计算机犯罪问题的调查分析与防范

夏锦尧 主编

中国人民公安大学出版社

JISUANJI FANZUI WENTI DE DIAOCHA FENXI YU FANGFAN

计算机犯罪问题的调查分析与防范

主　编： 夏锦尧
副主编： 马君显
撰稿人：（以姓氏笔画为序）
马君显　罗仁东
夏锦尧　魏　中

中国人民公安大学出版社
·北　京·

图书在版编目(CIP)数据

计算机犯罪问题的调查分析与防范/夏锦尧主编.—北京:中国人民公安大学出版社,2001.4
ISBN 7-81059-646-2

Ⅰ.计… Ⅱ.夏… Ⅲ.计算机犯罪-研究 Ⅳ.D917

中国版本图书馆 CIP 数据核字(2001)第 17156 号

计算机犯罪问题的调查分析与防范

JISUANJI FANZUI WENTI DE
DIAOCHA FENXI YU FANGFAN

夏锦尧 主编

出版发行:中国人民公安大学出版社
地　　址:北京市西城区木樨地南里
邮政编码:100038
印　　刷:北京牛山世兴印刷厂

版　　次:2001 年 4 月第 1 版
印　　次:2001 年 4 月第 1 次
印　　张:13
开　　本:787 毫米×1092 毫米　1/16
字　　数:303 千字
印　　数:0001-3000 册

ISBN 7-81059-646-2/D·526
定　　价:28.00 元

本社图书出现印装质量问题,由发行部负责调换
联系电话:(010)83905728

E-mail:cpep@public.bta.net.cn

序言

二十一世纪是信息世纪，也是计算机犯罪更为多发的世纪，对现有计算机犯罪进行深刻的调查分析，必将对日益增加的计算机犯罪的防范和打击，产生重要的作用。

我和中国计算机安全专业委员会的同道们，多年来急切盼望中国有机编著的有关计算机犯罪的专著。夏伟亮教授的这本书正是我们盼望的，它收集了大量中外已发生的计算机犯罪案件，对这类案件的外在形状，特点，立案，侦查，以律判据各方面进行了详尽分析，其素材翔实丰富，论证的精辟令我十分兴奋，特为之序。

夏伟亮教授是中国公安战线的老战士，长期从事技术侦察和培训教育工作，从1996年起顺应趋势，转为研究计算机犯罪，凭借其深厚的功力，编写了本书。我相信此书受到业界和社会各界热烈关注，将是防范和打击计算机犯罪的重要参考书。

[illegible]

[illegible]月

编者的话

计算机犯罪是利用暴力和非暴力形式，故意泄露或破坏系统中的机密信息，以及危害系统实体和信息安全的不法行为。暴力形式是对计算机设备和设施进行物理破坏，如使用武器摧毁计算机设备，炸毁计算机中心建筑等。而非暴力形式是利用计算机技术知识及其他技术而进行的犯罪活动。

世界计算机犯罪活动始于60年代末，70年代迅速增长，80年代形成威胁。随着计算机应用的日趋广泛和社会化，国际上正掀起计算机犯罪的浪潮。据伦敦举行的“1996年信息安全博览会”提供的数据，全球1995年因计算机犯罪造成的损失达150亿美元。据有关部门的资料表明，美国每年计算机犯罪发案率增长400%，英国每年计算机犯罪增长率为213%。

近年来，随着中国现代化的发展，国际互联网的形成，振兴了经济，促进了国际间的交流，随之而来的计算机犯罪问题，也日趋突出。据中国公安部门统计资料表明，1988年至1989年仅发生计算机犯罪案件9起，1989年至1990年发生计算机犯罪案件上百起，1993年计算机犯罪案件为1000多起，1994年为1450多起，90年代后期，计算机犯罪的发案率成直线上升趋势。

以计算机犯罪为代表的高科技犯罪，已成为发达国家和发展中国家的重大社会问题。

计算机犯罪案件不仅范围广，涉及经济、政治及社会各个领域，而且技术含量高，侦破难度大。为了使公、检、法、司机关的工作人员及计算机的从业人员对计算机犯罪有较系统的了解，我们在对计算机犯罪有关问题的调查与分析的基础上，编写了本书，期望能引起全社会的重视，广泛开展对计算机犯罪的研究，加强对计算机犯罪的防范，以适应21世纪我们所面临的挑战。

本书的第一—四、六章，由夏锦尧撰写，其中金融系统的计算机犯罪的技术部分由罗仁东撰写，部分案例由魏中撰写；第七、八章由马君显撰写。

在编写本书的过程中，得到了许多专家和同行的帮助和支持。中国计算机安全专业委员会主任缪道期教授百忙中审阅了全书，并作序；本书中第五章计算机犯罪证据及第六章的部分内容，在征得中国政法大学马秋枫主任同意下，采用了由他主编的《计算机信息网络的法律问题》一书中的第十一章的主要内容；本书中许多有关计算机安全的法律、法规等内容考虑到其权威性，采用公安部十一局1998年编写的计算机信息安全系统培训教材中的主要内容；中国人民公安大学蒋占卿、张峰、孙伟、沈伟峰等同志帮助收集了许多资料及给予技术上的帮助；出版社的领导和编辑也给了大力支持，在此表示衷心的感谢。

由于编者水平有限，资料（尤其是案例资料）收集不完整，难免有错误和不足之处，谨请指正。

目　录

第一章　计算机犯罪的概念和定义

随着计算机技术的迅猛发展和广泛应用，计算机犯罪的类型和领域不断地增加和扩展。虽然“计算机犯罪”已经成为国际社会普遍使用的一个惯用词，但是关于计算机犯罪的概念和定义，世界各国学术界、司法界认识不尽一致，因而，国际上尚未对“计算机犯罪”形成一个公认的定义。其法律界定也有差异。

第一节　国际上有代表性的观点

一、美国的观点

美国是世界上计算机技术最发达的国家之一，对计算机犯罪早有研究。美国佛罗里达州于1978年，通过了第一个有关计算机犯罪法。到1987年，美国又有48个州相继立法；1984年12月，美国联邦出台了《非法使用电脑设备、电脑诈骗及盗用法》；1987年由国会通过，1988年开始实施《1987年计算机安全法》；1995年1月，美国商务部议定了《全球信息设施（C11）合作协议书》，以确保个人的隐私或组织的机密得到保护，确保网络及信息安全可靠性得到保护，确保有关知识产权得到保护；1998年，美国参议院通过了一项《关闭美国所有因特网上赌博场所》的决议，并对参赌者和经营者作出了处罚规定。另据资料介绍，在美国议会的第105号立法备案卷宗袋中，有关因特网的法律条例已陡增到300项。近年来，还有50余件有关因特网立法的新法案又摆到了美国国会面前。这50余件法案涵盖了网络税收、电子商务、网上赌博、网上个人隐私权、网上版权、黄色站点以及垃圾邮件等方面。但是关于“计算机犯罪”的概念和定义，也有不尽相同的观点与看法。

（一）美国司法部把计算机犯罪定义为：“在导致成功起诉的非法行为中计算机技术和知识起了基本作用的非法行为。”这种定义只把计算机犯罪解释为纯技术性的犯罪，混淆了违法与犯罪的界限，并没有包括计算机犯罪的全部含义。

（二）美国斯坦福研究所国际著名的计算机安全专家唐·帕克认为：计算机犯罪的概念应包括三个部分：

1. 计算机滥用。

即含有计算机的任何故意行为。在这一行为中，受害遭受到或可能遭受到损失，犯罪行为人得到或可能得到好处。

2. 计算机犯罪。

指在实施犯罪的过程中直接涉及到计算机。

3. 与计算机有关的犯罪。

在成功起诉的非法行为方面犯罪的特征中指出，计算机犯罪由这三方面组成。由于具有和计算机相关这一共性，因而成为计算机犯罪。这一观点的缺陷是从不同的角度描述计算机犯罪，难免会有交叉重叠，从而使得对于计算机犯罪在三个方面的认识存在模糊。

（三）其他的一些观点和规定：在美国政府进行的一项研究中，总会计学办公室调查了联邦政府中计算机犯罪的程度。它用的是“与计算机有关的犯罪”这一术语，并定义为：故意对政府或个体的私人利益造成损失的行为，这些行为与被实施时所在之系统的设计、使用或操作有关。

1984 年 6 月，美国律师协会刑事司法处公布了它的工作组调查，题为“计算机犯罪报告”，认为计算机犯罪是一种现象，而不是一个具体行为。这一广义定义是比较切合实际的，因为它将概念分成两个部分：一是计算机是犯罪的工具；另一是计算机是犯罪的受害者。

美国联邦计算机犯罪法（《计算机诈骗和滥用法》，Computer Fraud And abuse Act）规定，具有以下犯罪行为的，分别处以罚款或者十年以下监禁和五年以下监禁：

1. 未经授权或越权访问计算机，并以此手段获取属于美国政府为国防或外交关系的利益防止非法泄露予以保护的信息，或者 1954 年原子能法第十一章规定的数据，而且有理由认为获取这类信息并加以利用，会损害美国利益或有利于他国利益。

2. 闯入计算机系统获取金融机构、信用卡发行机构或包括顾客信用报告的文件中有关财务记录信息。正当信用报告法对此作了规定。

3. 未经允许或越权闯入由政府控制或会影响政府应用的计算机系统。

4. 闯入与联邦利益有关的计算机系统，并企图诈骗获取任何除应用此计算机以外的有价值的东西。

5. 未经授权，故意访问涉及联邦利益的计算机，并有一个以上例子说明有更改、损害、毁灭这种计算机中的信息，或者阻碍对这种计算机或信息的合法使用，以致：

（1）在任何一年期间总计造成损失 1000 美元；

（2）篡改或损害医疗检查、诊断、治疗、保健数据。

6. 故意和有预谋地对美国州际、外贸或者政府用或用于政府的计算机口令进行诈骗。

二、其他一些国家的观点

（一）对计算机犯罪，欧洲经济合作与发展组织定义为：“在自动数据处理过程中，任何非法的，违反职业道德的，未批准的行为都是计算机犯罪行为。”该定义的优点在于揭示出计算机犯罪和计算机知识起了基本作用。本定义应该说是展示了计算机犯罪行为与计算机相关的计算机系统的自动数据处理功能之间的内在联系。但将“违反职业道德的，未经批准的行为”均视为犯罪，与犯罪需要是不法行为达到一定危害性依刑事法律规定应受惩罚的行为不符，有过于扩大打击面之嫌。

（二）瑞典从司法角度在其数据法中，对计算机犯罪作了很有限的定义：侵犯个人隐私的行为为计算机犯罪。如未经允许保存计算机私人文档；有关侵犯受保护数据的行为，如非法存取电子数据记录或非法修改、消除、录入这种记录，或准确侵犯数据等。这种定义没有包括数据诈骗的全部内容，更不包括对计算机信息系统破坏等犯罪行为。

（三）比较有代表性的观点，是联邦德国的观点。原西德于 1977 年就开始修改刑法，

增加了有关计算机犯罪的条款，调整了相应的罚则，加强了对计算机安全的刑事保护；1985年5月15日颁布了《经济犯罪防治法》，对刑法内容又作了系统修改，专门有关于计算机立法的规定；1997年8月又通过了《德国多媒体法》，1997年12月30日德国公布了《计算机信息网络国际安全保护管理办法》。联邦德国有人认为：计算机犯罪是针对计算机或把计算机作为犯罪工具的任何犯罪行为。如原联邦德国的犯罪学专家汉斯·约阿希姆·施奈德在其著作“犯罪学”一书中，将计算机犯罪定义为：利用电子数据处理设备作为作案对象的犯罪行为。它有四种表现形式：

1. 窜改输入数据或改变数据和数据程序；

2. 计算机间谍；

3. 破坏计算机；

4. 偷用计算机和计算机时间。

（四）澳大利亚有人把计算机犯罪称为计算机滥用，并把计算机犯罪行为解释为与计算机有关的盗窃、贪污、诈骗、破坏行为。计算机滥用行为包括：

1. 未经批准修改输入或输出数据；

2. 未经批准通过终端访问计算机系统；

3. 未经批准修改或使用应用程序；

4. 对电子数据处理设备实施犯罪：盗窃设备、文件或数据；

5. 破坏计算机设备；

6. 未经批准进行数据截收。

该定义用“滥用”一词来表达计算机犯罪的全部含义，显然是不妥当的。它没有表述出计算机在计算机犯罪中所处的重要地位和作用。

（五）加拿大在刑法中，把计算机犯罪规定为非法使用电脑系统或损坏资料的行为。加拿大于1985年12月12日通过的刑法修正案，规定了非法使用电脑系统或损坏资料为犯罪行为。具体包括：

1. 非法取得电脑服务；

2. 截取系统功能；

3. 借用电脑取得利益；

4. 故意损毁、修改数据或干扰电信资料的合法使用等。

第二节　中国的观点

在中国国内，对计算机犯罪的定义也有许多不同的表述与看法。

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

中国政法大学信息技术立法课题组从学术角度对计算机犯罪所下的定义是：“与计算机相关的危害社会并应当处以刑罚的行为。”该定义用“相关”一词，来包括所有的各种计算机犯罪，没有把计算机在计算机犯罪中的地位表达出来。

比较有代表性的观点有：

一、公安部计算机安全监察司提出的观点

1991 年，公安部计算机安全监察司提出的定义是："以计算机为工具或以计算机资产为对象实施的犯罪行为。"并进一步解释说："这里所说的工具是指计算机信息系统（包括大、中、小、微型系统），也包括在犯罪进程中计算机技术知识所起的作用和非技术知识的犯罪行为。犯罪一词中包含了危害社会和应处以刑罚的含义。"这一定义可以说是比较完整的定义。它避免了纯技术性、片面性，还对计算机在计算机犯罪中所处的地位和作用进行了简单表述，并且通过定义后的解释，对"犯罪"一词的基本含义作了说明。

二、清华的观点

1991 年 11 月 13 日，郭清华在《计算机世界》上载文"计算机犯罪概念初探"，他在评论了中国国内外关于计算机犯罪概念的论述后认为：

要想正确地把握计算机犯罪这一概念，必须明确其内涵和外延。作为一种独立的刑事犯罪类型，计算机犯罪至少应有以下本质属性：

（一）它应是一种犯罪行为，即应是危害社会、触犯刑律、应受刑罚的行为。只有符合刑法的理论关于犯罪的定义，具备犯罪的基本特征的行为，才能称其为计算机犯罪；凡是不符合刑法理论关于犯罪的定义，不具备犯罪的基本特征的行为，自然不是计算机犯罪。这是一个大的前提，是计算机犯罪和那些与计算机有关的非法行为或者不道德行为的区别所在。

（二）它应是危害计算机安全的行为。计算机安全是指计算机资产安全，即计算机系统资源和计算机信息资源不受危害，处于正常工作或者自然存在的状态，是刑法所保护的一种社会关系。形形色色的计算机犯罪不论其犯罪行为的具体表现形式如何不同，不论其侵害的对象如何不同，也不论其危害结果如何不同，共同的一点就是这些犯罪行为侵害的客体是相同的，即计算机安全。就是说任何计算机犯罪行为最终侵害的都是计算机系统资源和计算机信息资源，导致其不能正常工作或自然存在，危害了计算机安全。这是计算机犯罪与其他各种类型刑事犯罪的本质区别。是它能够作为一种犯罪类型独立存在的根本原因。例如：同是以侵财为目的的计算机诈骗罪和一般诈骗罪，计算机贪污罪和一般贪污罪，盗窃计算机资产罪和一般盗窃罪等，相互之间的区别就是因为二者所侵犯的客体不同，前者侵害的客体是计算机安全，后者侵害的客体是公私财产所有权。

（三）它应是刑事责任主体故意实施的行为。危害计算机安全的情况包括计算机犯罪和计算机安全事故两种。这一点指明了计算机犯罪的主体和主观要件，是计算机犯罪与计算机安全事故的区别所在。刑事责任主体是达到刑事责任年龄、具有刑事责任能力的自然人。计算机犯罪是刑事责任主体实施的，是人为地危害计算机安全，这是计算机犯罪与自然因素引起的计算机安全事故的区别。故意是指行为人明知其行为会发生危害社会的结果，并且希望或者放任这种结果发生。人为因素引起的计算机安全事故，其行为人在主观上不是出于故意而是由于过失造成了危害计算机安全的事故，这是计算机犯罪与人为因素引起的计算机安全事故的区别。

（四）它应是以计算机为工具或者以计算机资产为对象实施的行为。这是由各种具体

形态的计算机犯罪中抽象出来的计算机犯罪的客观要件。就目前出现的计算机犯罪来分析，在客观方面主要表现为以下几种行为方式：

1. 向计算机信息系统装入欺骗性数据或记录；

2. 未经批准使用计算机信息系统资源；

3. 篡改或窃取信息或文件；

4. 盗窃或诈骗系统中的钱财；

5. 破坏计算机资产。

其中前两种方式可以归结为以计算机为工具的行为，后三种方式可以归结为以计算机资产为对象的行为。可以说无论是现存的以上五种形式之内的计算机犯罪，还是将来可能出现的新型计算机犯罪，在客观上必定表现为两种情形，或者是以计算机为工具，或者是以计算机资产为对象，概莫能外。明确了这一点，也就正确地把握了计算机犯罪的基本特征，可以对各种形式的计算机犯罪有一个层次的认识。

计算机犯罪概念的外延是指一切形式的计算机犯罪。计算机犯罪是一种非常纷繁复杂的事物，从不同的角度分析可以有各种不同的犯罪形式。从犯罪人员上看，既有计算机技术人员，也有非计算机技术人员。从犯罪手段上看，既有使用技术手段的，也有使用暴力手段或其他非暴力手段的。从犯罪对象上看，既有以计算机资产为对象的，也有不以计算机资产为对象的。从犯罪目的上看，既有侵财性的，也有政治性的、发泄性的。从犯罪方式上看，既有贪污、诈骗、敲诈等形式的，也有盗窃、掠夺、破坏等形式的。作为一个科学的计算机犯罪概念必须将以上各种形式的计算机犯罪都概括在内。相反的，如果一个计算机犯罪概念只包括以上数项内容的两个方面中的一个方面，而不包括另外一个方面，都会是不全面的，甚至是错误的。

综上所述，郭清华认为，既能准确地表达计算机犯罪的内涵，恰当地界定计算机犯罪的外延，又能深刻地揭示计算机犯罪的本质属性的基本特征，说明计算机犯罪作为一种犯罪类型独立存在价值的计算机犯罪概念，可作如下表述：

计算机犯罪是刑事责任主体以计算机为工具或者以计算机资产为对象故意实施的危害计算机安全的犯罪行为。

这一概念由五个要素构成，分别是基本属性（犯罪行为）、犯罪主体（刑事责任主体）、犯罪客体（计算机安全）、犯罪的主观方面（故意）、犯罪的客观方面（以计算机为工具或以计算机资产为对象）。其中最关键的要素有二：其一是指出计算机犯罪是以计算机为工具或者以计算机资产为对象实施的行为，概括了计算机犯罪的基本特征，阐明了计算机犯罪的客观要件。其二是指出计算机犯罪是危害计算机安全的行为。这是对计算机犯罪所侵害的社会关系的精确概括，揭示了计算机犯罪的本质属性，说明了计算机犯罪作为一种类型犯罪独立存在的价值。犯罪客体这一点是计算机犯罪概念的核心。

三、中国政法大学的观点

根据马秋枫等的研究课题《计算机信息网络的法律问题》（1998 年 2 月）的观点认为：计算机犯罪可以定义为：计算机犯罪是针对计算机信息系统或利用计算机特性具有社会危害性并达到应受刑罚处罚程度的行为。他们从计算机、电信技术与计算机犯罪的产生和发展的关系的历史考察出发，基于以下基本结论而得出以上定义的：

（一）现代社会已步入信息社会。中国虽是发展中国家，但信息技术的发展表现出层次性特征，即不同的领域，不同的地区信息自动化的程度是不同的。在某些地区、某些领域中计算机信息技术的运用是很普遍和深入的。

（二）计算机及信息网络是信息社会的基础，由于计算机及信息网络处理、存储、传输、转换着社会所必需的各种信息，所以一旦某个环节出了问题，依赖于计算机的社会的正常运行就会处于混乱状态，从而造成巨大的经济损失。信息社会的这种高度脆弱性要求计算机系统的高度秩序。这种秩序虽不如传统犯罪，如“打砸抢”犯罪破坏正常的社会秩序那样显而易见，但一旦它被犯罪所侵犯，它所造成的物质损害、精神和心理上的损失远非“打砸抢”犯罪可比。例如：倘若在医院或银行的计算机系统中投放计算机病毒，则在短时间内即可造成医院或银行的数据混乱或丢失，从而给医护中的病人或储户的利益带来怎样的混乱可想而知。更为严重的是，会损害人们对计算机系统的信心。这是经济尺度不易衡量的。因此，信息社会对计算机信息的完整性和保密性，可用性以及系统功能正常发挥的高度要求不容忽视。

（三）计算机犯罪的核心应当是针对计算机信息系统的犯罪。由于其对信息秩序的潜在的或现实的危害性，会对社会有质和量上传统犯罪无法比拟的严重危害性，我们必须视其为犯罪，从犯罪学方面研究其对策，并在刑事法律方面寻找对策以最大限度地制止该类犯罪。

（四）计算机犯罪还应当包括利用计算机知识的犯罪或以计算机为工具的犯罪。我们认为利用计算机知识的犯罪涵盖的范围较之以计算机为工具的犯罪要广。利用计算机知识的犯罪基本上还包括以计算机为对象的犯罪。由于在实际的犯罪中，以计算机为对象的犯罪和以计算机为工具的犯罪经常表现在手段和结果上的牵连关系，因此，为了分类上的明确、简洁，把利用计算机犯罪作狭义的理解，与以计算机为工具的犯罪都同时指通过计算机知识或以计算机为手段触犯了传统刑法的犯罪，以区别于针对计算机信息系统的犯罪。我们认为，可以称该犯罪为滥用计算机。该类犯罪由于计算机技术的应用，在犯罪的速度、广度和深度上都有区别于传统之处，并且侦查，起诉和审判的策略也有所不同。因此，也应该成为计算机犯罪的研究范畴。值得注意的是，滥用计算机犯罪这种形态不宜把范围搞得太广，它的犯罪行为必须是利用计算机知识和以计算机为工具。只有不利用计算机就无法轻易达到犯罪目的的犯罪，才有必要在计算机犯罪领域加以特别的研究。

（五）1994 年 2 月 18 日发布的《中华人民共和国计算机信息系统安全保护条例》，作为中国颁布的关于计算机信息系统安全保护的第一部专门法规，第七条规定：“任何组织或个人，不得利用计算机信息系统从事危害国家利益、集体利益和公民合法利益的活动，不得危害计算机信息系统的安全。”这就表明凡把计算机信息系统作为工具，危害了国家利益，集体利益和公民合法利益；或者有意危害计算机信息系统安全的行为就是计算机违法行为。并且该法规确认了信息资源是国家重要资源，计算机信息系统安全是社会公共安全的一部分。因此，我们在研究计算机犯罪，尤其是制定计算机犯罪刑事法律规范时，应当以该法规体现出的国家意志为依据。

第三节　中国刑法的有关规定

在中国新刑法中，虽然没有“计算机犯罪”的明确定义，但有关计算机犯罪的专门条款已规定在《妨害社会管理秩序罪—扰乱公共秩序罪》中。包括：

第二百八十五条规定的非法侵入计算机信息系统罪；

第二百八十六条规定的破坏计算机信息系统罪；

第二百八十七条规定的以计算机为工具实施的犯罪。

一、刑法规定的具体条款

新的刑法规定的具体条款为：

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

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

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程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。

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

二、理解刑法规定条款应注意的几个问题

《刑法》规定的以上条款，规定了关于计算机犯罪的罪名和处刑幅度，在理解和操作时必须注意以下几个问题：

（一）关于“违反国家规定”及“计算机信息系统”问题

《刑法》第二百八十五条、第二百八十六条中所指的“违反国家规定”，在《刑法》第九十六条作了明确的规定，即“违反全国人民代表大会及其常务委员会制定的法律和决定，国务院制定的行政法规、规定的行政措施、发布的决定和命令”。

关于计算机信息系统方面的国家规定有三件：

1994 年 2 月 18 日国务院颁布的《中华人民共和国计算机信息系统安全保护条例》（简称《条例》）

1996 年 2 月 1 日国务院颁布的《中华人民共和国计算机信息网络国际联网管理暂行规定》（简称《规定》）

1997 年 12 月 8 日国务院颁布的《中华人民共和国计算机信息网络国际联网暂行规定实施办法》（简称《办法》）

所谓的“计算机信息系统”，根据《条例》第二条规定：“是指由计算机及其相关的和配套的设备、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。”第四条规定：“计算机信息系统的安全保护工作，重点维护国家事务、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。”第五条规定：“中华人民共和国境内的计算机信息系统的安全保护，适用本条例。未联网的微型计算机的安全保护办法，另行制定。”因此，在适用刑法专用条款时，应把握以下几点：

1. 人机系统与原始系统的区别。

信息系统是由信息组成的有秩序的、自成体系的一个统一体。而所谓的计算机信息系统，即由计算机作为信息载体的系统。比如，一台计算机出厂时，只要已安装程序文件或应用软件，并具有信息处理功能，即构成计算机信息系统。但由于没有投入使用，没有“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”，因而不能称为“人机系统”，其信息安全不受《条例》保护，更不受刑法保护。

2. 网络系统与单机系统的区别。

人机系统既可以是网络系统，也可以是单机系统。但《条例》规定，“未联网的微型计算机的安全保护办法另行制定”。因此，刑法专款涉及到的犯罪客体应重点指已实施联网的计算机信息系统。

3. 重要系统和一般系统的区别。

《条例》规定：受保护的重点是国家事务、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。因此，在适用《刑法》时应注意将上述系统与一般性的涉及地区、部门或局部的系统区分开来。《刑法》第二百八十五条进一步将计算机信息系统的性质限制为“国家事务”、“国防建设”和“尖端科学技术领域”。“国家事务”系统，应指涉及国家政治、经济、外交等重大事项的计算机信息系统，一般由国务院各部委牵头建设，比如“金”字工程。“国防建设”系统，是指由军事部门建设的、涉及国家安全和军事秘密的所有计算机信息系统。“尖端科学技术领域”系统，一般应指国务院、国家科委、国防科工委确定的居世界领先地位的科技项目。

《条例》第四条，是判定是否属于计算机信息系统安全重点保护单位的依据。这里列出了信息安全重点保护单位的基本类型：

党政首脑机关；

国防尖端企事业单位；

国家重要经济部门；

重要科研单位；

重要广播电视、邮电单位：

重要金融单位；

重要动力单位；

重要物资储备单位：

国家级、省级重点建设工程；

其他应当列为要害单位的。

4. 国内网络系统与国外网络系统的区别。

《条例》规定：“安全保护的对象是中华人民共和国境内的计算机信息系统”，诸如 Internet 国外计算机信息系统，由于中国尚未就此签订任何国际公约，因而如果发现中国公

民非授权进入该网进行功能、数据、程序破坏的，不应依据《刑法》追究刑事责任。

（二）关于犯罪的主体和主观方面问题

《刑法》第二百八十五条、第二百八十六条所指的犯罪主体皆为一般主体。从目前中国计算机信息系统安全管理的实际情况看，重要信息系统不但采取了较为先进的技术安全措施，而且制定了一整套安全管理制度，因而无意或过失进入重要信息系统，删除系统功能、数据、程序等事件，基本上不可能发生，此类案件一般都是故意犯罪。其中，第二百八十五条的含义是，只要是非授权（不论是窃取密码、口令，还是采用技术手段）进入“国家事务”、“国防建设”和“尖端科学技术领域”的信息系统都具有可罚性，都应立案定罪，其动机如何，造成的损失大小，产生的危害程度轻重，均不影响案件的构成。如进入上述系统后窃取国家秘密信息，因“窃取国家秘密罪”重于“非法侵入计算机信息系统罪”，应依据从重原则，按“窃取国家秘密罪”处罚。如果进入上述系统后对系统功能进行删除、修改、增加、干扰，造成系统不能正常运行，或对系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作的，应根据犯罪后果区别对待：若造成“严重后果的”，依据从重原则，按“破坏计算机信息系统罪”处罚；若未造成“严重后果的”，按“非法侵入计算机信息系统罪”处罚。

（三）关于“后果严重的”问题

谈“后果”，在刑法上一般指已遂犯罪。第二百八十六条三款明文规定，不论是哪一种行为，造成的影响必须是“后果严重的”；如果有犯罪动机、犯罪行为，但没有产生犯罪结果，或者不是“后果严重的”，一般不予定罪量刑。何为“后果严重的”？可从以下几方面考虑：

1. 经济损失情况：包括两个方面，即系统本身的经济损失和由此造成的直接经济损失，可参照有关罪名的立案标准，确定数额等次，从而界定“后果严重的”和“后果特别严重的”。

2. 系统受损坏的程度：如果系统瘫痪，不能正常运行，当属“后果严重的”；如果瘫痪时间较长，一段时间无法恢复工作，当属“后果特别严重的”。

3. 工作受影响的程度：即使系统没有瘫痪，但因某项功能受到损害，使正常工作受到影响，作为“后果严重”的标准。

此外，对于公务员或从事信息服务业的职员、滥用职权的系统管理员、程序员、操作员，由于他们具备操作计算机的条件，并具有计算机知识和技术，犯罪后有条件逃避侦查、起诉，造成破坏的可能性也较大，又利用职务之便，知法犯法，因而应与一般的犯罪嫌疑人有所区别。

（四）关于利用计算机作为手段的犯罪问题

《刑法》第二百八十七条指的都是利用计算机为手段的犯罪，最终侵害的是中国刑法保护的传统社会关系，根据刑法的手段和目的、过程和结果的牵连关系的处理原则，应依照刑法有关规定定罪处罚。此条体现了中国刑法的量刑依据，即根据犯罪的事实、犯罪的性质、情节和对于社会的危害程度，使用的手段不作特别强调。但需要注意的是，如果犯罪嫌疑人利用计算机信息系统进行诸如盗窃、挪用资金等传统犯罪，因其他原因未产生犯罪结果，按传统罪名可能处罚较轻或不予处罚时，可依据扰乱计算机信息安全秩序管理的某种罪名予以处罚：

1. 如侵入第二百八十五条所保护的信息系统，盗窃、挪用等犯罪未遂，又未进行系统破坏，可按“非法侵入计算机信息系统罪”处罚。

2. 如侵入第二百八十六条所保护的信息系统，盗窃、挪用等犯罪未遂，但对系统实施了破坏，并产生“严重后果的”，可按“破坏计算机信息系统罪”处罚。

中国新《刑法》补充了计算机犯罪条款，标志着中国信息社会安全保护向规范化、法制化、科学化迈上了一个新的台阶。也从安全保护的角度，确认了计算机信息系统的应用发展在中国发展前进中的重大作用，反映了并预示着中国计算机信息系统应用发展的蓬勃局面，以及计算机信息系统安全保护的重要地位。

在新《刑法》中，所列入的有关计算机犯罪的内容有：危害公共秩序罪，妨害社会管理秩序罪，扰乱公共秩序罪，非法侵入国家重要计算机信息系统罪，故意破坏计算机信息系统功能罪，故意破坏计算机信息系统数据、应用程序罪，故意制作、传播破坏性程序罪，传授犯罪方法罪，破坏通信设备罪，利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家机密等犯罪。

随着中国新《刑法》的实施和中国法制建设的不断健全，必将对计算机犯罪提出一个科学的定义。

综观国内外提出的有关计算机犯罪的定义，按其提出的顺序，大体可分为两个阶段：第一阶段是计算机应用于社会的初期，由于应用领域的局限性，计算机犯罪所侵害的往往是单一权益，如财产权或个人隐私权，从这个角度给计算机犯罪所下的定义，往往没有包括计算机犯罪的全部含义。第二阶段，随着计算机普及到社会各个领域，计算机犯罪可能侵犯到法律所保护的各种权益，这时多根据行为人与计算机系统之间关系的认识来界定计算机犯罪，这类观点比较完整。

实际上，计算机犯罪是当代社会出现的一种新的犯罪形式，日益呈现出新的特点，很难形成较一致的看法，其定义尚在深入研究之中。随着计算机技术和应用实践的发展和检验，最终会有一个较统一的定义。