·信息法学·

美国计算机犯罪立法的发展与启示

张 琳 （南京农业大学信息科技学院 江苏南京 210095）

摘 要：计算机犯罪已严重危害了信息系统安全，各国政府也已认识到打击和惩罚计算机犯罪、保护信息系统安全的重要性。美国很早就将保护信息系统安全纳入了法治化的轨道，在打击计算机犯罪中也积累了丰富的经验。文章通过探讨美国计算机犯罪立法的历史沿革和最新发展，对信息系统安全的法治化进程中的规律进行总结，以期为我国的信息法制建设提供借鉴。

关键词：计算机犯罪 信息系统安全 立法 美国

中图分类号：TP393.08 文献标码：A 文章编号：1003-6938（2006）05-0089-04

Legislation on Computer Crimes in U. S. A.：Latest Development and Experiences

Zhang Lin （College of Information Science and Technology，Nanjing Agricultural University，Nanjing，Jiangsu，210095）

Abstract：Along with the rapid development of technology of network and information, computer crimes have become main killer to information system security. Awareness of the importance to punish computer crimes by the governments all over the world has bee increased. The United States is among the earliest countries which protect information system security with the legal measures, and become experienced in punishing computer crimes by the rule of law. This paper first briefly surveys the history and latest development of computer crime legislation in U.S., and then summarizes some experiences in the course of protection of information system security, which can serve as a model for China.

Key words：computer crime；information system security；legislation；The United states

CLC number：TP393.08 Document code：A Article ID：1003-6938（2006）05-0089-04

1 计算机犯罪的独特性与法律意义

对于什么是计算机犯罪，无论是理论界还是实务界均未形成一个普遍接受的定义。根据美国司法部的定义，任何一种违反刑法的行为，只要在其实施或对其侦查、起诉过程中涉及到计算机的知识与技术，均可称为计算机犯罪。这个定义显然过于宽泛，也模糊了计算机犯罪与一般犯罪的区别。美国学者卡太尔认为，可以从其表现形态的角度对计算机犯罪的概念进行界定。计算机犯罪有两种表现形式：一是使用计算机技术手段以计算机及信息系统为侵害对象的犯罪。它包括：（1）对计算机文档和程序的非授权进入；（2）在未经授权的情况下，对计算机文档和程序的破坏；（3）盗取电子身份识别号码。二是借助计算机技术手段实施的传统型犯罪，如在网络上广泛传播淫秽性的文字、图片、录音、录像或者进行保险欺诈等。计算机技术的使用，使这些传统类型的犯罪具有新的特点。[1] 卡太尔所说的这两种情况属于狭义的计算机犯罪，广义的计算机犯罪还包括其他涉及计算机的犯罪，如盗窃案中的犯罪分子对计算机设备或软

基金项目：南京农业大学青年科技创新基金“电子商务中信息安全问题研究”（项目号 KJ04021）的成果之一。

收稿日期：2005-11-03；责任编辑：王景发

件实物的窃取等。笔者认为，狭义的计算机犯罪体现了网络时代计算机信息系统安全的基本特点，应当成为信息安全法的主要规制对象。

不过，狭义的计算机犯罪概念既包含了以计算机信息系统为对象的犯罪，又包含了以计算机技术为手段的传统型犯罪，这给我们对计算机犯罪的认识带来了复杂性。因为，这关系到计算机犯罪是否能成为与传统犯罪相互独立的一种犯罪类型，是否应采取专门的法律来规范？对这个问题，人们的观点也不统一。持反对意见者认为，利用计算机在网络空间内实施的犯罪除了工具比较特殊外，与普通犯罪并无不同。几乎没有哪一个门类的法律是依据工具使用的独特性来划分。因此，计算机犯罪或网络犯罪并不值得给予特别的关注。美国第七巡回上诉法院的伊斯特布鲁克法官甚至以讥讽的口吻指出，如果我们因为这种工具的独特性而将计算机犯罪作为一种独立的犯罪类型，那么，是不是因为犯罪分子有时要将马作为交通手段，我们就要设立一门独立的“马法”呢？[2]美国学者奥利文鲍姆认为，技术性因素不应当得到过分的强调，通过现行的刑事法律进行必要的调整完全可以有效地惩治这种新型犯罪，没有必要进行单独的立法。[3]

更多的人赞成将计算机犯罪作为一种独特的犯罪类型，并用特别的法律规范来进行规制。他们认为，计算机犯罪在工具上的独特性使之无法归入普通的犯罪类别，比如侵入（未经授权进入）计算机系统的犯罪就是如此。它对法律提出的问题具有独特的性质，需要由一个新的法律类别来对之加以特别的调节。计算机技术本身的一些特点如运行上的无形性和高速性，活动范围上的广阔性，决定了计算机犯罪的独特性质，也决定了进行特别立法的必要性，即应当针对计算机犯罪制定单行刑法。

笔者认为，是否赞成将计算机犯罪作为一种独特的犯罪类型，并以特殊的法律来加以规范，其核心在于能否认识到由于网络信息时代信息系统及其安全保护的一些新的特点，使得犯罪分子无论是在使用的手段上还是侵害的社会利益上与传统的犯罪已经具有很大的区别，同时，也在于能否将信息系统的安全作为特殊的犯罪客体和法律来对待。从美国打击计算机犯罪的法律发展进程，我们可以清晰地看出这种态度的转变。

2　美国计算机犯罪立法的发展

直到20世纪80年代初期，美国法律界人士对信息安全的独特性尚未有足够的认识，刑事司法实践对计算机犯罪问题也并未给予特别的关注。对于一些利用计算机技术或以信息系统为对象的犯罪往往由检控机关根据案件的具体情况而将其归于传统的罪名，但根据传统的罪名和刑罚往往不能对计算机犯罪进行有效的打击。而与此同时，美国的计算机犯罪却以惊人的速度持续增长。1988年有记录的重大计算机安全事件仅有6项，到1999年则达到8000项；1995年仅是利用因特网实施盗窃的罪案就导致2亿美元的损失，进入21世纪，这个数字继续增长；一家公司在一年半的时间内就发现10万起针对其网站的非法活动；[4]目前，每天有10到15种新的病毒产生并向外传播，2000年“我爱你”病毒造成累计11亿美元的损失，同年针对美国国防部信息系统实施的攻击经确认的案例就有22,000件。[5]在汹涌的计算机犯罪浪潮面前，美国法律界人士感到通过法律手段予以回击的迫切性，同时也逐步认识到网络时代信息安全保护的独特性质，于是开始构建规范和保护信息安全的法律体系。在联邦层次上，涉及计算机犯罪的立法主要有《电子通讯隐私法》、《联邦计算机安全处罚条例》、《商业间谍法》等，而最重要的一部立法是《计算机欺诈与滥用法》（The Computer Fraud and Abuse Act，CFAA），这部法律自制定之日起，已历经了几次修订，其调整范围也不断扩大，为计算机犯罪立法提供了一个基本的框架，而20年来的频繁修订也反映了人们对计算机犯罪问题在认识上的不断深化。

这部法律在1984年最初制定时所涉及的罪名都属于故意犯罪，只涉及三个很窄的领域：（1）进入计算机系统以获取机密的国防或外交信息，危害本国或使某一外国获益；政府工作人员无意中对未经授权的文件的访问行为不属于犯罪，而故意超越授权则属于犯罪行为。（2）进入计算机系统以获取金融机构的金融信息或者从客户信息机构获取客户信息。触犯这一罪名必须以存在破坏的犯罪意图为构成要件，无意中接触此类信息不构成此罪。（3）修改、破坏或者透露某种信息，致使政府对该计算机系统的使用受到影响。它的构成应以进入行为影响到计算机系统的运作为要件。[6]立法对非法进入行为进行明确的界定，指明未经授权而进入某计算机系统，或者虽经授权，但却利用机会进入了超越授权的领域。

1984年这部立法颁布之后即招致许多批评：就第一类犯罪而言，与其他的相关法律相比，故意的要求显得过高。第二类犯罪对于金融信息的保护又显得过于狭窄，其一是所涉及的信息种类过窄，例如银行在其他机构中的存款信息以及贷款记录就不在保护范围之内；其二是它所保护的仅仅是个人利益而不涉及法人利益。第三类犯罪不仅要求控方证明系统信息已经遭到篡改、破坏或泄露，而且要求证

明这些行为确系影响到计算机系统的运作，难度较大。同时，在第二类犯罪和第三类犯罪中，如果一个人获得授权进入系统但却访问了授权范围以外的领域，这样的行为是否属于犯罪常常难以定性。

1986 年，美国国会对《计算机欺诈与滥用法》进行了修订，根据相应的批评进一步扩大了该法的调整范围，并增加了三项新的罪名：(1) 计算机欺诈罪。为了与《邮政通信欺诈法》区别，这一罪名要求以计算机作为其内在要素。仅仅是在实施欺诈时使用了计算机并不构成此罪。[7] (2) 篡改、毁坏数据或者阻止正常使用。这一罪名主要针对 :在年度之内导致 1000 美元以上的损失，或者篡改医疗记录的行为。[8] 由于这是一个重罪，因此设立了 1000 美元的门槛限制。不过，由于损失之中包含下列费用 :计算机使用时间、程序的重新调试、数据的恢复、网络通信费用、授权用户使用这些数据所损失的时间等，因此这一门槛限制很容易达到。如果篡改、毁坏数据或者阻止正常使用行为涉及医疗记录，则无需计算损失额。被侵害的对象——医疗记录本身就已经说明了行为的严重性，因而直接构成重罪。(3) 借助于任何一种密码以欺诈性交易为意图的进入。这一罪名涉及计算机密码，所要打击的是黑客们在公告栏上进行计算机密码交易的行为。[9] 主观上要求具有两个要求 :故意并且存在欺诈的意图。1988 年的修正案还将法律的调整范围扩大到所有的金融机构，且不限于信用卡事项。

在 1988 年的大规模修改之后，美国国会对于计算机犯罪始终给予了密切的关注，并根据现实的需要适时地对有关内容进行修改。1989 年的修正案将“ 银行 ”修改为“ 机构 ”，并明确指出，所谓“ 机构 ”是指其存款业务由联邦存贷保险公司提供担保的那些机构，从而进一步扩大了调整范围。1990 年又再一次对这一条中的“ 金融机构 ”的范围进行了扩展。1994 年的修正案则将故意行为与过失所导致的后果加以区分，分别规定在两个不同的条款之中，同时，将进一步明确了犯罪的行为类型：(1) 毁坏或可能毁坏计算机系统及部件；(2) 对合法使用计算机系统或其部件的阻挡、拒绝行为或者导致了这种阻挡、拒绝的行为，构成这一罪名还要求行为未能取得授权，其行为在某一年度之内导致 1000 美元的损失或者其篡改的对象是医疗记录。2000 年，这部法律经美国国会批准，编入 《美国法典》 第 18 卷第 1030 节。

通过若干次的修订，《计算机欺诈与滥用法》的规制范围越来越细密与合理，它除了规定了未经授权进入计算机系统而导致的刑事或民事责任之外，还专门界定了“ 超越授权进入 ”的概念，即虽经授权可以进入某计算机系统，但却非法获取了或者修改了进入者无权获得和修改的信息，这充分体现了计算机信息使用与处理的特点。同时，这部法律还是惩罚计算机病毒程序传播者的有力武器。它详细列举了各种故意传播计算机病毒程序、信息、命令导致受保护的计算机系统损害的情况，以及过失行为导致损害的情况，从而为打击和惩罚以计算机病毒程序危害信息安全的行为提供了明确的法律依据。1999 年，“ 美丽莎 ”病毒的编写和传播者戴维·史密斯就是依据该条规定而被判处了 20 个月的监禁。

3 信息系统安全法治化的启示与思考

3.1 明确将信息安全提升为刑法所保护的犯罪客体种类

如前所述，一开始美国法律界人士对信息安全的独特性尚未有足够的认识，在追诉和惩罚计算机犯罪时往往套用传统的罪名及相应的刑罚措施，如美国某些州的法律通过扩展现行立法中关于财产的概念，将存储于计算机系统和网络中的信息包容在内，这种方法初看起来对于处理计算机犯罪问题具有效率，也无须突破现行法律的基本框架，但是，对于计算机犯罪这种新型犯罪而言，传统的罪名和刑罚却时常并不那么奏效。如以计算机技术为手段实施的邮件欺诈罪、盗窃罪和非法侵入罪等在构成上通常要求具备两项要件 :一是侵害了一定的财产利益 ;二是产权人因此而丧失了他的财产。由于计算机使用权和存储在计算机系统中的数据具有财产上的价值，因此，非法侵用他人计算机或窃取他人计算机系统中的数据能够符合前一项条件，但问题是难以确定被害人是否丧失了其财产，以及何时丧失了他的财产。于是，适用于普通犯罪的刑法规则在调整计算机犯罪时就出现了不确定性。在这种情况下，法院就依据刑法解释的原则做出了有利于被告人的判决，传统的刑法在规制计算机犯罪就显得捉襟见肘了。

这种做法的缺陷在于没有将计算机信息系统安全作为独立而统一的犯罪客体来对待，从而导致了打击上的零散性和无效性。犯罪客体是犯罪主体的犯罪行为所侵害的、为刑法所保护的社会关系。犯罪客体是制定和适用刑法的根据，只有某种侵害社会利益行为的危害性到了一定程度才应该被刑法所规制，这种社会利益被表述为犯罪客体。对某一犯罪的犯罪客体没有正确认识，则会引起一系列问题。某犯罪的规定章节、刑罚幅度等都可能产生相对于整个刑法体系的不协调。[10] 计算机犯罪尽管也可能侵犯到一定的财产利益，但财产利益显然不能涵盖其独特性质的全部，这正是美国 20 世纪 80 年代以前通过传统刑法来打击计算机犯罪缺乏实效的重要原因之一。无论是从计算机及网络的发

展现状及其对社会生活的巨大影响来看，还是从计算机技术本身的特点来看，我们都有理由将计算机信息系统安全作为一种独立的犯罪客体来对待，从而为有关罪名及刑罚的设置提供理论前提。对于计算机或网络信息而言，其安全性问题主要包括四个方面：网络实体的安全即硬件设施的安全、软件的安全、数据的安全、运行的安全。对于安全保护所应达到的目标，简单地说就是信息不能传至未经授权的人，要保证信息的完整性。《计算机欺诈与滥用法》这部专门针对计算机犯罪的单行刑法的制定及其以后的数次修订，正是体现了对于计算机信息系统安全的统一认识，从而实现对于传统法律框架的突破，在追究和惩治计算机犯罪方面取得了成效。可见，只有将计算机犯罪的打击放在当代计算机及网络技术迅猛发展的宏大背景之下，将计算机信息系统安全作为一种特殊的犯罪客体来看待，才能对计算机犯罪给予有效的和恰如其分的打击。

3.2　适应信息系统安全及其保护的基本特点，增设计算机犯罪的新罪名

计算机犯罪是一种新型犯罪，世界各国对这种犯罪的研究也是刚刚起步，从这个意义上说，目前大多数国家防治计算机犯罪的法律都是不健全的，远远滞后于计算机犯罪的现实罪情，这在计算机犯罪罪名的设定上尤其如此。《联合国关于预防和控制与计算机相关犯罪指南》将计算机犯罪分为五种类型：(1) 计算机操作欺诈；(2) 计算机伪造；(3) 破坏和修正计算机数据或程序；(4) 授权访问计算机系统；(5) 非法复制计算机软件。美国有学者将计算机犯罪分为六类：(1) 非法进入或使用计算机；(2) 电子传播隐私；(3) 篡改或损毁资料；(4) 窃取或盗用服务；(5) 妨碍他人使用计算机；(6) 非法持有密码。[11] 其实，无论哪一种分类，关于计算机犯罪类型范围都相对偏窄。随着计算机在社会各领域的广泛应用以及网络技术的发展，可以预见，计算机犯罪将会渗透到社会的方方面面。因此，除了常见的利用计算机技术进行盗窃、诈骗、侵占、贪污等侵犯财产罪外，还可能会出现进行危害国家安全、扰乱社会秩序、破坏市场经济秩序等方面的犯罪类型。有学者甚至指出，除了强奸罪等必须以行为人自身或者他人的人身作为犯罪工具的犯罪以外，其他犯罪均可通过计算机加以实施，甚至杀人罪也可以通过计算机来实施。[12]

不过，关于计算机犯罪的罪名并非多多益善，一种新罪名的设立往往要求考虑多种因素。这是因为刑罚权的行使并不是越普遍越好，而刑法的目的也不只是打击和遏制，它还应当保障人权，有利于推动技术发展，并不至于过度干涉公民自由。刑法从其本质上说是一种必要的“恶”，应当赋予其一定的谦抑性，即刑法的介入应当限定在必要的范围之内，只有当其他法律不能充分保护时，才适用刑罚这一种最为严厉的责任方式。因此，在考虑设定计算机新罪名时，应当理性地审视计算机犯罪既有罪名与现实需要之间的关系，在打击计算机犯罪与尊重公民自由、推动技术发展之间寻找到一个合理的平衡点。从美国《计算机欺诈与滥用法》的制定与发展的基本趋势来看，这部单行刑法的适用范围在不断扩大，打击力度也在渐次增强，相关的罪名也在增加，但是，这种扩大是渐进的和慎重的，比如，一开始仅仅保护国防和外交信息系统、金融信息系统，其后又扩展到关乎百姓生命健康的医疗信息系统。又如，对于篡改、毁坏数据或者阻止正常使用进行刑事制裁要求所造成的损失达到一定的数额，从而使刑罚对于网络世界的介入具有了适度性。同时，这部法律关于计算机犯罪罪名的设置还体现了计算机技术的特点，比如，计算机系统不仅存在未经授权进入的行为，还包括超越授权进入的行为，因此后者也被纳入刑事制裁的范围。又如，计算机密码不仅是保障计算机信息系统安全的重要技术措施，也常常成为犯罪行为所侵害的对象和使用的手段，因此，1986 年的修改设立了涉及计算机密码的犯罪类型，恰如其分地反映了计算机技术及计算机犯罪行为的特殊性。

3.3　构建计算机犯罪侦查的特别制度

计算机犯罪与其他犯罪相比具有鲜明的特点，即形式上的极强隐蔽性、技术上的极高智能性、空间上的跨越性、实施上的低成本性、证据上的易改性、后果上的高度危害性。由于犯罪手段上的特异性，计算机犯罪对传统的侦查与证据制度产生了冲击与挑战。计算机犯罪的高隐蔽性使得传统的“调查摸底、诸个排查”方法应付乏力。传统证据如笔录、指纹、足迹、血迹等，在司法实践中都可以直截了当地使用。而计算机证据却可能留在计算机及其相应媒介中，这对于司法机关从计算机及其媒介中获取证据的能力提出了较高的要求。计算机及其网络上的犯罪，大都是在“虚拟世界”或“虚拟空间”里进行，这种无现场性使得传统犯罪的侦查理论与技术难以适应要求。计算机犯罪证据易于遗失与损坏的特性也增加了获取并处理这种证据的难度。[13] 计算机犯罪在侦查活动和证据运用上的特殊性要求构建特别的侦查制度。其中最为重要的有以下三个方面：

(1) 适当地扩大侦查权力。涉及计算机犯罪的有关信息或非法资料往往很隐蔽地隐藏在因特网的连接系统中，甚至一个合法文件、操作系统之中。传统的侦查制度要求侦查权只能用于那些有犯罪嫌疑的地点或人员，这就无法完成对这种隐藏在合法人计算机里犯罪线索 (下转第 97 页)

[27] 国务院信息办 1997 年 6 月 3 日颁布。

[28]《中国互联网络域名注册暂行管理办法》第五章 注册域名的变更和注销 中 第二十四条 注册域名可以变更或者注销,不许转让或者买卖。

[29] 国务院信息办 1997 年 6 月 3 日颁布。

[30] 参考《中国互联网络域名注册实施细则》第三章第十三条的规定。

[31] 美国商标专利局 http://www.uspto.gov/web/offices/pac/mpep/consolidated_laws.pdf

[32] 刑法 285 条规定的非法侵入计算机系统罪、第 286 条规定的破坏计算机系统的犯罪、第 287 条规定的利用计算机实施的犯罪。

[33] 全国人大常委会于 2000 年 12 月 28 日第九届全国人民代表大会常务委员会第十九次会议通过。

[34] 该条款未能明确一个清楚的与计算机犯罪相关的定义

[35] 根据《Establishment of a European Network and Information Security Agency (ENISA)》整理归纳 http://europa.eu.int/scadplus/leg/en/lvb/l24153.htm

作者简介:周磊(1981-),男,华中师范大学信息管理系研究生,研究方向为信息管理与竞争情报。

(上接第 92 页)的侦查与调查。美国在 9·11 事件以后为了有效地打击和遏制本土的恐怖犯罪活动,颁布了《美国爱国者法》,其中涉及了有关计算机信息或证据的收集问题。其第 209 条规定,依据一定的搜查令,联邦执法部门可以搜查、扣押保存在电子通讯设备中存储的信息,如未经阅读的电子邮件等,还可以对正在传递中的信息进行截取等。其第 210 条和 211 条规定联邦执法部门可以在未经司法审查的情况下要求电脑和网络服务机构提供客户的详细情况。[14] 这些规定在一定程度内扩大了刑事侦查部门的侦查权力,它对于计算机犯罪的侦查必将产生重要的影响。

(2) 建立兼顾计算机犯罪侦查与预防的专项制度。在计算机犯罪预防方面,人们通常可以借助于计算机技术采取身份认证、加密与数字签名等制度,但计算机黑客们仍然可能突破技术上的壁垒,特定的预防技术与相应的遗存记录或痕迹存在着很大的关系,从而也就要求将侦查与预防紧密地结合起来,以增强实效。

(3) 设置专门针对计算机犯罪侦查的特别侦查机构。在美国,为了应对愈演愈烈的计算机犯罪,一些民间的团体组织起来采取相应的措施,如卡耐基—梅隆大学由 15 个程序师组成了“计算机紧急反应小组”(Computer Emergency Response Team,CERT),为在网络上打击犯罪行为提供商业性的服务,如果用户的系统出现了未经授权侵入的情况,该小组可以帮助用户进行调查。但是这种民间团体不能行使公共权力,加之力量不足,因而效果也有限。逐渐地,经过特殊训练的执法人员成为在网上打击犯罪的主要力量。美国在联邦调查局内部设立了国家计算机犯罪侦查队,简称 NCCS,负责侦查违反《联邦计算机诈骗与滥用法》的犯罪行为。通过设置专门的侦查机构,吸纳和培训专业的侦查人员,对于全面提高侦查计算机犯罪的工作能力与效力具有至关重要的作用。

参考文献:

[1] Neal Kumar Katyal. Criminal Law in Cyberspace, University of Pennsylvania Law Review[J].April, 2001,1013-1014.

[2] Frank Easterbrook. Cyberspace and the Law of the Horse [M].1996 U. Chi. Legal F. 207.

[3] Laura Nicholson. et al, Weinberg Computer Crimes, American Criminal Law Review[M]. Published by Georgetown University Law Center, 2000,58.

[4] http://www.msnbc.com/news/178744.asp

[5] http://www.cnn.com/2000/tech/computing/08/01/pentagon.at.defcon.idg/index.html

[6] 18 U.S.C. s 1030(a)(1)-(3)(1984).

[7] 18 U.S.C. s 1030(a)(4)(1988).

[8] 18 U.S.C. s 1030(a)(5)(1988).

[9] 18 U.S.C. s 1030(a)(6)(1988).

[10] 张晓红.计算机犯罪之犯罪客体再研讨[J].行政与法,2003,(12).

[11] 郑汉军.从比较法角度看我国计算机犯罪侦查问题[J].江苏警官学院学报,2003,(5).

[12] [13] 刘宁生.“计算机犯罪”对传统刑事法的冲击及对策[J].甘肃政法学院学报,2002,(4).

[14] 秦策.9·11 事件后美国的刑事诉讼与人权保护[J].江苏警官学院学报,2003,(6).

作者简介:张琳(1970-),女,南京农业大学信息科技学院讲师,主要研究方向为信息安全与信息立法。