上网的用户都可以自由地发布信息，商业网站很少要求网络用户提供身份信息，即使要求提供身份信息，网络用户往往不愿提供真实的身份信息，而使用一些虚构的信息就可以容易地通过信息登记。其次，发布信息内容审核实际也难以落实，由于网上发布信息的用户很多，发布的信息量庞大，商业网站等信息网络经营单位要在浩如烟海的信息海洋中审核每一条信息是非常困难的。例如著名的“找到啦”网站刊载他人裸体照片被诉案。在这一案件中，“找到啦”网站将被害人杨某的5张艺术照与一不知名的女性裸体照连续编排在同一网页上，而“找到啦”网站无奈地宣称事先并不知情，自己的技术力量不可能对所有的信息进行审查①。

3.《计算机信息网络国际联网安全保护管理办法》制定了用户账号使用管理制度。该办法第11条规定，“用户在接入单位办理入网手续时，应当填写用户备案表”。第12条规定互连单位、接入单位、使用计算机信息网络国际联网的法人或者其他组织必须在一定时间内进行备案工作。第13条规定“使用公用账号的注册者应当加强对公用账号的管理，建立账号使用登记制度。用户账号不得转借、转让”。但是，由于电信市场的迅速发展，这种用户账号管理制度实际上名存实亡，根本起不到约束违法犯罪行为人的作用。导致用户账号管理制度失效的原因很多，例如目前许多信息网络经营单位提供上网卡业务，人们只要在市面上购买了上网卡，无需任何登记备案，就可以使用信息网络。市面上大量衍生的网吧也是有效规避该制度的方法，行为人在网吧按时间付费上网，根本不会有任何人查问身份和在网上的行为，或者

① 曹英、汲传排：《“裸照”上网小姐索赔十六万》，《北京日报》，2000年7月13日。

网吧只要求顾客做形式的登记，对确定上网人的身份不起任何作用。

我国电信企业曾作出规定，用户在网上进行违法行为的，电信公司将暂停甚至终止拨号用户的上网账号。作者认为，该条如果没有列入网络接入服务合同，那么发生用户在网上进行违法活动时，电信企业无权限制或者停止用户账号的使用。但是，限制用户账号是处罚一部分用户网上违法行为的有效办法，要使这一举措合法化，可以通过两种途径：(1) 公安机关会同工商行政管理机关，要求在电信企业的网络接入服务标准合同中加入上述条款，使电信企业的限制上网账号的行为合法化，公安机关监督电信企业落实账号的管理；(2) 修改行政处罚法规，明确限制使用上网账号制度，即公安机关依法要求电信企业暂停或者停止用户上网账号的使用。

4. 以上行政法律法规、规章制度和我国其他法律，如《保密法》、《计算机软件保护条例》、《治安管理处罚条例》等规定了若干违法行为，但是以上法律法规并没有涵盖发生在互联网络空间的全部违法行为，如网络广告骚扰、商业网站侵犯网络用户个人数据、网上非法行医等。此外，对于有些规定为违法的行为，没有规定行政处罚措施，如《计算机信息网络国际联网安全保护管理办法》第 7 条规定，“用户的通信自由和通信秘密受法律保护。任何单位和个人不得违反法律规定，利用国际联网侵犯用户的通信自由和通信秘密”，但是对于利用国际联网侵犯用户的通信自由和通信秘密的违法行为，却没有制定行政处罚措施。

总之，我国电子商务领域违法行为的行政规范管理制度，需要跟随计算机、网络技术和电子商务的发展进行改进和完善。

二、完善信息网络经营单位和个人的协助制度

《计算机信息网络国际联网安全保护管理办法》规定了我国从事国际联网业务的单位和个人协助公安机关的制度，为了更好

地发挥协助制度遏制犯罪的积极作用，作者认为应当从以下两个方面进行完善：

（一）完善信息网络使用原始记录保留制度

行为人在互联网络空间进行违法犯罪活动，必然在使用过的计算机信息系统上留下操作、使用的电子记录，这些电子记录常常是追诉违法犯罪的惟一证据，但这些电子记录的保存要消耗计算机信息系统的大量资源，往往被网络管理者清除。为了有效追究违法犯罪，网络服务提供者的利益必须为社会利益作一定的妥协，国家应当建立信息网络使用原始记录强制保留制度。

《计算机信息网络国际联网安全保护管理办法》第 10 条规定，从事国际联网业务的单位和个人应当对该办法第 4 条、第 5 条、第 6 条、第 7 条规定的违法行为的原始记录进行保留，但对其他种类的违法行为则不作要求。《互联网电子公告服务管理规定》要求电子公告服务、互联网接入服务经营者保留用户上网的有关信息，对于其他种类的网络信息服务则不作要求。这无疑为利用其他网络信息服务实施违法犯罪留下了空档。另外，《互联网电子公告服务管理规定》只是一个部门规章，法律效力较弱，不利于相关规定的落实。《电信条例》第 62 条规定，“在公共信息服务中，电信业务经营者发现电信网络中传输的信息明显属于本条例第 57 条规定所列内容的，应当立即停止传输，保存有关记录，并向国家有关机关报告”。该条要求电信业务经营者对网上的非法信息及其相关记录予以保留，但不涉及其他违法行为的记录，而且该条例对不履行该条义务没有规定罚则。总之，我国信息网络使用原始记录强制保留制度需要进一步完善。

在这个问题上，欧盟国家和美国在互联网服务提供商协助制度上的经验值得借鉴。2000 年 7 月底欧盟各成员国讨论通过的“RIP”法案，要求各互联网服务提供商共同参加监督互联网使用者的行动，通过在互联网服务提供商的网络系统中安装并运行

“黑盒”来实现相关监督活动①。美国联邦立法允许执法人员在寻求法院批准获取涉及记录的同时，可命令互联网服务提供商立即保留相关电子证据，保留期为 90 天，且执法部门每要求一次，该证据的保留期就要多保留 90 天。

借鉴国外相关立法经验，作者建议制定《互联网络服务管理办法》，要求网络接入服务提供者和各种网络信息服务提供者履行网络使用原始记录保留制度，并规定相关罚则，即网络接入服务提供者应当记录上网用户的上网时间、用户账号、互联网地址或者域名、主叫电话号码等信息，各种网络信息服务提供者应当记录在系统中发布的信息内容及其发布的时间、互联网地址或者域名，以上记录备份应当保存 60 日，并在国家有关机关依法查询时，予以提供。

（二）有害信息的限制清除制度

《计算机信息网络国际联网安全保护管理办法》第 10 条规定，互连单位、接入单位及使用计算机信息网络国际联网的法人和其他组织，应当按照国家有关规定，删除本网络中含有该管理办法第 5 条内容的地址、目录或者关闭服务器。该条规定了对信息网络内的有害信息的清除制度。但是，许多有害信息不是都存储在以上单位的信息网络内部，国外的淫秽色情网站和反动宣传网站通过各种渠道直接向国内网络用户发送有害信息，因此，仅仅消除信息网络内部的有害信息，达不到遏制有害信息造成的危害。建议修改《计算机信息网络国际联网安全保护管理办法》，建立有害信息限制清除制度，要求互连单位、接入单位及使用计算机信息网络国际联网的单位安装有害信息识别、限制、清除软件系统，并且及时更新，杜绝有害信息传入我国，消除有害信息对我国网络用户的危害。

---

① 《欧盟采取行动对付电脑犯罪》，《计算机世界日报》，2000 年 8 月 2 日。

三、建立自然人电子身份证管理制度和“回溯查因”制度

互联网络社会是人类社会的一个新的组成部分，由于用户在互联网络上使用的网络身份可以与真实身份不一致，难以确定网上违法行为人的真实身份，因而互联网络空间被认为是“绝对自由王国”。我国《计算机信息网络国际联网安全保护管理办法》规定了用户账号使用管理制度，但是，随着计算机网络应用和电子商务发展，这种管理制度已经名存实亡，管理用户账号的方法根本不能制约电子商务领域违法犯罪，必须建立自然人电子身份证管理制度，使用户在信息网络空间的身份可以与其真实身份惟一对应。

要建立自然人网上身份证制度，首先必须确定自然人的生理身份，而且这种生理身份必须具有惟一性特征，否则无法区别不同的自然人。实际上，自然人的这种惟一的生理身份是存在的。由于世界上不存在两个完全相同的人，即使是孪生人，其 DNA、视网膜虹膜、指纹和掌纹等都不完全相同，将这些个体特征信息按照一定规则进行数字化，可以制成与每个人的生理身份惟一对应的数字身份。行为人使用有这种数字身份的信息网络，就可以消除网上身份虚拟化、假冒他人网上身份等带来的消极影响，而使用假冒的数字身份，将无法通过生物特征检测，从而被拒绝在互联网络之外。一些发达国家为维护电子商务安全，已经开发并应用了各种生理身份认证技术。例如日本产业界和学术界最近开发出了一项新技术，由作为第三者的有关机构采集用户的皮肤细胞进行分析，然后根据基因序列和指纹来制作个人特定的数值信息①。当他人盗用密钥时，只要对照密钥中包含的人体信息和本人的基因序列和指纹，就能够立即发现问题。1999 年芬兰开始实行公民电子身份证，这种电子身份证中不仅存储了有关个人身

① 刘新宇：《人体信息作密码》，《参考消息》，2000 年 2 月 28 日。

份的各种信息，同时存储了持证人的签名手迹。公民除了获得一张身份证卡片，还获得一块可以安装在计算机中的识别卡，通过电子身份证和识别卡，持证人可以通过计算机办理电子事务①。

在我国应用生理身份的技术条件也日益成熟。公安部物证鉴定中心经过“八五”攻关，DNA 检验项目由原来单一的 DNA 指纹技术到更先进的 STR 复合扩增技术、线粒体 DNA 序列测定技术等多项检验，都处于国际先进水平。我国开展 DNA 检验的单位由原来的一两家发展到了几十家，许多省、自治区、直辖市计划在近期内将 DNA 实验室普及到地市一级，为建立全国 DNA 犯罪数据库打下了良好的基础②。一旦全国范围内的 DNA 库建立起来，就能为每位公民提供电子身份证，顺利建立公民电子身份证管理制度，可以从根本上解决网上使用虚假身份、假冒他人身份等进行的违法犯罪问题。

电子身份证管理制度与信息网络经营单位协助制度相配合，能够将上网者在网络上的一举一动全部记录下来，使信息网络上的违法犯罪人不再是来无影去无踪的“隐身人”，而是处在法网的有效控制之下。这种记录、追踪违法犯罪行为的制度，可以被称为“回溯查因”制度。毫无疑问，“回溯查因”制度能够给违法犯罪行为人构成极大的威慑力，迫使行为人自觉遵守法律法规、社会规范，从而有效遏制电子商务领域违法犯罪行为。但是，有人担心电子身份证制度和信息网络经营单位协助制度的实施，将使公民的隐私权处于危险的境地，在美国更是遭到人权主义者的强烈反对，有关监控公民网络行为的《通信法案》仅仅通过一天就被废除。

---

① 《芬兰推行公民电子身份证 一张 IC 卡记录重要信息》，《电脑日报》，1999 年 9 月 16 日。

② 仲昌：《打击犯罪的有利武器 中国紧张建设 DNA 数据库》，《电脑日报》，2000 年 6 月 3 日。

作者认为，自由从来不是绝对的，绝对的自由也就意味着自由的丧失。由于没有控制电子商务领域违法犯罪的有效措施，在互联网络上进行涉及个人财产和人身权利的事务将得不到安全保障，这种状况必将阻碍我国电子商务发展，因此，“回溯查因”制度有利于社会发展，也有利于广大网络用户的利益，应当尽快建立起来。但建立“回溯查因”制度的同时，也应该为网络用户隐私权提供有效保障，如果网络用户隐私权得不到保障，也将阻碍网络用户参与电子商务。所以，对网络用户个人数据的使用应规定严格的法定程序，并配合技术手段予以保障：各信息网络经营单位和个人必须使用公安机关规定的专用网络用户数据记录设备，该设备中记录的数据必须使用专门的技术才能进行提取和输出，否则设备中的数据将自毁，任何其他单位和个人擅自提取该设备中的数据都为违法；该专门技术仅供公安机关持有，任何其他单位和个人获取该技术都构成违法；公安机关提取这些设备中的数据时必须经法定程序才可进行。总之，这种在法律程序和技术措施控制下的“回溯查因”制度，能够有效遏制电子商务领域违法犯罪，同时，最大程度地维护网络用户的隐私权，从而保障电子商务安全发展。

电子身份证管理制度和“回溯查因”制度是电子商务正常发展的必然要求，随着各项技术条件的成熟和人们对电子商务安全认识的提高，以上两项制度在不远的将来将成为现实。

四、完善电子商务资信管理制度

由于电子商务交易中交易方无需会面，因此，交易的安全性、交易对方身份的真实性和资信的可信性为交易方特别关注。近年来，人们对电子商务安全提出多种要求，如信息保密性、交易者身份的确定性、不可否认性、不可修改性等，并制定出不同网络层次的安全标准和协议，有安全套接层协议（SSL：Secure Sockets Layer）、安全超文本传输协议（S-HTTP）、安全电子交

易协议（SET：Secure Electronic Transaction）① 等。在这些安全交易协议中，采纳了一些常用的安全电子交易的方法和手段，典型的有密码技术②（包括公私密钥加密和数字消息认证）、数字签名③、认证中心（CA：Certification Authority）、数字时间戳（digital time-stamp）、数字凭证（digital certification，digital ID）等。以上技术措施能在最大程度上维护电子商务安全，而应用以上技术建立有效的电子商务资信管理制度，才能使这些安全技术措施发挥功效。

（一）加强电子商务企业的电子身份证管理制度

电子商务企业电子身份证管理制度是电子商务资信管理制度

---

① SSL 是用来保证 Internet 上安全通信的协议，S-HTTP 是用于为应用程序进行鉴别和保证秘密的协议，SET 是对电子商务事务进行安全保证的协议，它们用于数据通信的不同层次上的安全防护。

② 采用密码技术对信息加密是最常用的安全交易手段，在电子商务中获得广泛应用。（1）公私密钥（public key and private key）加密方法亦称为 RSA 编码法，公私密钥实质上是一对很大的质数，用其中一个对文件加密，均可由另一个质数来解密，但要用一个质数来求出另一个质数则十分困难。在加密应用时，客户保留其中一个密钥（私钥），而将另一个密钥（公钥）公开，需发信的人员将信息用公钥加密后发给该客户，只有具有私钥的客户才能解密，这样保证在 Internet 上传输信息的保密和安全。（2）数字摘要（digital digest）加密方法亦称安全 Hash 编码法，该编码法采用单向 Hash 函数将需加密的明文“摘要”成一串 128bit 的密文，这一串密文亦称为数字指纹，它有固定的长度，且不同的明文摘要成密文，其结果总是不同的，而同样的明文其摘要必定一致。这样摘要就可用来验证原文是否被修改。

③ 数字签名（digital signature）是公私密钥和数字消息认证技术的结合应用，通过在文件中附带文件的 Hash 编码信息，接受方据此认定文件在传输过程中未被他人修改，从而可用来防止电子信息因易被修改而有人作伪证，或冒用别人名义发送信息，或发出（收到）信件后又加以否认等情况发生。

的重点，它通过电子商务认证机构来完成。电子商务认证机构是电子商务体系中的重要部门，其作用是解决电子商务交易方的身份、资信认定，维护交易活动的安全。没有电子商务认证，就无法消除交易方互不见面、互不了解而产生的担心和疑虑。

电子商务认证是电子商务的关键，世界各国纷纷加紧电子商务认证机构的建设，甚至各个行业、部门也陆续建立自己的认证机构。从各国电子商务建设的模式来看，基本上有两种类型，其一是政府主导或者授权建立的相对统一的电子商务认证体系，如加拿大和新加坡等国的电子商务认证体系；其二是民间自发建立的各自独立的电子商务认证机构。前者的优势在于电子商务认证机构的统一，通用性强，而在适应各行业部门特点方面尤显不足，后者则能够弥补前者的不足，并且各行业部门建立自己的电子商务认证机构已经是既成事实，但是在电子商务认证的通用性方面显得欠缺。我国电子商务认证机构建设发展迅速，1999 年中国人民银行支付科技司组织工行、农行、建行等 12 家商业银行联合共建中国金融认证中心（CFCA），2000 年 3 月 30 日中国金融认证中心 SET CA 系统试发了第一批证书，首都信息发展有限公司、新浪网站、8848 网站、鲨威体育用品公司和工商银行、广东发展银行成为第一批 SET 证书的持有者，CFCA 于 2000 年 6 月正式开始运行，第一阶段将发放 SET 和非 SET 证书共 25 万张，CFCA 所提供的网上支付身份认证，将为我国电子商务的开展提供更为有利的操作环境①。关于我国的电子商务认证模式，当时任中国信息产业部信息化推进司的宋玲司长在北京国际电子商务应用博览会上说，电子商务的安全认证是实现电子商务的关键，必须统筹规划认证体系的建设，由政府有关主管部门实行授

① 《网上支付"身份证"试发放》，http://www.cnw.com.cn/，2000 年 11 月 11 日。

权管理①。

作者认为，根据我国国情，我国的电子商务认证机构建设应该在政府部门的统一规划下，以国家电子商务认证中心为主干，建立树状认证机构系统，允许各行业部门建立各自的横向的职能认证中心，并使之成为认证系统中的分支，实行认证机构由上而下的授权确认管理，保证整个认证体系中认证的统一和通用。

目前，我国的电子商务认证机构的性质尚未确定，从目前发展状况来看，它应该属于国家统一管理下的独立服务企业。在法律关系上，电子商务认证机构是执行监督管理职能的服务单位，交易各方按约定接受认证机构的监督，同时，电子认证机构必须对进行电子商务交易各方负责，对整个电子商务的交易秩序负责，忠实地履行自己的认证职责。

如果发生电子商务认证机构未发出通知、通知有误、泄密或者虚假认证而导致交易方经济利益或者名誉遭受损害的，认证机构是否承担责任和怎样承担责任？新加坡等国家的电子商务立法对认证机构的责任进行限制，即规定经政府管理机构许可的安全认证机构可以在其签发的电子凭证中说明其承担责任的限额，有学者建议我国电子商务立法应参照新加坡的做法。有学者则认为，应当采取“有限责任为主、兼采完全责任的原则，即指中心因过失未发出通知、通知有误或因黑客袭击等意外事件导致泄密的，其赔偿额仅限于传递费、服务费加利息（即直接损失），对间接损失则不赔偿；因认证人故意或欺诈地泄密或更改、毁损用户交易资料的，或者认证人虚假认证的，则中心对用户的赔偿应为用户的全部损失”②。本书在第一章第二节中提到，电子商务

① 《中国电子商务安全认证实行政府授权管理，自行设立的 CA 认证必须得到政府认可》，《电脑日报》，1999 年 9 月 12 日。

② 徐继响、毛崴、马刚：《电子商务认证机构若干法律问题初探》，《河北法学》，2000 年第 6 期。

认证机构是电子商务民事主体体系中的一员，法律对认证机构的保护过多或者过少（限制认证机构责任就是保护方法的一种）都会损害某类民事主体的利益，最终不利于我国电子商务的发展，所以，作者认为，应当避免政府对电子商务认证行业发展的过多干预，电子商务认证机构的责任主要应由市场来调节，即政府立法规定电子商务认证机构应当承担的基本责任，同时规定认证机构可以与交易方约定承担其他责任，市场的竞争必然淘汰那些责任承担能力弱的认证机构，产生实力雄厚、服务质量优良的认证企业，最终促进电子商务安全迅速发展。电子商务立法规定电子商务认证机构承担的基本责任应当包括：(1) 认证机构过失导致交易方损失的，赔偿额为交易方的直接损失和当次交易的服务费；(2) 认证人故意或欺诈地泄密或更改、毁损用户交易资料的，或者认证人虚假认证的，应当赔偿用户的全部损失，构成犯罪的还应承担刑事责任。

（二）建立个人电子商务交易资信管理制度

在电子商务发展中，除了企业对企业和企业对个人的电子商务外，个人对个人的电子商务也大量存在。以网上拍卖为例，网络用户在拍卖区刊登拍卖品的信息和联系方式，其他网络用户在网上报价，一定时间内最高的价格为成交价，拍卖中用户往往被要求向拍卖者汇寄货款，接收者收到货款后才寄出货物。这种交易方式明显对卖方有利，对买方不利，行为人利用虚假身份拍卖不存在的商品，骗得他人货款后消失了，而后，他还可以使用其他身份继续诈骗，例如前面提到的我国雅宝竞拍网站上发生的网上拍卖诈骗案。因此，建立个人电子商务资信管理制度具有现实的重要意义。

由于没有解决自然人电子身份证管理制度，还无法建立较高安全度的个人电子商务资信管理制度。但是，目前有些商业网站已经着手试行一些个人电子商务资信制度：在进行网上销售、拍卖的个人，如果在商业网站的电子商务区销售时，必须登记个人

基本资料，如身份证号码、住址、联系方式等。商业网站经过基本检查后（如按联系电话与登记者联系，核查有关资料），认为个人资料可信的才准许在商业网站上出售商品。同时，随时跟踪登记者的交易记录，能够成功交易并且让交易对方满意的，达到一定次数后可以授予成功交易标志，如在其网络用户名后挂交易成功星标志，星标志越多表明其商业信用越高，其他交易人自然倾向与其进行电子商务交易；如果行为人有过欺诈行为，则在其用户名后挂欺诈标志，甚至删除其交易身份，不允许其参与网上交易。这种个人资信管理制度虽然不能完全清除网上诈骗行为，但在一定程度上引导网络用户进行合法的、有信用的电子商务交易，减少个人电子商务交易的盲目、混乱状况，对推进个人电子商务资信管理制度具有积极意义。

第三节　迅速完善电子商务领域的刑事实体法

电子商务是一项宏伟的社会工程，电子商务领域犯罪是信息时代特有的社会现象，在电子商务安全的诸项对策中，电子商务领域的刑事法律是预防惩治电子商务领域犯罪的有力武器和维护电子商务安全的重要屏障。但由于电子商务在我国发展十分迅速，新的法律问题层出不穷，形式复杂多变，现行法律没有及时跟上电子商务的发展，刑事法律的滞后削弱了其功效的正常发挥，因此，必须迅速完善电子商务领域刑事法律。由于前面已经讨论了一部分犯罪的立法完善建议，本节主要讨论完善电子商务领域刑事立法应当设立的新犯罪，有关电子商务领域刑事程序法的完善将在下一节中讨论。

随着电子商务的发展，许多新形式的犯罪陆续出现，其中有些犯罪可以在现行刑法体系的范围内处罚，如电子商务认证机构

虚假认证或者认证重大失实，造成严重后果的行为，这种新形式的犯罪行为仍然可以适用《刑法》第 229 条和第 231 条，按中介组织人员提供虚假认证文件罪或者出具证明文件重大失实罪定罪处罚；有些行为则难以用现行刑法处罚，需要对刑法予以修正，增加新犯罪的法条。由于本书难以穷尽全部新的犯罪行为，鉴于计算机数据类商品对国计民生的重要作用，以及侵犯计算机数据类商品犯罪的严重势态，我们拟着重讨论侵犯计算机数据类商品犯罪的立法问题。

所谓计算机数据类商品，是指计算机软件和数据库等计算机数据形式的商品。与计算机硬件、设备等有形商品不同，它们没有固定的形态，需要存储在磁盘、光盘等媒介上，或者在数据通信网络中传输，但是，它们与其他任何商品一样，凝结了人类的劳动，并具有一定的经济价值。近年来，随着计算机数据类产品在社会生产生活中的广泛应用，电子商务活动中计算机数据类商品交易量迅速增加。

计算机数据类商品的大量生产和广泛应用的同时，侵犯计算机数据类商品的犯罪也日益猖獗，严重影响了相关信息产业的发展。根据世界软件制造商组织 1999 年公布的数字，西欧盗版软件所占的比例平均为 36%，东欧国家为 76%①，计算机软件保护最有力的美国，2000 年的盗版率也达到了 27%，使相关产业一年损失大约 2 000 亿美元。

侵犯计算机数据类商品的犯罪表现为以下几种形式：(1) 未经权利人许可，复制发行他人的计算机数据类商品牟利的，即所谓盗版发行的行为。(2) 未经权利人许可，复制使用他人计算机数据类商品并使用的。(3) 未经权利人许可，破解他人计算机数据类商品的安全保护并使用的。(4) 明知是盗版的计算机数据类

① 《盗版软件到处都有，瑞典用户 38% 使用盗版软件》，《电脑日报》，1999 年 6 月 3 日。

商品而使用的，这些人是盗版产品的最终用户，数量庞大，而且通常是其他侵犯计算机数据类商品犯罪的广阔市场。

面对日益严峻的犯罪形势，世界各国和地区纷纷制定法律，打击各种侵犯计算机数据类商品的犯罪。目前大多数国家和地区都规定盗版发行计算机数据类商品的行为为违法，甚至将其规定为犯罪。但是，对于侵犯计算机数据类商品的犯罪，法律界则有不同的态度：2000 年意大利都灵的一位法官审理了一起软件盗版案，一位都灵企业家被控未经许可复制字处理、会计和设计软件，并在自己的企业中使用。这位法官裁定，只要用户拷贝软件的目的不是用来获利，而且，被拷贝的软件没有出售给第三者，那么，拷贝软件就不能视为一种犯罪行为。与此相反，我国香港特别行政区对侵犯计算机数据类商品的行为则严厉得多，如 2000 年 6 月我国香港特别行政区通过了新的版权条例，其中把知情下使用盗版软件列为刑事罪行。可见，香港对计算机数据类商品制造行业提供了强势法律保护，而意大利的属于弱势保护。对计算机数据类商品的立法保护，直接影响计算机数据类商品制造行业的发展，法律保护越有力，该行业的发展越兴旺，反之，则发展缓慢，甚至长期停滞不前。

我国从 1990 年开始先后颁布了《著作权法》、《计算机软件保护条例》等法律法规，1994 年把侵犯计算机软件著作权的行为规定为犯罪，并于 1997 年写入修改后的刑法，但对非营利性侵犯计算机数据类商品的行为不以犯罪论，显然我国对计算机数据类商品制造行业的立法属于弱势保护，因而，必须加紧完善计算机数据类商品保护的刑事立法。

1. 扩大计算机数据类商品法律保护的范围

根据《著作权法》、《计算机软件保护条例》和《刑法》相关规定，我国对计算机数据类商品的法律保护仅限于计算机软件的范围。根据《计算机软件保护条例》第 2 条和第 3 条的规定，计算机软件是指计算机程序及其有关文档。非计算机软件的其他计

算机数据类商品如数据库，不属于我国《著作权法》第3条规定的9类作品之列，不受我国著作权相关法律的保护。实际上，数据库等其他计算机数据类商品和计算机软件一样，是凝结人类劳动、具有经济价值的创造，应当享有著作权。在美国、英国等国家，数据库产品如某地区商品详细情况数据库等，是一种具有很高商业价值的计算机数据类商品，在这些国家受到法律的严格保护。在我国随着电子商务的发展，不仅计算机软件商品应用越来越广泛，数据库等其他计算机数据类商品也将在社会生产生活中发挥重要作用，这类商品缺乏法律保护将阻碍甚至扼杀该类商品制造产业的发展，最终不利于我国经济的正常发展，因此，应当扩大计算机数据类商品法律保护的范围，把数据库等其他计算机数据类商品纳入《著作权法》规定的作品行列。

2．增设破解他人计算机数据类商品使用保护措施牟利罪

一般来说，计算机数据类商品使用加密或者序列号等安全保护技术措施，防止他人侵犯其著作权等合法权利，这些安全技术措施在维护权利人合法权益方面具有显著功效，一般人很难突破这些安全保护技术措施。但也有一些行为人为牟取不法利益，专门进行计算机数据类商品安全保护措施的破解，他们利用各种技术手段破解保护技术，获取产品使用序列号，或者解除产品的保护措施，然后将获得的使用序列号或者解除保护后的产品卖给盗版组织。为了获取更多的非法利益，他们逐渐形成系统的破解技术，大肆破解他人计算机数据类商品的保护措施，使任何新的计算机数据类商品一上市，很快就有盗版产品出现，给计算机数据类商品生产厂家造成极为严重的经济损失。我国法律没有规定破解他人计算机数据类商品使用保护措施的犯罪，法律上的疏漏使这类行为近年来越来越猖獗，甚至发展成有组织的、经营性的破解技术单位，给我国信息产业造成严重冲击。

作者建议，在侵犯知识产权罪一节，增加破解计算机数据类商品使用保护措施牟利罪。对破解他人计算机数据类商品使用保

护措施，获取非法利益数量较大、多次破解或者造成严重后果的，以犯罪论处。具体罪状可以表述如下：以牟利为目的，未经权利人许可，破解他人计算机数据类商品并提供给他人，多次实施以上行为，或者违法所得数额较大的，或者有其他严重情节的，处3年以下有期徒刑或者拘役，可以并处或者单处罚金；违法所得数额巨大或者有其他特别严重情节的，处3年以上7年以下有期徒刑，并处罚金。

3. 增设非法获取、使用计算机数据类商品罪

在侵犯计算机数据类商品的行为中，有一种是行为人非法获取计算机数据类商品并使用的行为，如目前大量存在的计算机用户购买、使用盗版软件的行为。对于这种行为如何处理，有人认为，计算机数据类商品不同于物质性财物，物质财富具有惟一性和排他性，盗窃他人财物也就意味着被害人丧失了该财物，而计算机数据类商品则具有共享性，通过复制或者网络共享的方法，能够供多人同时使用。因此，非法复制他人的计算机数据类商品的，不论商品价值多少，获利多少，应以民事侵权行为处理，不能认定为盗窃行为。同时，根据《刑法》第217条规定，以营利为目的，未经著作权人许可，复制发行计算机软件的，才可能构成侵犯著作权罪。因此，非法复制他人的计算机数据类商品，如果没有以营利为目的复制发行，无论复制多少份，向多少人分发，都不可能构成犯罪，只能构成民事侵权行为。

作者认为，对于非法复制他人的计算机数据类商品，数额较大或者有其他严重情节的，应该以犯罪论处。理由如下：

(1) 在信息时代，计算机数据类商品制造业已经成为生产生活资料生产的重要部门，计算机数据类商品是信息社会的重要资源，是一种与物质财富同样重要的财富。

(2) 非法复制计算机数据类商品使生产企业损失严重。生产企业为开发一种产品，从研究开发到向市场推广，乃至后继的升级、维护等售后服务，都要花费大量资金，并且这类商品销售的

风险大，产品性能优越不一定会收到好的市场回报，如美国IBM公司研究开发的OS/2操作系统，投入了几十亿美元，而至今没有获得预期的回报。非法复制、使用将缩小计算机数据类商品的市场，使企业得不到合理的回报，无法回收投资成本而面临亏损的困境，以致严重打击我国计算机数据类商品制造业的发展，同时，也使合法用户遭遇不公平的待遇，使部分合法用户转向使用盗版的商品。

（3）将非法复制计算机数据类商品的行为按民事侵权行为处理，实质上无法有效地打击非法复制行为，保护所有者的合法权益。计算机数据类商品的重要特点是易于复制，计算机用户可以用普通的计算机设备，以极低廉的成本复制成千上万份，而计算机数据类商品生产企业要将千万名侵权人告上法庭，要求民事赔偿，从费用和时间上考虑都是不可能实现的；加之，我国计算机数据类商品制造业立足未稳，规模尚不够雄厚，多为中小企业，往往无力以法律手段追诉侵权人，只能眼巴巴地看着企业在不法复制者的侵蚀下昙花一现地消亡。

（4）应该利用刑法手段打击非法复制计算机数据类商品的行为。计算机数据类商品是国家的战略资源，我国计算机数据类商品制造业长期得不到法律的有效保护，导致发展缓慢。因此，为保障我国计算机数据类商品制造业正常发展，必须营造有利的法律环境，我国刑法应增设非法复制计算机数据类商品罪，对非法复制他人的计算机数据类商品，数额较大或者有其他严重情节的，依法定罪处罚。

（5）打击非法复制计算机数据类商品应转变观念。传统的版权法不涉及最终消费者，复印书刊和使用盗版书籍的，不构成违法。计算机数据类商品不同于普通的书籍、资料，它作为一种数字化的信息产品，可以直接作用于生产和生活，是一种重要的生产资料，不能把计算机数据类商品赋予同纸质的文字资料同样的法律地位。我国《著作权法》第22条规定，“为个人学习、研究

或者欣赏”和“为学校课堂教学或者科学研究”，可以不经著作权人许可，不向其支付报酬，使用他人作品。这一规定有制定时的特殊时代背景，因当时我国计算机应用程度很低，为扶持我国计算机应用的开展，著作权法放松对非法复制、使用他人作品的限制，这符合当时的国情。但目前我国计算机应用程度已经达到较高的水平，且计算机数据类商品制造业由于得不到有效的法律保障而一直徘徊不前或者发展缓慢，因此社会信息化发展需要加强对计算机数据类商品的保护，这也是信息产业界、司法界的期望。正如国家版权局许超副司长所讲，计算机软件功能性强，工具性强，很容易被复制的特点，使计算机软件著作权的保护与别的作品不同，不仅要在制造、销售领域予以保护，禁止违法复制和销售，而且要把法律延伸到最终用户的领域，对软件最终用户的复制和非法使用也要禁止①。为实现法律延伸到最终用户，现实的手段是利用刑法手段打击非法复制计算机数据类商品的行为。

综上所述，在刑法修改时应增设非法获取、使用计算机数据类商品罪。具体罪状表述如下：非法获取并使用计算机数据类商品，数额巨大或者有其他严重情节的，处 3 年以下有期徒刑或者拘役，并处或者单处罚金；数额特别巨大或者有其他特别严重情节的，处 3 年以上 7 年以下有期徒刑，并处罚金。

有学者对电子商务领域犯罪、计算机犯罪提出了增设“资格刑”的建议，认为计算机犯罪是一种高技术的职业犯罪，相应来说，如果设置或者规定一些剥夺其从事计算机行业的职业资格，将会对遏制和预防犯罪（包括特殊预防和一般预防）起到十分突出的作用。作者认为，为这类犯罪增设“资格刑”实际上行不通。这是因为：(1) 计算机犯罪不是高技术职业犯罪。计算机知

① 吴红志：《专家认为使用盗版软件也违法》，《光明日报》，1999 年 9 月 1 日。

识和技能并非仅为从事计算机相关职业的人员所掌握，随着计算机教育的普及、互联网络的广泛应用，计算机设备广泛进入普通家庭，非计算机职业的人员同样能够掌握计算机犯罪的技能、工具，实际生活中有大量计算机犯罪是非职业人员所为，因此，禁止犯罪人从事计算机有关职业的资格刑实际上起不到遏制和预防犯罪的作用。(2) 计算机、网络应用的广泛深入使禁止使用计算机、网络等设备的“资格刑”难以执行。随着计算机、网络技术和应用的迅速发展，曾经作为科学研究、专业处理工具的计算机、网络等设备设施已经进入家庭，网上购物、手机上网、能上网的信息化家电等使计算机、网络无处不在，要禁止犯罪人使用计算机、网络等于将其与日益信息化的社会隔绝，实际上难以执行。要强制执行这种“资格刑”几乎是剥夺了犯罪人的生存权，这种刑罚明显罚不当罪，是非人道的。

还有学者建议给计算机犯罪增设“罚金刑”，理由是计算机犯罪往往以牟利为目的。作者认为，这种建议值得商榷，计算机犯罪是一类犯罪，其中有些犯罪直接或者间接以牟利为目的，如利用计算机盗窃金融机构资产、利用计算机实施信用卡诈骗犯罪等，有些犯罪则不以牟利为目的，如出于泄愤报复而破坏他人电子商务网站的计算机信息系统。对这些犯罪一概处以罚金刑，显然没有反映犯罪的真实情况。此外，行为人出于牟利目的实施计算机犯罪、电子商务领域犯罪的，往往构成刑法规定的其他犯罪，依照《刑法》第 287 条和《关于维护互联网安全的决定》按照其他相应犯罪定罪量刑，而这些犯罪大多配置了罚金刑。因此，专门为计算机犯罪、电子商务领域犯罪增设‘罚金刑’实为多余。

第四节　迅速完善关于电子商务领域犯罪的刑事程序立法

一、有关计算机数据类证据的法律效力及其使用问题

证据在司法审判中起着关键作用，能否获取有法律效力的证明犯罪事实的证据，直接影响犯罪的认定和量刑的轻重。电子商务领域犯罪的证据不同于一般犯罪的证据，其中有一部分是计算机信息系统中存储、处理或者传输的计算机数据，它们往往对犯罪的认定起着关键作用，在有些电子商务领域犯罪案件中，能够证明犯罪事实的甚至只有这些计算机数据类证据。因此，计算机数据类证据的法律效力和使用方法，对有效追诉电子商务领域犯罪起着关键性的作用。

（一）计算机数据类证据的概念和特点

所谓计算机数据类证据，是指行为人在犯罪过程中，在计算机、网络设备设施以及附属外部设备如磁盘、可擦写光盘上留下的数字化信息痕迹，主要有：计算机信息系统事务日志文件中记录的操作、访问的系统资源，金融计算机信息系统资金账户上异常变动的资金数据，计算机病毒或者其他破坏性程序，淫秽色情图片、文字、声音、影像计算机文件，BBS 公告栏或者网页上的文字、广告等。这些证据的存储介质主要是计算机相关的存储、输出设备设施，如计算机信息系统上的硬盘、内部存储器（RAM），脱离计算机信息系统的光盘、软盘、磁带以及工作状况下的显示器、打印机内部存储器等。计算机数据类证据与传统的证据有很多不同之处，它有以下基本特点：

1. 容易伪造或者被篡改

计算机、网络技术的特性使计算机数据类证据难以保存。这些计算机数据类证据大多以电磁记录形式存在，电磁记录的重要

特点是容易被重新磁化即被修改或者破坏，修改后的数据完全不保留修改前数据的痕迹，而且，多数情况下被修改、删除的计算机数据难以恢复。电子商务领域犯罪行为人可以利用网络技术，远程侵入计算机信息系统作案，并及时转移或者销毁罪证。此外，计算机操作人员的差错、侦查人员的错误处理以及供电系统、通信网络的故障等方面的原因，都可能导致计算机数据类证据的变动。

2. 无形、不直观

计算机数据类证据是数字化的信息记录，它没有固定的表现形态，必须借助于一定的介质如磁盘、光盘才能存储固定下来，不能脱离其介质来展示这类证据。这类证据内容的表现不像其他法定证据一样直观，仅仅展示存储计算机数据类证据的磁盘、光盘和存储器并不能起到证明的作用，还必须借助于一定的设备才能进行，而且必须运用一定的计算机专业知识，例如理解事务日志文件记录的内容需要一定的计算机技术基础知识。有些计算机数据类证据内容的展示，技术性要求很高，必须在一定的技术环境下才能正确表现其真实面貌，例如侵犯商业秘密的行为人把商业秘密文件数据隐藏在普通图像文件中，或者将商业秘密数据加密，不凭借一定的专业技术难以找出罪证。

此外，计算机数据类证据还具有高技术性、信息复合性、易存储性、能够反复展示等特性。

（二）计算机数据是否为具有法律效力的证据

我国《刑事诉讼法》规定了七种证据：物证、书证；证人证言；被害人陈述；犯罪嫌疑人、被告人供述和辩解；鉴定结论；勘验、检查笔录；视听资料。计算机数据类证据是否属于以上七类之一，学者们根据对视听资料的不同理解，得出不同结论。有人认为，“无论怎样理解，计算机电磁记录及命令记录都不可能

为任何一种证据类型所包括”①，从而否认计算机数据是具有法律效力的证据。又有人认为，“我国现行《刑事诉讼法》第 42 条明确规定，视听资料为刑事诉讼中一项独立的证据，因而电子计算机记录成为一项独立证据似乎有了合法依据”②；“视听资料主要是在案件发生过程中对有关声音和形象的记录形成的，它以声象的动态复原反映案件事实”，“主要包括：录音资料、录像资料、电子计算机贮存的资料，以及其他运用专门技术设备得到的信息资料”③，从而倾向于承认计算机数据类证据的法律效力。

在国际上，关于计算机数据的法律效力也存在激烈的争论，但是，承认计算机数据类证据的成为发展趋势。在 1982 年欧洲理事会的报告《电子处理资金划拨》和 1982 年英国 A.Kelman 和 R.Sizer 论文《计算机在法庭上的地位》中，已经提出了计算机记录相当于书面文件，并作为证据的看法。联合国贸易法委员会秘书处在第 18 届会议上提出《计算机记录的法律价值》的报告，建议各国政府重新审查涉及使用计算机记录作为诉讼证据的法律规则。1996 年联合国贸易法委员会通过了《电子商务示范法》，该文件第 5 条规定，不得仅以某项信息采用数据电文形式为理由而否认其法律效力、有效性和可执行性。1996 年国际海事委员会采用了一套资源规则，承认数码信息具有与书面单证同样的效力。2000 年 6 月 30 日美国总统克林顿签署《美国全球和国家商务中的电子签名法》法案，该法案给数字签名交易提供了法律支持，使得数字签名在法律上等同于书面签名。

作者认为，计算机数据成为我国刑事审判中具有法律效力的

---

① 于志刚《计算机犯罪研究》，中国检察出版社 1999 年版，第 226 页。

② 刘广三：《计算机犯罪论》，中国人民大学出版社 1999 年版，第 198 页。

③ 徐静村：《刑事诉讼法学》（上），法律出版社 1997 年版，第 162 页。

证据是社会发展的必然趋势，也为惩治电子商务领域犯罪所必需。但是，视听资料证据不能涵盖计算机数据，必须通过刑事诉讼法明确其证据效力，同时规定使用的程序。理由如下：(1) 计算机数据类证据是信息社会发展的必然产物，是信息时代广义物证的一种，是科学证据的一种新类型，承认其在我国刑事诉讼中的法律效力符合社会发展的趋势，对打击日益严重的电子商务领域犯罪，计算机数据类证据是必需的法律武器。此外，在民商法等其他部门法律中，计算机数据类证据已经为法律所认可，如我国修改后的《合同法》第 11 条明确规定合同的书面形式包括数据电文。(2) 所谓视听资料，如前面有的学者所述，“是指在案件发生过程中对有关声音和形象的记录形成的，它以声像的动态复原反映案件事实”，把计算机数据纳入视听资料，是因为它可以通过一定设备显示出来。但是，计算机数据承载的信息通过一定的设备表现出来，并非全部可为人们视觉、听觉直接感知，例如行为人破坏远程医疗，向正在进行计算机控制的手术中的病人发送强电磁波干扰，侦查人员虽然可以获取行为人发送的干扰电波计算机数据文件，但是这些数据通过电子设备所表现出来的，却不是人们视觉或者听觉所能直接感知的。因此，视听资料和计算机数据类证据是两个相交的集合，不能把计算机数据类证据简单纳入视听资料的范围。(3) 由于计算机数据必须存储在一定的介质上，必须通过一定的电子设备才能表现其承载的信息。因此，使用这些计算机数据作为证据，必须考虑可能由于使用的设备或应用的技术不同，导致计算机数据证据在表现上的差异，如使用一台不满足计算机病毒发作条件的计算机，就无法展示计算机病毒的破坏作用。因此，我国刑事诉讼法在规定计算机数据类证据时，应该同时规定这类证据的使用条件和程序，即犯罪发生时相同或最相似的环境条件。

综上所述，建议修改刑事诉讼法，增设计算机数据类证据，并规定查证这类证据时，必须使查证所使用的设备处于与犯罪时

相同或者最相似的环境条件下。

（三）计算机数据类证据使用中的原件问题

在刑事审判中，证据查证是必需的环节，而且一般情况下证据查证应当使用证据原件。计算机数据类证据的特性使得这类证据的使用具有一定特殊性。计算机数据类证据是犯罪过程中留在计算机信息系统中的电磁记录，如果证据查证必须使用原件，就必须将保留有犯罪证据的计算机信息系统整体搬运到法庭上，并且在适合计算机信息系统正常工作的条件下，将其运行起来。如果需要转移的只是设备较少的计算机信息系统，直接使用证据原件还有可能，如果计算机数据类证据保留在多个或者规模庞大的计算机信息系统中，要使用计算机数据类证据的原件就无法实现了。因此，计算机数据类证据举证查证时，大量使用的是这类证据的复制件而非原件。这样，计算机数据类证据复制件的法律效力问题，或者说，计算机数据类证据的使用程序问题直接关系能否有效追诉电子商务领域犯罪。

世界各国证据法对法庭是否必须使用证据原件有不同的规定。在英美证据法中，根据最佳证据规则，只有证据原件才能被法院采纳，这给惩治电子商务领域犯罪带来法律上的障碍。为消除传统证据法对电子商务发展的阻碍，1996 年联合国贸易法委员会通过了《电子商务示范法》，该文件第 9 条规定了对数据电文的可接受性和证据力：(1) 在任何法律诉讼中，证据规则的适用在任何方面均不得以下述任何理由否定一项数据电文作为证据的可接受性：(a) 仅仅以它是一项数据电文为由；或 (b) 如果它是举证人按合理预期所能得到的最佳证据，以它不是原样为由。(2) 对于以数据电文为形式的信息，应给予应有的证据力。可见，确认计算机数据类证据复制件在一定条件下与原件具有相同的法律效力，是电子商务发展的需要，也是证据法发展的趋势。

我国刑事诉讼法没有明确规定在刑事审判中是否可以使用证

据复制件。作者认为，应当修改我国刑事诉讼法关于证据使用的规定，即规定在一定条件下，提交计算机数据类证据复制件具有原件相同的法律效力。理由如下：(1) 承认计算机数据类证据复制件的法律效力是社会发展的需要，也是世界各国证据法的发展趋势。(2) 我国《民事诉讼法》第 68 条规定，“书证应当提交原件。物证应当提交原物。提交原件或者原物确有困难的，可以提交复制品、照片、副本、节录本。提交外文书证，必须附有中文译本”。在特殊情况下允许使用证据复制件的原则，应当为我国刑事诉讼法所采纳。(3) 由于计算机数据类证据具有自身特有的容易伪造和被篡改、无形、表现不直观等特点，使用计算机数据类证据复制品应该规定严格的使用程序，保证复制品制作、使用能够真实体现原件所反映的犯罪情况。

二、建立回溯查因的网络行踪刑事侦查制度

电子商务领域犯罪不同于普通形式的犯罪，它凭借计算机、网络技术潜行于互联网络空间，传统的刑事侦查不适应这类特殊的犯罪，难以有效地发现犯罪嫌疑人并获取犯罪证据。因此，必须建立针对这类犯罪的特殊的刑事侦查制度。

所谓回溯查因的网络行踪刑事侦查制度，是指依照法定程序，记录互联网络用户网络上的行踪，并根据这些计算机数据记录追踪犯罪嫌疑人，获取犯罪证据的刑事侦查制度。为实现这一特殊的刑事侦查制度，首先必须有相应的技术装备，并建立一定的行政管理制度，如前面提出的网络经营单位和个人的协助制度、个人电子身份证管理制度，以实现对互联网络上的违法犯罪行为的有效控制。网络经营单位和个人的协助制度要求网络经营单位和个人根据公安机关的要求，安装专用的记录网络用户在该网络中使用情况的技术设备，并负有保护其正常工作的义务；个人电子身份证管理制度要求根据自然人的惟一性生理特征建立电子身份证，个人使用互联网络时首先要经过生理特征和电子身份

证的验证，否则不允许其使用互联网络，或者提请他人警觉。电子身份证管理制度与信息网络经营单位协助制度相配合，将能够将上网者在网络上的一举一动和活动的行踪全部记录下来，使信息网络上的违法犯罪人再不是来无影去无踪的“隐身人”。当发生利用互联网络的刑事案件时，公安机关根据“回溯查因”刑事侦查制度，依照法定程序，调取网络经营单位计算机信息系统中的记录信息，追踪犯罪嫌疑人，获取犯罪证据。

“回溯查因”刑事侦查制度是专门针对利用计算机、互联网络犯罪建立的特殊刑事侦查制度，真正实现了对互联网络活动的全面、有效监控，能够给违法犯罪行为人构成极大的威慑力，迫使行为人自觉遵守法律法规、社会规范，其更重要的作用是能够有效地追踪犯罪嫌疑人的网上行踪，查获犯罪证据，侦破刑事案件，弥补传统刑事侦查制度在计算机、互联网络环境中的不足。

“回溯查因”刑事侦查制度要求记录并调查网络用户在网络上的行为，而政府机构监控、调查网络用户网上行为，在国外被认为有侵犯公民隐私权之嫌，因此，“回溯查因”刑事侦查制度是否侵犯人权，决定其能否成为刑事侦查制度。作者认为，“回溯查因”制度不仅不侵犯公民的人权，而且是对公民在互联网络上合法行使权利的有力保障，理由如下：(1) 由于互联网络应用虚拟化、跨度大、范围广泛，以及利用计算机、网络犯罪具有高技术性的特点，传统的侦查手段难以有效发现犯罪嫌疑人，获取有效犯罪证据，致使这类犯罪猖獗一时，对国家利益、社会公共利益和公民个人合法权利造成严重危害。而建立“回溯查因”制度，是为了有效追诉这类违法犯罪行为，惩治犯罪，为公民在互联网络上合法行使权利提供有力的法律保障。(2)“回溯查因”制度在调查犯罪时，对公民的隐私权可能构成一定程度的侵犯，如侦查人员在执行公务活动中了解了合法公民的私人秘密，但这是法律保障公民权利正常行使所必须付出的代价，这一代价可以通过规定“回溯查因”刑事侦查的严格程序降低到最小的程度。

(3)“回溯查因”刑事侦查与未经法律允许的秘密侦查行为有本质区别。后者是刑事侦查人员为获取犯罪证据，不经法定程序，采用非法手段如秘密窃听等的侦查行为，是一种非法行为，但有些西方国家认为这样获取的证据不具有法律效力；前者是侦查人员根据刑事诉讼法规定的特殊刑事侦查制度，经过法定程序批准，严格履行法律规定的各项职权，追踪犯罪行为，获取犯罪证据的行为。

“回溯查因”刑事侦查制度是一种特殊的侦查制度，在进行这类侦查时不可避免要接触较大范围内的网络用户的个人网上行为资料，在一定程度上侵犯到公民的权利，因此，在制定“回溯查因”刑事侦查制度时，必须严格规定进行这类侦查的程序、侦查人员的职责权限范围等，避免扩大对公民合法权利的侵犯。作者认为“回溯查因”刑事侦查制度应当包括以下几个方面的规定：

1. 批准程序

“回溯查因”侦查应当经过人民检察院批准才可以实施。我国《刑事诉讼法》第7条规定，“人民法院、人民检察院和公安机关进行刑事诉讼，应当分工负责，相互配合，相互制约，以保证准确有效地执行法律”。第8条规定，“人们检察院依法对刑事诉讼实行法律监督”。为体现我国刑事诉讼法的基本原则，避免公安机关自批自侦带来侵犯公民合法权利的弊端，公安机关实施“回溯查因”侦查，应当经同级人民检察院批准或者决定，公安机关持人民检察院签发的批准文件到网络经营单位进行侦查，被侦查单位有协助义务。

2. 侦查人员的泄露责任

侦查人员只能把与案件相关的犯罪嫌疑人的个人记录作为案件材料，不得泄露合法用户的个人资料和犯罪嫌疑人的个人资料，就是说，不仅合法用户的个人资料不得泄露，犯罪嫌疑人的非案件相关的个人资料也不得泄露，否则也构成对犯罪嫌疑人正

当权利的侵犯。

3. 规定“回溯查因”刑事侦查获取的信息的保存、使用、销毁程序。

4. 规定非法进行“回溯查因”侦查的法律责任，包括行政、民事、刑事责任和国家赔偿责任等。

第五节　在司法中应该注意的问题

电子商务领域犯罪的刑事司法主要体现在侦查和审判两个阶段，以下对其在刑事侦查和审判阶段应该特别注意的问题进行研究①。

一、侦查阶段

我国刑事诉讼法规定，刑事案件的侦查由公安机关负责，公安机关在侦查中的主要职责是收集、调取犯罪嫌疑人有罪或者无罪、罪轻或者罪重的证据材料。电子商务领域犯罪证据与一般犯罪证据不同，它们主要是计算机信息系统中存储、处理和传输的计算机数据，由于这类证据具有自身的特点，对这类证据的侦查应当有相应的特殊处理方法，具体表现在证据的搜查、保全和固定等环节上。

（一）计算机数据类证据的搜查

由于计算机数据类证据的特殊性，对这类证据的搜查比较困难，而且，搜查到一些计算机数据类证据后，如何保证其证据力，是侦查人员应当认真对待的问题，否则，就容易导致对计算机数据类证据的处理不当而使搜查到的证据丢失。美国司法实践

---

① 以下内容主要参考：马秋枫、江向阳、邢颖、冉瑞雪著：《计算机信息网络的法律问题》，人民邮电出版社 1998 年版，第 263～284 页；刘广三著：《计算机犯罪论》，中国人民大学出版社 1999 年版，第 196～213 页。

中有这样一个案例，警察在搜查贩毒集团总部时，发现一台正在运行的计算机，计算机显示表明机内存储有毒品分销渠道的信息和吸毒人员名单，警方对如何提取这一证据不知所措，于是将整个计算机拆卸运送到警方的技术中心，然而在警方拆卸、运送过程中，磁盘文件已经被损坏，导致重要的证据材料因为搜查方法不当而得而复失。因此，对这类证据搜查的一些环节应当予以特别注意。

1. 搜查证

法律规定，进行搜查必须持县级以上侦查机关负责人签发的《搜查证》，只有在紧急情况下，例如不提取证据有可能灭失、改变、伪造、变造，可以不需要搜查证进行搜查。签发搜查证，应当注意：(1) 无论是进行公开搜查或秘密搜查，只在必要时才对计算机信息系统进行搜查。(2) 选择搜查时机。(3) 确定搜查范围。决定前应当征求计算机专家的意见。(4) 在搜查证上指明协助专家。

2. 依靠专家的协助

每一个计算机信息系统都有自己的特点，搜查不同的计算机信息系统应根据其特点进行，如果不具备存取特殊计算机信息系统的技能，在搜查中一定要有一位可靠的专家协助，以避免处理不当丢失信息或者造成证据的毁灭。侦查中专家的地位不同于鉴定人，他们是协助侦查机关的专业人员，不存在专家结论性意见的问题，而且必须对侦察员、计算机侦查现场专家进行训练，以使他们对证据的规定和调查方法非常了解。此外，如果有疑问，应当向有专门技能的人员咨询，咨询的对象可能包括受害者、顾问、证人、计算机软硬件的供货人，或者计算机安全系统的设计者。询问犯罪嫌疑人的意见也是其中之一，但是应当认真审查，防止因为其虚伪陈述导致证据的毁灭。

3. 作好搜查前的准备工作

首先，要设法获取被搜查系统的尽可能多的信息。在准备搜

查时，必须做到充分了解计算机信息系统，以保证有适当的技能进行搜查，对系统及布局知道得越清楚，搜查准备工作就做得越好，其中应当特别注意掌握安全系统的安全方法。其次，要准备搜查所需的工具，包括操作系统软件、应用软件、硬件设备和拆卸维修工具等。再次，要制定搜查计划。对计算机信息系统的搜查要力争一次成功，避免犯罪分子察觉后转移或者销毁证据，系统越大，计划越重要，计划的制定也应当越细致，计划内容应当包括行动的指挥，设备、人员的分工，预定的目的等。

4．搜查的实施

进行搜查应当遵循以下原则：(1）立即让操作人员离开计算机信息系统；(2）把放计算机的地方，系统的屏幕、外设和其他设备进行照像和录像；(3）遵守计算机操作的基本原则；(4）给所有的硬件、文件资料、磁盘等做标记；(5）搜寻包含用户标识和密码的文件资料；（6）若移动可拆卸设备，必须注意磁场；(7）使用静电保护设备，保护证据不受损坏；(8）使用自备的软件检查系统；（9）搜获的文件做好清楚、完整的拷贝，供审查用，审查证据时不得使用原始软件或者证据，防止造成原始证据的损坏；(10）搜索系统中是否还有未提取的证据；(11）使搜获的原始软件、计算机文件等处于不可改写状态；(12）把采取的各步骤及遇到的情况记录成文；(13）应谨慎对待犯罪嫌疑人的问答。

此外，还应对以下环节特别注意：(1）对正在运行的计算机信息系统，如果不带回搜查，而要求现场搜查的，必须严格依照操作程序进行。对正在利用互联网络下载或者上载信息的，应当查明联络对方，并记录传输的文件。(2）注重外部搜查，包括书面文件、打印机、显示器和其他外围设备，提取这些设备上保留的证据记录。（3）检查系统设备时，应当采用照像、录像、记录、绘图等方法记录清楚系统的结构布局。(4）搜查访问控制系统，可能遇到物理上或者逻辑上加有安全措施的系统，对此，最

好找到提供用户标识和密码的人，如果暂时无法进入系统，应当先把系统保存好，请专家、软件供应商或者系统制作者绕过系统控制。(5) 搜查系统中的计算机文件，要有条理地详细进行，同时防止犯罪人利用改变文件后缀、加密等手段隐瞒真实情况。

5. 制作搜查笔录

对搜查的情况应当写成笔录，并写明发现何种证据，提取和扣押物证、书证、视听资料的名称、数量和特征等。对软件和系统部件实施扣押时，要注意做好标签，贴标签时应当注意便于机器的重新装配和以后的系统检查及作为证据呈堂。笔录应当由侦查人员、被搜查人或者他的家属、邻居、单位负责人或代表，或者其他见证人签名或者盖章，如果被搜查人或者他的家属不在现场，或者拒绝签名或盖章的，应当在笔录上注明。此外，对计算机信息系统的秘密搜查和扣押，应当告知系统所有人、使用人、负责人，并且侦查部门应当决定何时告知已被搜查和被扣押的证据。

6. 运送证据

计算机数据类证据的运送主要考虑防止证据的毁灭或者损坏，如使用装备无线电设备的车辆运送时，要关掉所有无线电发送设备，防止电磁波对计算机存储设备的损坏；注意证据设备的防潮、防撞击和温度控制；用文字记载设备的监护过程等。

(二) 计算机数据类证据的保全和固定

证据的固定直接关系到能否保障证据的证据能力与证明力，证据固定和保全如果符合法律手续，证据的真实性和可靠性才有保障。我国《刑事诉讼法》第 114 条第 2 款规定，“对于扣押的物品、文件，要妥善保管或者封存，不得使用或者损毁”。依据这一法律规定，并结合计算机数据类证据的特点，保存这类证据应当注意以下方面：(1) 制作多个备份。对于计算机数据类证据最少要保留两个复制品，原件应当存储在专门的保管室中，由专门的保管员负责。复制品再次复制后供侦查人员审查证据时使

用。(2) 保障证据安全。自然因素导致的意外事故和人为的破坏都可能造成证据的毁损或者改变，应当做好存储证据环境的防静电、防磁场干扰、防高温、防湿和除尘等工作，同时，还要做好防止人为破坏。(3) 严格过程管理。证据的移交、保管、开封、拆卸的过程必须有侦查人员和保管人员共同完成，对于证据的封印，必须每个环节都检查封印的真实性和完整性，并制作详细的笔录，由行为人共同签名。(4) 制定责任追究制度。法律应规定保管人员有义务真实可靠地保管好证据并应司法机关的要求提交证据和违反保管义务所应负的法律责任，以及保管人员有义务在法庭上就证据保管作证并提供笔录，协助法庭判断保管过程中证据的真实性。

二、审判阶段

(一) 计算机数据类证据的审查判断

我国刑事诉讼法规定，证据必须经过查证属实，才能作为定案的根据。计算机数据类证据的审查判断，是指审判人员对收集的计算机数据类证据进行分析研究，鉴别其真伪，找出它们与案件事实之间的客观联系，确定其证明力。由于计算机数据类证据的特殊性，对这类证据的审查判断应当关注以下几个方面：

1. 计算机信息系统是否正常工作

计算机数据类证据在计算机信息系统中产生、存储和传输，因此计算机信息系统是否正常工作，直接影响这类证据的客观性。对计算机信息系统功能是否正常的判断，主要关注两个方面：

其一，是与计算机数据类证据产生、存储和处理直接相关的设备和工作环境是否正常，能否对证据产生影响，考虑的因素有：(1) 输入输出、处理、存储等设备是否工作正常和可靠；(2) 计算机信息系统运行依赖的软件程序是否正常运行，是否能够保障设计功能的正常发挥；(3) 网络传输设备设施及应用程序

是否工作正常和可靠；(4) 系统存储设备和存储介质是否工作正常可靠；(5) 系统运行的工作环境是否正常可靠。

其二，计算机信息系统的安全性能是否可靠，主要是指计算机信息系统是否具有防止非法侵入、对系统资源数据的访问控制能力和自我恢复、自我保护的能力，计算机信息系统安全性是否可靠，直接关系到系统内计算机数据的安全可靠。判断计算机信息系统安全性主要衡量计算机信息系统设备设施的物理安全性，安全管理是否健全落实，以及计算机信息系统是否配备有效的安全技术措施。

2. 计算机数据类证据的收集、固定的合法性和可靠性

计算机数据类证据的收集、固定的合法性和可靠性要求，主要是保障在证据收集、固定过程中的技术可靠性和程序合法性。由于计算机数据类证据的技术特征，侦查机关使用侦查设备收集证据时，必须保证计算机数据类证据不被损毁、损坏或者被非法篡改，保障提取证据的真实性。

侦查人员侦查行为是否合法，直接关系到证据的有效性，因此，应当审查收集这些证据之前是否履行了必要的审批手段，对于通过搜查、扣押等方式取得的证据，要审查进行搜查和扣押时是否遵守法定程序，以保障搜集的证据符合法定要求，保障公民的人身权利和民主权利不受侵犯，同时，也为了防止不法分子利用非法收集证据的机会来伪造证据，栽赃陷害。

3. 计算机数据类证据内容的关联性

搜集到计算机数据类证据后，还应对证据所提供的内容进行分析，注意是否前后一致，自身是否存在逻辑矛盾，内容是否合乎情理，对于涉及专业知识的计算机数据类证据，还应该由专家进行分析鉴定，以判断证据的真伪和与案件的联系。对于与案件事实无关的计算机数据类证据，即使客观真实也无助于查明案情，不具有任何证明作用。

4. 结合全案其他证据综合审查判断

在分析计算机数据类证据的来源和内容之外，还要将这类证据结合案件其他证据，进行综合分析，从证据与证据的相互印证、相互联系上去考虑，看它们所反映的情况是否一致，是否协调，以便比较容易地发现问题，判明真伪。在对案件全部证据进行综合审查判断时，应当注意以下几个方面：(1) 审查有无事件或者行为的原始书面记录。要求当事人提供原始的、未经加工的数据，以与结果数据进行对比，寻找其中可能存在的差异，判别计算机数据类证据的真伪。(2) 审查各种在业务过程中形成的书证。计算机系统的日程管理和案情审查记录、故障分析记录、维修和检测记录这些书面材料，在诉讼中都应提交司法机关作为书证使用，它们对系统的可靠性和系统负责人提供的证言起到相互印证的作用，此外，完整的过程记录材料还能为侦查提供线索，确定可能的作案时间和犯罪人。(3) 审查计算机信息系统对数据的备份和是否有可恢复的剩余数据。这些数据是计算机系统自动生成，由于其数据的特性和存储方式不同于一般计算机数据文件，因而难以篡改、删除，能够反映案件的真实情况。(4) 审查计算机信息系统运行各个环节可能存储下来的信息之间的印证关系。计算机信息系统的一个处理过程能够同时在其各个环节有所反映，犯罪行为人即使能够删除、伪造某些主要的犯罪证据，但往往难以穷尽所有环节留下的信息，综合审查计算机信息系统各个环节可能保留的信息，有利于鉴别证据的真伪和发现新的线索。(5) 审查计算机信息系统的各种日志文件和其他监控记录文件。对不同环节的日志文件和其他监控记录文件进行分析比较，可能为案件的侦破提供一些线索，并有助于鉴别其他计算机数据类证据的真实性。

(二) 计算机数据类证据的法庭出示程序

我国《刑事诉讼法》第 157 条规定：“公诉人、辩护人应当向法庭出示物证，让当事人辨认，对未到庭的证人的证言笔录、鉴定人的鉴定结论、勘验笔录和其他作为证据的文书，应当当庭

宣读。审判人员应当听取公诉人、当事人和辩护人、诉讼代理人的意见。”第160条规定：“经审判长许可，公诉人、当事人和辩护人、诉讼代理人可以对证据和案件情况发表意见，并且可以相互辩论。”计算机数据类证据要作为定案的根据，一般应当出示，听取公诉人、当事人和辩护人、诉讼代理人以及其他诉讼参与人对该证据的内容以及其他方面的意见。在计算机数据类证据的法庭出示环节中，可能存在两个应当注意的问题，其一是可以在法庭出示的计算机数据类证据的范围；其二是计算机数据类证据的出示方式。

1. 计算机数据类证据的出示范围

计算机数据类证据出示范围问题主要是涉及国家秘密、商业秘密和个人隐私的证据是否在法庭出示和如何在法庭出示。我国《刑事诉讼法》第152条规定：“人民法院审判第一审案件应当公开进行，但是有关国家秘密或者个人隐私的案件，不公开审理。”这里的不公开审理，是指法庭审理过程不公之于众，但是，涉及国家秘密、个人隐私的证据同样要依刑事诉讼程序在法庭上出示，经过法庭查证，才能成为定案的根据。因此，如果计算机数据类证据包含有国家秘密、商业秘密和个人隐私的，法庭应该行使自由裁量权：如果该证据对诉讼证明至关重要，在诉讼中需要作为证据采纳时，原则上应当在法庭上出示和查证；如果该证据对诉讼证明不属于关键证据，可以不引用该证据。同时，应当在程序上作适当限制，以防止国家秘密、商业秘密和个人隐私被泄露。对于故意泄露者，甚至利用商业秘密牟取商业利益者，要依法追究法律责任。

2. 计算机数据类证据的出示方式

计算机数据类证据表现的信息可能有多种媒体方式，如文字、图片、声音、影像等，这些媒体形式的信息不一定必须以打印方式输出出示，各种信息输出方式可以相互印证，有利于加深法官的理解。计算机数据类证据的存储体必须提交法庭，以利于

双方当事人对存储体进行检索和查询；对于存储体存储的信息内容，提供方应当说明该信息内容的目录、数据组织方式、操作系统和应用系统及正确查询该信息所需的资料，以及可用以证明其诉讼主张的信息内容的产生方式和打印输出件。这些材料应当分类组织，以清单方式提交法庭；对方当事人申请查询存储体时，应由检察官、双方当事人及他们的律师和诉讼代理人在场，并且其查询的方法必须有合理的根据；计算机数据类证据存储体及其产生的各种形式的材料，都应当附卷备查。查询得知的资料，与案件的证明没有关系的，应在检察院的监督下不迟延销毁。并且，法律规定不得泄露的信息，不得泄露或者恶意利用，否则，应当承担相应的法律责任。

为证明产生、处理、存储计算机数据类证据的计算机信息系统的安全性和可靠性，必须对计算机信息系统本身进行审查。一般而言，对计算机信息系统的审查应当到系统所在地进行，由司法机关依照鉴定的程序指定或者聘请专家进行。依照法律程序当事人申请鉴定，司法机关决定进行鉴定的，也要依照鉴定的程序、方式和手续进行。

主要参考文献

一、论　　著

1. 马克昌主编：《犯罪通论》，武汉大学出版社 1995 年版。
2. 马克昌主编：《刑罚通论》，武汉大学出版社 1995 年版。
3. 马克昌：《刑法理论探索》，法律出版社 1995 年版。
4. 高铭暄、马克昌主编：《刑法学》（上、下编），中国法制出版社 1999 年版。
5. 赵廷光主编：《中国刑法原理》，武汉大学出版社 1992 年版。
6. 康树华主编：《犯罪学通论》，北京大学出版社 1992 年版。
7. 莫洪宪主编：《犯罪学概论》，中国检察出版社 1999 年版。
8. 莫洪宪著：《有组织犯罪研究》，湖北人民出版社 1998 年版。
9. 高铭暄、赵秉志主编：《刑法论丛》第 1 卷，法律出版社 1998 年版。
10. 高铭暄、赵秉志主编：《刑法论丛》第 2 卷，法律出版社 1999 年版。
11. 谢望原主编：《台、港、澳刑法与大陆刑法比较研究》，中国人民公安大学出版社 1998 年版。
12. 陈兴良主编：《刑事法评论》第 3 卷，中国政法大学出

版社 1999 年版。
13. 姜伟著：《犯罪形态通论》，法律出版社 1994 年版。
14. [德] 汉斯·约阿希姆·施奈德著，吴家涛、马君玉译：《犯罪学》，中国人民公安大学出版社 1990 年版。
15. 赵廷光、朱华池、皮勇著：《计算机犯罪定罪量刑》，人民法院出版社 2000 年版。
16. 金融系统电子商务联络与研究小组编：《电子商务——安全认证与网上支付》，人民出版社 2000 年版。
17. 姚立新著：《电子商务透视》，经济管理出版社 1999 年版。
18. 张楚著：《电子商务法初论》，中国政法大学出版社 2000 年版。
19. 台湾法学会编印：《网路与法律研讨会专辑》，《台湾法学会学报》第 19 辑。
20. 冯震宇著：《网路法基本问题研究（一）》，学林文化事业有限公司 1999 年版。
21. [美] 基蒂·卡拉维塔著，李斯译：《白领犯罪——金融业巨额诈骗及权术》，光明日报出版社 1998 年版。
22. 黄学彬编著：《接近零点——全球反计算机犯罪透视》，四川人民出版社 1997 年版。
23. （法）安德鲁·博萨著，陈正云、孙丽波等译：《跨国犯罪与刑法》，中国检察出版社 1997 年版。
24. 刘广三著：《犯罪现象论》，北京大学出版社 1996 年版。
25. 刘广三著：《计算机法》，中国社会科学出版社 1993 年版。
26. 刘广三著：《论计算机犯罪》，中国人民大学出版社 1999 年版。
27. 于志刚著：《计算机犯罪研究》，中国检察出版社 1999 年版。

28. 孙铁成著：《计算机与法》，法律出版社 1998 年版。
29. 陈兴实、付东阳编著：《计算机、计算机犯罪、计算机犯罪的对策》，中国检察出版社 1998 年版。
30. 王世洲著：《德国经济犯罪与经济刑法研究》，北京大学出版社 1999 年版。
31. [美] 刘江彬：《计算机法律概论》，北京大学出版社 1992 年版。
32. [英] 尼尔·巴雷特著，郝海洋译：《数字化犯罪》，辽宁教育出版社 1998 年版。
33. [美] 马克·斯劳卡著，黄倍坚译：《大冲突：赛博空间和高科技对现实的威胁》，江西教育出版社 1999 年版。
34. [美] 爱德华·A·卡瓦佐、加斐诺·莫林著，王月瑞译：《赛博空间和法律：网上生活的权利和义务》，江西教育出版社 1999 年版。
35. [美] 劳拉·昆兰蒂罗著，王涌译：《赛博犯罪：如何防范计算机犯罪》，江西教育出版社 1999 年版。
36. [英] 巴雷特著，李新玲译：《赛伯族状态：因特网的文化政治和经济》，河北大学出版社 1998 年版。
37. [美] 普拉特著，郭立峰译：《混乱的联线：因特网上的冲突与秩序》，河北大学出版社 1998 年版。
38. [美] 理查德·A·斯皮内洛著，刘钢译：《世纪道德：信息技术的伦理方面》，中央编译出版社 1999 年版。
39. 胡泳、范海燕著：《黑客——电脑时代的牛仔》，中国人民大学出版社 1997 年版。
40. 周能友、朱晓兰编著：《Internet 集中营》，中国城市出版社 1998 年版。
41. 杨杰超、武斐等编译：《计算机病毒危机》，北京大学出版社 1992 年版。
42. 张汉亭编著：《计算机病毒与反病毒技术》，清华大学出

版社 1996 年版。
43. 余建斌编著：《黑客的攻击手段及用户对策》，人民邮电出版社 1998 年版。
44. 林山田、林东茂著：《犯罪学》，台湾三民书局印行 1995 年版。
45. 张台先：《网路法律》，美商艾迪生维斯理、儒林图书公司 1997 年版。
46. [美] 无名氏著，王锐等译：《网络最高安全技术指南》，机械工业出版社 1998 年版。
47. [美] Marc Parley、Tom Stearns、Jeffrey Hsu 著，李明之、赵粮、张侃等译：《网络安全与数据完整性指南》，机械工业出版社 1998 年版。
48. [美] David J·Stang、SylviaMoon 著，程佩青、闰慧娟等译：《计算机网络安全奥秘》，电子工业出版社 1994 年版。
49. [日] 日本律师联合会、刑法修正对策委员会合编：《计算机犯罪与现代刑法》，三省堂 1990 年版。
50. [日] 芝原邦尔等著：《刑法理论之现代的展开》（各论），日本评论社 1996 年版。
51. [日] 本江威熹监修：《与民商事相交错的经济犯罪》，立花书房出版社平成 7 年版。
52. [日]《法律时报》第 70 期。
53. [澳] 张立中编：Computer Crime and Legal Prevention，法律出版社 1999 年版。

二、论　文

1. 赵廷光：《信息时代的电脑犯罪与刑事立法》，《法商研究》1997 年第 2 期。
2. 皮勇：《略论网络上计算机犯罪与对策》，《法学评论》

1998 年第 1 期。
3. 赵廷光、皮勇：《论我国刑法中的计算机犯罪》，《现代法学》1999 年第 4 期。
4. 赵廷光、皮勇：《关于利用计算机实施盗窃罪的几个问题》，《中国刑事法杂志》2000 年第 1 期。
5. 赵廷光、皮勇：《电子商务与计算机犯罪》，《法学杂志》2000 年第 2 期。
6. 皮勇：《论金融领域计算机犯罪》，《法学研究》2000 年第 2 期。
7. 赵廷光、皮勇：《电子商务安全的几点刑法对策》，《法商研究》2000 年第 6 期。
8. 朱华池著：《计算机犯罪研究》，武汉大学 1999 年博士学位论文。
9. 文军、艾湘涛：《略论信息犯罪及其安全对策》，《刑事法学》1998 年第 6 期。
10. 王德全：《试论 INTERNET 案件的司法管辖权》，《中外法学》1998 年第 2 期。
11. 朱汉章：《侵犯商业秘密罪及其司法认定》，《法制论丛》1998 年第 1 期。
12. 江向阳、马秋枫：《计算机安全与电子监测》，《现代法学》1996 年第 5 期。
13. 袁泳：《计算机网络上数据传输的版权问题研究》，《中外法学》1998 年第 1 期。
14. 袁泳：《计算机网络上数据传输的版权问题研究》，《中外法学》1998 年第 1 期。
15. 藤琪：《台湾有关电脑犯罪的法学研究概述》，《台湾法研究学刊》1997 年第 3 期。
16. 于志刚、蒋浩：《论制作、传播破坏性计算机程序罪》，《法学家》1997 年第 5 期。

17. 冯英菊：《计算机犯罪罪名设置的立法探讨》，《法学与实践》1997 年第 4 期。
18. 毕惜茜、姜平：《美国计算机犯罪的刑事立法述评》，《法学家》1993 年第 4 期。
19. 张健：《美国计算机犯罪刑事立法动态研究》，《外国法学研究》1996 年第 3 期。
20. 张健、张亚光：《美国计算机犯罪的刑事立法》，《行政与法》1996 年第 4 期。
21. 杨根洪：《试论制作、传播计算机病毒罪》，《华南师范大学学报（社科版）》1997 年第 4 期。
22. 陈开琦：《论计算机犯罪主体》，《贵州大学学报：社科版》1997 年第 2 期。
23. 胡国平：《关于四种计算机犯罪的认定》，《法律科学》1997 年第 4 期。
24. 曹士贞：《金融计算机犯罪的特点与对策》，《行政与法》1998 年第 3 期。
25. 黄丁全：《台湾地区电脑犯罪立法评析》，《中外法学》1998 年第 2 期。
26. 周仰虎：《论信用卡犯罪的立法完善》，《刑事法学》1996 年第 12 期。
27. 吕保江：《利用计算机挪用公款应引起注意》，《天津检察》1996 年第 1 期。
28. 李杰：《计算机病毒的危害与不可判定性》，《电脑报》1994 年 8 月 5 日第 3 版。
29. 杨博：《计算机犯罪问题的若干法律思考》，《法商研究》1995 年第 2 期。
30. 辛泉：《打击电脑犯罪的行动计划》，《中国科协报》1998 年 3 月 12 日第 3 版。
31. 韩振宇：《计算机病毒的一般原则》，《电脑报》1994 年

6 月 3 日第 3 版。
32. 韩振宇：《计算机病毒的定义与分析》，《电脑报》1994 年 5 月 27 日第 3 版。
33. [日] 神山敏雄：《使用计算机的欺诈罪》，《现代外国哲学社会科学文摘》1997 年第 1 期。
34. [俄] 拉特波夫：《因特网——革命》，《现代外国哲学社会科学文摘》1998 年第 9 期。
35. [美] 加尔金：《有关计算机及网络的若干案例》，《现代外国哲学社会科学文摘》1998 年第 6 期。
36. [美] 吉伯尔特：《打击侵犯电子计算机版权》，《现代外国哲学社会科学文摘》1997 年第 7 期。
37. [美] 吉恩·史蒂芬斯：《计算机网络空间犯罪面面观》，《编译参考》1997 年第 1 期。
38. [美] 阿兰德：《网络空间的安全与隐私问题》，《现代外国哲学社会科学文摘》1998 年第 2 期。
39. [美] 施拉格：《计算机的实际问题》，《现代外国哲学社会科学文摘》1998 年第 6 期。
40. 管高岳：《电脑犯罪》，《台、港、澳及海外法学》1996 第 7 期。
41. 蔡惠芳：《电脑犯罪和刑事立法的课题》，《台、港、澳及海外法学》1995 年第 12 期。
42. 黄三荣：《论网际网路服务业及其所面临的法律问题》，《台、港、澳及海外法学》1997 年第 4 期。
43. 陈家骏：《网路传播媒体适用现行法律规范之探讨》，《台、港、澳及海外法学》1997 年第 9 期。
44. 陈家骏：《资讯高速公路与科技著作权》，《台、港、澳及海外法学》1996 年第 5 期。
45. 黄朝晖：《谈谈信息的保护》，《台、港、澳及海外法学》1996 年第 l 期。

46. 洪荣彬：《论资讯时代跨越国境之资料处理与资料保护》，《台、港、澳及海外法学》1996 年第 1 期。
47. 陈聪明：《盗用自动提款卡之刑事责任》，台湾《法令月刊》第 42 期，第 497 页。
48. 黄荣坚：《电脑犯罪的刑法问题》，台湾《法学论丛》第 25 期。
49. 林永谋：《电脑犯罪与刑事立法》，台湾《法令月刊》第 41 期，第 596 页。
50. 刘静怡：《电脑网路上之智慧财产权保护问题》，台湾《月旦法学》1997 年第 1 期。
51. 刘静怡：《电脑网路世界之新兴言论自由议题：资讯时代的法律与科技》，台湾《月旦法学》1997 年第 6 期。
52. Benjamin. Wright & Jane. Winn, The Law of Electronic Commerce, N.Y., Aspen Law & Business, 1998.
53. Bernard. Reams, Electronic Contracting Law and EDI Business Transaction, 1997.
54. Jay S. Albanese, White-Collar Crime in America, Prentice Hall, Englewood Cliffs, New Jersey 07632, 1995.
55. 联合国国际贸易法律委员会《电子商务示范法》(UNCITRAL Model Law on Electronic Commerce), http://www.un.or.at/uncitral/.

后　记

本书是在我的同名博士学位论文的基础上扩充、修改形成的，在刑法学基金的资助和武汉大学出版社的大力支持下，终于得以付梓。

我是半路出家来学习、研究刑法学的，这既是机遇所铸，也是母校武汉大学及其教师们培养的结果：1991 年我考入武汉大学原无线电电子学系时，武汉大学已经实行学分制和主辅修制，我在学习本专业课程的同时，有意识地学习了一些法律课程，这些知识使我在本科毕业后，得以顺利考取律师资格，1995 年我考入中山大学电子学系攻读硕士学位，研究计算机图像传输与处理，一次偶然机会，我认识了导师赵廷光教授，了解到赵教授刚刚开设计算机犯罪及法律对策研究方向，招收博士研究生，其后两年时间里在赵教授的指导下，我全面学习刑法学课程，并于 1998 年报考并顺利考上了武汉大学刑法学博士研究生。进入武汉大学后，赵教授安排我重新学习刑法学，听刑法学硕士研究生的课程，在家里给我个别讲课，同时，指导我进行计算机犯罪问题的研究，我则如虔诚的修道士，陶醉于乐趣无穷的学习中。珞珈山麓黄装绿装替换了三次，三年的学习转眼结束，我圆满地完成了学业，顺利通过博士学位论文答辩并获得法学博士学位。

以上个人的成功不仅有个人的艰苦努力，还与导师赵廷光教授、武汉大学刑法教研室的其他老师的关怀和悉心教导分不开，我要深深地感谢帮助我的人们：

感谢恩师赵廷光教授和师母对我的诸多方面的关心和帮助。

赵教授引导我走上刑法学研究的道路，指导我探索计算机犯罪领域问题，给我教益颇多。赵教授为人刚正，品德高尚，知识广博，治学严谨、务实、创新，其人品学问是我修身、治学的榜样。

感谢德高望重、造诣精深的马克昌先生，先生谆谆教诲，正我为人，惠我学业，学生永志不忘。感谢喻伟教授、刘明祥教授、莫洪宪教授、李希慧教授、林亚刚教授、康均心副教授，感谢他们给我学业以关心、帮助和指导。再次感谢武汉大学刑法教研室各位老师对我的关怀、教导和栽培。

本书的付梓，离不开马克昌先生的极力推荐和武汉大学出版社郭园园老师的支持，这里要再次致以衷心的感谢。武汉大学出版社第一编辑室各位编辑为本书的出版倾注了大量的心血，没有他们的辛勤工作，本书不可能与读者见面，这里致以衷心的感谢。

感谢武汉大学刑法学博士张正新、但伟、朱华池、金泽刚、李邦友、鲜铁可、郭园园、唐若愚、刘金林、陈岚、黄开诚、陈正沓、李兰英、赵文胜、徐振华、于跃江、聂立泽、郭立新、黄明儒、童德华等，感谢他们给我学业上的诸多帮助。

感谢武汉大学法学院资料室的各位老师，感谢她们为我学业和论文的完成所提供的帮助。

谨以此书献给我的母校——武汉大学。

皮　勇

2002 年 1 月于武汉大学珞珈山