联合国 A/CONF.203/14

第十一届联合国预防犯罪和刑事司法大会

2005 年 4 月 18 日至 25 日，曼谷

Distr.: General
14 March 2005

Chinese
Original: English

临时议程*项目 3
打击跨国有组织犯罪的有效措施

讲习班 6：采取措施打击计算机犯罪**

背景文件***

摘要

新的信息和通信技术在世界范围内迅猛发展，带来了更多形式的计算机犯罪，不仅威胁到计算机系统的保密性、完整性和可利用性，而且威胁到关键基础设施的安全。而且，技术创新带来了不同形式的犯罪创新；因而，计算机犯罪的不同威胁折射出所谓的“数字鸿沟”的差异。在打击这类犯罪时，调查人员、检察官和法官面对许多引起争论的问题——部分源于无形和瞬时的数字证据。此外，为了有效调查和起诉计算机犯罪，经常需要跟踪犯罪活动及其影响，而这件事须通过各种因特网服务供应商或公司进行，有时它们分属不同的国家，这可能带来管辖权和主权等难题。

计算机犯罪特有的挑战的复杂性要求开展国际合作，最终需要各国都有必要的法律、程序和规章手段。为了制定有效的办法，开展高效的国际合作打击计算机犯罪，最近几年，做了许多区域和区域间工作，取得了几项重大成就。为了使这些努力开花结果，必须支持广泛研究打击计算机犯罪所涉各方面问题，促进在政府和私营部门之间建立活跃的伙伴关系。

本背景文件强调计算机犯罪所造成的挑战，以便讲习班 6 的参加者可以考虑第十一届预防犯罪和刑事司法大会各区域筹备会议提出的建议，并制订采取有效的全球对策的方针。

* A/CONF.203/1。

** 秘书长谨感谢韩国犯罪学协会和加拿大政府协助举办讲习班 6。

*** 本文件的提交有所推迟，因为需要进行更多的研究和磋商。

V.05-82258 (C) 120405 130405

目 录

段次页次

一、导言 1-2 3

二、计算机犯罪 3-13 4

三、数字鸿沟和计算机犯罪 14-22 8

四、跨越边界：跨国界犯罪和计算机取证 23-35 10

五、国内立法：必要的先决条件 36-50 13

A. 不依赖其他罪的独立的犯罪行为 39-41 14

B. 程序权力 42-50 14

六、通过国际合作寻求解决办法 51-61 16

七、计算机犯罪研究中的合作 62-63 18

八、公共和私营部门合作，对付计算机犯罪 64-69 19

九、建议 70 20

一、导言

1. 信息和通信技术正在全世界范围内改变着我们的社会。技术创新正创造出商品和服务的新市场。这类技术正在使劳动过程发生变革、提高传统工业的生产力，并且改变着资金流动的速度和方向。然而，经济变化仅仅代表了等式的一边。社会也在经历着深远的文化变化——塑造着大众传媒并被其塑造以及适应着因特网的迅速发展。新的信息和通信技术在世界范围内的迅速发展也带来了阴暗的一面：它使新的剥削方式成为可能，为犯罪活动提供了新的机会，并且事实上带来了新的犯罪形式。

2. 第十一届联合国预防犯罪和刑事司法大会的四次区域筹备会议提出了很多建议供第十一届大会审议，其中包括：（a）审查关于国家间以及国家与因特网供应商之间合作的当前实践以及现有的国内法律框架与安排；（b）研究促进政府和私营部门之间进行合作、交流专长、知识和专有技术的最佳方法，从而建立并实施预防和控制计算机犯罪并确保计算机网络和通信系统安全的机制，并且建立适当的反应机制；（c）探索增强政府开发和使用适当的特别调查技术的能力以及检控能力，包括制定和确立对刑事司法官员的全面培训方案；（d）处理使用电脑化技术剥削妇女和儿童的问题，特别是关于色情制品和恋童癖读物；（e）研究可否建立一个全球因特网工作组，为打击计算机犯罪进行国际合作；（f）考虑提议进行有关打击网络犯罪的新公约的谈判，目的在于为采取有效的集体行动打击此类犯罪活动奠定基础。[1]

在过去三十年中，“计算机犯罪”或“网络犯罪”等类似措辞的概念化成为了人们争论的主题。该词的原型可以追溯至斯坦福研究所的一份报告，[1] 并且在 1979 年 [2] 和 1989 年 [3] 以稍微不同的形式重新出现。其构造安排在随后关于网络犯罪的文章中被广泛采用：计算机作为犯罪的主体；计算机作为犯罪的客体；或计算机作为一种工具（于 1973 年提出了第四种作用，即计算机作为一种象征，似乎在 1980 年代就不再有这种提法了）。对这一概念模式的有益的重新阐述为，将计算机犯罪视为由立法和/或法学理论所规定的这样一种行为：（a）针对计算和通信技术本身；（b）在实施犯罪时使用了数字技术；或（c）进行其他犯罪时偶然使用计算机，并且使计算机因此成为数字证据的来源。[4] 法律和条约，包括欧洲委员会制定的《网络犯罪公约》[5]，界定了各种类型的计算机犯罪（例如，危害计算机系统保密性、完整性或可利用性的犯罪；与内容有关的犯罪行为；以及有关知识产权的犯罪行为）。

二、计算机犯罪

3. 有很多形式的计算机犯罪针对的是信息和通信技术本身，这类犯罪有时被称为危害计算机系统保密性、完整性或可利用性的犯罪。它们的形式包括使用不同的黑客技术盗窃电信服务和盗窃计算机服务（依据所使用的技术，它们包括未经授权的访问、破解密码和口令、数字克隆、盗取信用卡数据等）。服务器和网站可能成为阻绝服务攻击的目标。在一些情况中，这类犯罪是分散的阻绝服务攻击造成的后果，在阻绝服务攻击中，数十或数百台暴露的计算机被用作“僵尸”来按照要求攻击目标，而由于要求过多，以至于没有一个要求可以执行。在其他情况下，阻绝服务是由于“数据包风暴”产生的，而这种风暴是由于超快蠕虫（自我复制计算机程序）的蔓延式繁殖造成的，这种蠕虫可以在很短的时间内自我复制数十亿份——它们的纯体积会阻塞最快的光纤线路并使大型的公司计算机系统停止工作。在过去二十年中，全球计算机病毒的肆虐曾破坏商业和消费者网络；并间歇地出现毒性和破坏性特别的新蠕虫和病毒株。近期的例子反映出两个专门化的极端：一个极端是以运行最流行的操作系统的上千万计算机系统的特定总体为目标的特制蠕虫；另一个极端是设计只针对在几千个平台上运行的高端安全应用程序进行攻击的蠕虫。

澳大利亚墨尔本的两位居民向澳大利亚和美利坚合众国的一些地址发出了600至700万封电子邮件，并在主要的因特网服务供应者的留言板上张贴了大量的信息。传递这些信息的目的是鼓励人们购买在全国证券交易商自动报价系统协会（纳斯达克）股票交易所交易的一家美国公司的股份。这些用假名称发送并通过第三方服务器转发的信息通报说该公司的股价会上涨900%。此后不久，在交易暂停以及该公司否认各种通信中所作的声明之前，该股票的交易量增加了十倍，价格也上涨了一倍。

这两个居民所从事的是典型的“哄抬股价、出清股票”计划：他们的一个合谋者——该公司的一位股东——知道他所传递的是虚假信息，而当公司的股价上涨时，他就出售该公司的股票牟利。

这两个人同时违反了澳大利亚和美国的法律。除操纵股市之外，由垃圾邮件产生的通信量足以构成干扰计算机合法运行罪。澳大利亚证券和投资委员会（ASIC）采取行动以回应澳大利亚公众的投诉以及美国当局提供的信息。从通过不令人起疑的商业网络发送的电子邮件信息的轨迹以及用来支付因特网服务费的财务轨迹查出了犯罪人。

正如有关此类性质的犯罪所常见的那样，美国证券和交易委员会请求返还不法所得，并要求发出禁止这两名共犯再次进行他们的活动的临时和永久禁令。要求他们交出不法所得，并承诺以后不再进行这种行为。美国当局相信澳大利亚有能力处理在澳大利亚进行的这一刑事诉讼。澳大利亚证券和投资委员会对两名被告提出了 19 项犯罪指控。两人都承认散布可能诱导人们购买证券的虚假或重大误导性信息，并干扰、妨碍或阻碍了计算机的合法使用。两人都被判两年刑期，缓期执行（主谋在三个月监禁后）。

4. 如果是公司，不能获得数据存在各种情形，从可能恢复的数据（例如，不满的雇员进行的攻击，他对数据文档进行了未经授权的加密），到不可恢复的数据破坏（指不仅仅是文档的删除还包括物理的清除和/或销毁硬盘驱动器或其他储存这些文档的存储介质）。近些年为公司所迅速采用的无线局部区域网容易受到阻绝服务的攻击（例如人为干扰），即便它们可以阻止未经授权的访问。[6]

5. 认识到计算机是如何被用作进行其他犯罪的手段或工具也是必需的。有许多各种各样的犯罪是和数据修改联系在一起的——其中一些涉及恶意损害他人财产的行为比如电子破坏行为（例如，损毁网站），其他的则包括专业伪造和假冒行为。有一些网站专门从事“制造卡片”（伪造信用卡），其活动包括提供高质量的假币和假护照。数据盗窃[7]涵盖了从信息盗版和工业间谍到侵害版权（盗版软件、MP3 音乐文档、数字视频等形式的知识产权盗窃）。[8]数据盗窃可能不仅仅是经济犯罪，在和身份盗窃相关的新兴犯罪中，还可能侵害到个人的隐私及其他相关权利。

6. 有很多类计算机犯罪涉及经济盗窃，比如对银行或金融系统进行黑客攻击以及与资金电子转账有关的欺诈行为。还有人表示了对电子洗钱和偷漏税等相关问题的顾虑。

7. 计算机还被用来帮助进行范围广泛的涉及欺骗行为的电话销售和投资欺诈。基于消费者的投诉，拍卖欺诈是最广为报道的与计算机有关的欺诈行为，根据 2003 年美国的一份综合报告占到所提起的欺诈投诉的 61%。[9]其他形式的欺诈消费者行为属于较为普通的一类，即网上交易后“不交付商品或不付款”。与低值投资的证券市场操纵行为相关的证券欺诈在消费者层面上还比较少见。

一位 15 岁的加拿大人控制了很多台计算机，并于 2000 年 2 月利用它们对雅虎、Amazon.com 和其他著名的电子商务网站进行了阻绝服务攻击。通过减慢或限制对这些网站的访问，他给经营者造成了上百万美元的损失，这些损失包括营业损失、市场资本化和升级安全系统的费用。这个少年在网上聊天室夸耀他所进行的攻击后，美国联邦调查局查出了他，并将案件交给了加拿大皇家骑警队。即便有国家愿意引渡青少年，那也是为数不多的，在这个案件中，根据加拿大的法律排除了对青少年的引渡。2001 年 9 月，他被判在青少年拘留中心服刑八个月。

8. “网上钓鱼”（或欺骗性邮件）是指制作带有相关网页的电子邮件信息，这些网页被设计成类似于现有消费网站的样子。像垃圾邮件一样，上百万封这种欺诈性邮件被分发出去；然而，和直接诱导人们购买产品或服务的方法不同，这些邮件声称是银行、在线拍卖或其他合法网站发来的，并企图欺骗用户提交个人、财务或口令数据。然后利用这些个人信息进行欺诈性交易（有时是将这些信息出售给第三方之后）。

9. 现有的犯罪行为，例如敲诈勒索（威胁披露专有信息或个人信息或者损坏数据或系统）和骚扰，也可以在网上进行。还提出并成功地起诉了一些诽谤和诬蔑案件。

10. 还有一系列涉及计算机的与内容有关的犯罪，特别是散布非法和有害的材料。国际社会特别关注的是儿童色情读物。虽然几十年前就存在儿童色情读物（以照片、杂志、电影和录像的形式），但是自 1980 年代末期以来，通过各种计算机网络，利用包括网站、用户网络新闻组、因特网中继笔谈以及对等网络（P2P）在内的一系列因特网服务来传播儿童色情读物有增长的趋势。[10] 这些网络被用来帮助进行信息交换、儿童色情图片或录像交易、现金交易以及有关儿童性旅游的信息。散布儿童色情读物一部分是出于商业目的（而非恋童癖者之间的非金钱交换），并且和跨国有组织犯罪联系在一起。还有一个不是那么明确界定的灰色区域，其中违法行为跨入了一个一般被许可的领域，因为在过去 25 年中因特网都被用来散布色情读物，大部分的这种行为在很多法域都是合法的，并且是商业性的，经常被称为是“成人娱乐业”。[11] 但是，还有其他比较明确界定了的情况；构成色情读物的某些表现方式（不论是以数字图像还是以数字录像的形式）在很多国家在法律上被视为黄色读物，而散布这种黄

色材料是一项犯罪。因特网还被用来进行其他有关内容的犯罪，比如散布煽动仇恨的宣传和仇外材料。[12]

1990 年代最著名的案件就是俄罗斯联邦的一个年轻人对花旗银行的攻击，他擅自进入了位于美国的该银行的服务器。他找到了很多同谋在世界各地开设银行账户，接着指示花旗银行的计算机向这些不同的账户转入资金。当发现这个阴谋并确定了嫌疑犯时，美国联邦法院发出了逮捕令。当时，俄罗斯联邦和美国之间没有引渡条约，但是被告犯了一个错误——到联合王国去参加一个计算机展览。根据联合王国和美国之间有效的引渡安排，只要被告被指控进行的犯罪行为在联合王国法中有相应的罪名，联合王国当局就可以进行协助。被告申请人身保护令对引渡提出异议，特别争辩说，盗用行为是在俄罗斯联邦进行的，它的计算机键盘位于俄罗斯联邦，而不是美国。法院裁定被告对位于美国的磁盘所实施的行为比在圣彼得堡的物理存在更为重要。此外，被告被指控的行为在联合王国 1990 年《计算机不当使用法》中有明确的相应的罪名；如果他不是在俄罗斯联邦而是在联合王国进行的活动，那么联合王国法院就有管辖权。被告被引渡至美国，在美国他被宣判有罪并被关进了监狱。

11. 最近几年，人们对恐怖主义和因特网之间的关系给予了越来越多的关注，虽然在这方面也包含各种不同的活动。有迹象表明因特网正被用来帮助恐怖主义分子筹措资金以及作为计划和实施恐怖主义行动的后勤手段。人们还越来越集中注意到因特网在散布恐怖主义宣传资料以及利用因特网招募人员方面的作用。这些活动不同于网络恐怖主义，美国基础设施保护中心将后者定义为“通过计算机进行的导致暴力、死亡和/或破坏，以及为了强迫政府改变其政策而制造恐怖的犯罪行为”。[13] 人们对两个不同的方面有顾虑：对重要数据的攻击和对重要基础设施的攻击。

12. 现在，人们日益认识到重要信息基础设施的重要性，网络不仅使通信成为可能，还被用来管理和控制能源、交通、食品和公共卫生等其他重要基础设施的重要方面。在全球许多国家，重要基础设施可以是私有的，并特别容易受到攻击，这是因为它们的很多分布式控制系统与监控和数据采集系统与因特网连接在一起，犯罪分子可从因特网上对其进行破坏。鉴于现代社会越来越高的关联性，对这些基础设施的网上攻击可以给国家经济和政治系统造成严重的后果，并带来深远的跨国影响。必须能对针对重要信息基础设施的攻击做出反应（不管是恐怖主

义活动还是其他犯罪活动引起的），从而最大程度地降低对社会必不可少的其他重要基础设施可能造成互相干扰效应的严重危险。

13. 过去五年引起国际关注的可以广为获得的强化加密所带来的挑战还没有解决，新一代的量子密码术就又出现了。[14] 虽然密码术是商业和电子商务所必需的，但是它也可以为犯罪分子所利用。这种“两用技术”困境不仅包括隐写术，还涵盖了各种可以自由获得的对等网络软件，这种软件通过高度抗审查的强化加密（例如 Freenet）而获得增强。这类技术促进言论自由并且可以推动民主自由，但是也可以被犯罪分子用来隐藏他们的通信或传播非法材料。

三、数字鸿沟和计算机犯罪

14. 在信息和通信技术传播到世界各地之时，技术的分布并不均匀。当一个地区可能正在铺设大容量光纤电缆时，另一个地区可能正经历着移动和无线网络的迅速发展。不同类型的技术改造使各个区域有着不同的弱点，并且出现了特殊种类的计算机犯罪来利用这些不同的情况。

15. 发生的变化是巨大的：信息和通信技术设备数量的急剧纯增加（现在全世界大约有 20 亿台计算机和其他微处理器管理的设备在运转）；连通性的指数化增长；革命性的计算技术进步，比如小型化、速度和存储量上的突破；智能系统和机器人的出现以及人机对话的增强。但是，这种技术变化不仅以一种前所未有的方式渗透着我们的环境，将人、物和信息联系起来，而且还带来了下一代的数字威胁和弱点，并且使我们有必要对 21 世纪如何认识犯罪进行彻底的重新思考。

16. 认识到这一点，2002 年大会鼓励进行新的国际努力，以帮助会员国应付计算机犯罪。在 2002 年 1 月 31 日大会第 56/261 号决议所附“执行《关于犯罪与司法: 迎接 21 世纪的挑战的维也纳宣言》的行动计划”中，专门有一节的题目是“打击高科技和计算机犯罪行为”；在这一节中，就预防和控制这类形式的犯罪提出了面向行动的政策建议。在 2002 年 12 月 18 日第 57/170 号决议中，大会请预防犯罪和刑事司法委员会在根据大会 2001 年 12 月 19 日第 56/119 号决议拟订有关第十一届大会的建议时，考虑在落实《维也纳宣言》和行动计划方面取得的进展。

17. 认识到存在数字鸿沟，这是 21 世纪之初联合国最重要贡献之一。大会在 2000 年 9 月 8 日第 55/2 号决议中通过的《联合国千年宣言》提供了总体背景。在秘书长题为“执行《联合国千年宣言》路线图”的报告（A/56/326）所附《千年发展

目标》的目标 8 下，具体目标 18 是：“与私营部门合作，分享新技术尤其是信息和通信技术的益处”。在 2003 年 12 月 10 日至 12 日在日内瓦举行的信息社会世界高峰会议所通过的《原则宣言》（A/C.3/59/3，第一章，A 节）中，关于信息社会有一个共同的看法：“我们亦充分意识到，发达国家和发展中国家之间以及各个社会内部并非均等地享受到信息技术革命所带来的益处。我们充分致力于将数字鸿沟转变为人人享有的数字机遇，特别是面临落后和更加边缘化危险的人们所享有的数字机遇。”[15]

到 2004 年末，中国上网人口达到 9 400 万，约占中国总人口的 7.2%，其中有 45.5%是宽带用户。估计主机的数量总共有 4 160 万台，IPv4 地址有 6 000 万，域名 432 077 个 cn 网站 668 900 个。[16] 中国因特网用户以每年大约 18%的增长率增长，到 2008 年超过北美的上网人口，现在已经超过了日本和韩国的上网人口之和。在 1999 年还只有 890 万用户，在 2001 年就增加到 3 370 万人，主机的数量则从 1999 年的 350 万增加到 2001 年的 3 370 万。

18. 到 1985 年底，因特网主机数量超过了 2 000 台；在 1989 年达到了 10 万台，而在 1990 年则超过了 30 万台大关。1992 年中期，这一数量达到 100 万台，1995 年底或 1996 年初达到 1 000 万台，2000 年底达到 1 亿台，在 2002 年 7 月超过了 1.62 亿台。[17]2002 年，在发展中世界，每 100 个居民中只有 4.1 个因特网用户和 3.3 台个人电脑；而在发达世界，每 100 个居民中有 33.3 个因特网用户和 36.2 台个人电脑（E/2004/62 和 Corr.1）。生活在最高收入国家的世界上五分之一的人口拥有着世界上 81.9%的个人电脑，占全球因特网用户的 76.2%，并拥有全球因特网主机的 97.5%。[18]

19. 大多数发展中国家没有可以支持这些动态的现代和有效的信息和通信系统的电信部门。在 2000 年，联合国报告说全球人口只有大约 4.5%可以访问网络，相比之下，北美人有 44%，欧洲人有 10%，而在非洲、亚洲和南美的比率则只有 0.3%至 1.6%不等。[19] 目前，在地区层面上，全球 98%以上的因特网协议带宽都是连到北美或从北美连出的。55 个国家占了全球信息技术生产费用的 99%（E/200/52，第 50-51 段）。现在有向知识经济发展的明显趋势，但是除开发之外的其他因素，例如电信服务的结构和获得电信服务的费用，会影响获得和使用的比率。

20. 但是，随着信息和通信技术的益处开始更为广泛的传播开来，还有必要增强对随之而来的与计算机犯罪相关的威胁以及弱点的认识。数据差别不仅标志着发达国家、发展中国家和经济转型国家之间的区别，[20] 还反映出网络犯罪所产生的威胁和弱点的不同类型。信息和通信技术在不同时间、不同的区域被采用，这不仅仅是因为贫富之间的差异，还因为诸如区域地理之类的因素。例如，在一些多山区国家，铺设地下电信电缆的费用过高而不能进行，而设立微波中继塔和天线系统则使无线电话网络被有效采用。如此一来，一个国家或区域的信息和通信技术结构可能和邻近国家或区域的有很大不同。各国所进行的不同的技术革新导致了不同类型的新型犯罪，因而导致计算机犯罪引起的不同威胁。

21. 发展中国家只有最简单的电信基础设施，因此可能被用来作为进行攻击的基地，或作为发送攻击的经由国，特别是如果该国缺少阻碍计算机犯罪或使这种行为可以被起诉的法律制裁的话。就发展中国家而言，最初开始和继续使用这些技术可能会对特定区域带来新的威胁。一些人会提出，在该体系变得更健全并且安全标准贯彻得更彻底之前，新兴并依然脆弱的信息技术结构可能会十分脆弱。[21]

22. 公司或政府环境下的计算机及相应网络的类型和范围与消费者或居民环境下的有很大不同。随着普通人口开始越来越多的采用信息和通信技术，新的目标群出现，并且容易受到特定类型的计算机犯罪的攻击，这些犯罪包括了从病毒感染和计算机入侵到各种形式的消费欺诈。随着各国开始采用信息和通信技术，社会中的不同部门将会受到不同种类的计算机犯罪的威胁。

四、跨越边界：跨国界犯罪和计算机取证

23. 在调查计算机犯罪时，必须正视很多取证问题。还原涉及网络犯罪的事件的难题部分在于大部分证据都是无形且短暂的。计算机犯罪调查查出的并不是有形的证据，而是往往易失并短暂的数据轨迹。易失性的原因之一在于某些电子选址和路由信息（即“通信量数据”）不是永久储存的。这种信息可能只在一个计算机系统中储存很短的时间，接着就被其他路由信息改写。

24. 但是，新技术不仅造成了新的问题，也给调查者制造了新的机会，使重现电子轨迹成为可能。在很多情况下，通信量数据和其他形式的网络管理信息可能被储存在系统日志中而不会简单地被改写。在因特网和其他计算机网络上，各种网络管理信息一般被储存起来供随后分析，从而帮助进行网络账目管理、服务可靠性、网络设备可靠性、错误历史记录、运行趋向和能力预测。除了这些目的之外，

这种数据也可以用来进行营销和分析消费者特点（例如，零售网站上网页的点击可以帮助确定最受欢迎的产品、购物模式或消费者特点）。

25. 然而，通信量数据或类似的信息是否被储存是由很多因素决定的。例如，一个因素是服务的类型。一种网络访问服务（例如，使用远程准入投入用户服务（RADIUS）协议）可能会储存某些类型用户信息和一些通信量数据，从而允许用户访问因特网。这在必须记录用户是何时上网以及上网多长时间的计时服务中尤其流行。相反，在匿名或保密增强的服务中它则会最小化。[22]

26. 电子邮件可以追溯至因特网的最早时期（1971 年在 ARPANET 上就可以使用），一般在应用层包头中包含寻址信息和其他通信量数据。[23] 这些信息中的其中一些是由终端用户的客户程序产生的，一些是由电子邮件服务器产生的（运行简易邮件传输协议（SMTP））。

27. 最常见的因特网服务可能就是万维网了，它们中的大部分都使用域名系统（DNS）来建立与域名（网站位置的名称）和因特网协议地址（信息包传出和传至的数字地址）之间的联系。网站服务器可以储存大量的有关哪些网页被点击以及由谁（即从哪个 IP 地址）进行点击的通信量数据。这种做法在商业服务器中更为普遍，这是因为登录的数据会迅速达到千兆字节的水平，因而进行储存的代价是昂贵的。

28. 文件传输服务可能会也可能不会收集系统日志中的用户信息，这取决于实施情况。过去，文件传输是通过文件传输协议（FTP）进行的，虽然越来越多的安全传输使用了安全外壳（SSH）加密。近期，除了中央文件服务器之外，出现了 P2P 样式，P2P 使大量用户之间共享文件成为可能（分散的资源散布在由短暂实体组成的网络；例子包括 Napster、 KaZaA、 Morpheus、 Gnutella 以及 Freenet）。一些 P2P 形式有可以轻易获得的通信量数据，而其他形式则可以阻碍通信量分析。

29. 其他服务包括大约 10 万个处理可以想到的几乎每个主题的用户网新闻组。这些服务可以通过运行网络新闻传输协议（NNTP）的保存并转发服务器遍及全世界的网络来获得——一些通信量数据可以从服务器获得，而其他数据会在本地的个人电脑中。还有很多种包括从 IRC 到即时消息接发在内的实时聊天形式。

30. 不同的因特网服务一般是由不同的网络设备处理的（例如路由器或服务器）。根据服务供应商网站不同的配置方式，不同的系统日志会储存在很多不同的计算

机上，它们可能会被不同的法律实体所掌握，并且在一些情况下位于不同的法域。

31. 鉴于可能的服务的范围、不同的市场环境以及包括数据保持费用在内的很多因素，[24] 可以说没有收集和保持通信量数据和用户数据的单个的营业或工业位置。保持特定的通信量和用户数据明显可以便于执法机构通过因特网追踪犯罪分子；而一些国家近期通过立法强迫进行强制的数据保留。即便没有要求保留通信量数据的法律，法院调查者了解网络账目管理和因特网服务供应商的网络管理实践对于其决定因特网服务供应商满足执法机构要求的程度是至关重要的。[25] 在有关当局试图调查和起诉计算机犯罪时，与因特网服务供应商的合作是非常有价值的。

32. 对于计算机犯罪的有效调查和起诉往往要求通过各种因特网服务供应商或计算机连接到因特网的公司来追踪犯罪活动。调查要取得成功，调查者必须与不同国家的中间服务供应商进行合作来追踪通信轨迹，直到源头和受害的计算机或其他设备。为了确定犯罪源头的位置，执法机构往往必须依靠历史记录，这些记录反映出不同的连接是何时、从何处以及由谁进行的。在其他时候，执法机构也可能要在连接正在进行时进行追踪。当供应商位于调查者所处的管辖范围之外时，而事实上往往就是如此，执法机构就需要其他法域的类似机构的帮助。传统的、甚至是加速的司法互助办法一般是用来在只涉及两个国家（例如，受害者所在国和犯罪分子所在国）的情况下获得历史和实时数据。当犯罪分子经由三个、四个或五个国家发送信息时，在执法机构可以从位于通信轨迹最远处的每个服务供应商获得数据之前，司法协助程序会花费一连串的时间，这样会增加无法获得或丢失数据的机会，而犯罪分子则仍然查不出来并可以自由地进行进一步的犯罪活动。[26]

33. 为了协助对计算机犯罪的调查，1997 年八国集团高科技犯罪小组开始准备有关国际高科技和计算机犯罪的 24 小时联系。执法机构一天 24 小时、一周 7 天都可以获得计算机犯罪问题单位名单（以“24/ 7”为基础）。目前，该联系网涉及 40 个国家，也是《欧洲委员会网络犯罪公约》的组成部分，该公约为打击一切针对计算机系统、在计算机系统上和/或通过使用计算机系统进行的犯罪提供了一套调查工具。

34. 由于病毒、蠕虫以及黑客利用系统弱点的行为的盛行，有必要建立能做出可能的迅速反应的机制。目前，全世界有几十个国家都建立了计算机应急小组。其主要作用在于：

（a） 提供关于攻击方法、弱点以及攻击对信息系统和网络的影响的全面看法；提供关于事故和弱点趋势和特点的信息；

（b） 建立由越来越胜任的安全专业人员组成的基础队伍，他们能迅速地对与因特网联接的系统受到的攻击做出反应，并能够保护他们的系统不受安全威胁；

（c） 提供评估、改进和维持网络系统安全性和抗毁性的办法；

（d） 与卖方合作，改进已装船产品的安全性。[27]

35. 如果犯罪分子可能处于一个国家，攻击是从位于另一个国家的计算机发起的，而给第三国造成了影响，在这种情况下除了数据的易失性之外，明显还有由国界和管辖权问题所引起的法律难题。调查和起诉计算机犯罪时尤其要重视司法互助的重要性。但是主权问题只是在跨界搜查和扣押情况下所产生的问题之一。如果没有适当的司法互助，一国执法官员在查找位于另一国的计算机中的信息时就可能会对计算机系统进行未经授权的跨界搜查。然而，即便是在考虑司法互助之前，也有必要对国内立法进行反省。毕竟，国际合作首先要求各国已经具备了可以处理计算机犯罪的法律。

五、国内立法：必要的先决条件

36. 在一些情况下，某些类型的计算机犯罪会像传染病一样扩散，无视国家边界的存在。在其他情况下，犯罪的要素会利用小心预谋的令人困惑的或误导性策略而跨越国界。为了收获信息社会的益处，增强了信息和通信技术的密度，这一做法也增加了国内计算机犯罪发生的频率。因而，引入打击计算机犯罪的国内立法是符合各国自身的经济和公共安全利益的。

37. 国内法经历了几个世纪的发展，而因特网的发展历史则只有几十年。当然，法律会随着社会的变化而不断进行修改。为了应付计算机犯罪所带来的挑战，国内立法要现代化。Sieber 描述了 1970 年代以来各国所通过的六种主要的计算机犯罪立法潮流：[28]（a）数据保护以及隐私的保护；（b）处理与计算机有关的经济犯罪的刑法；（c）知识产权保护；（d）打击违法及有害内容；（e）刑事程序法；和（f）关于像密码术和数字签名之类的安全措施的法律规定。[29]

38. 在处理与计算机有关的犯罪时有很多因素是必要的：（a）确保法律规定了

这些犯罪；（b）建立打击网络犯罪的法律调查力量；和（c）通过提供保护基本人权和自由的安全措施来贯彻以上措施。

A. 不依赖其他罪的独立的犯罪行为

39. 已经制定出了一份有关侵害计算机系统保密性、完整性和可利用性的犯罪的全面的清单。[30] 还有一些与内容有关的犯罪（比如制造和传播儿童色情读物或仇外材料）属于计算机犯罪之列。

> 中国公安部信息安全监管局报告称，2001 年有不到 5 000 件计算机犯罪记录在案，而 2000 年只有约 2 900 件，1999 年有约 400 件。到 2002 年中，该局报告了 3 000 多起案件，据估计，到 2002 年底会处理 350 起系统入侵案和 800 多起毁损计算机系统的案件。[31] 该局所查明的案件数量正以不可抵挡的比率增加，尽管还有很多案件是没有报告或没被发现的。犯罪分子大部分都是年轻人（18-30 岁），他们进行的攻击大部分都是从网络或计算机聊天室发出的，并使用虚假 IP 地址或利用密码术或隐写术，通过连经 http 或 Sock 代理人来隐藏身份。因此，中国在计算机聊天室注册和监管方面采取了更有力的措施。

40. 当各国试图修改适用于有形商品的规定从而使其适用于数字商品所构成的无形和瞬息世界时，产生了大量的问题。

41. 在草拟规定时需要谨慎行事，以避免将合法的行为非法化。将刑法现代化时，在具体规定和概括规定之间存在着细微的分界线。措辞具体的规定在可以获得更新的技术时有可能会变得过时。因此，建议采用“技术中立性”的语言。

B. 程序权力

42. 最近几年，由于电子记录越来越盛行，这就要求很多国家去处理有关“文件”的定义问题。就算是像被搜查“地点”的概念之类的基本术语，在数据是通过计算机网络发送时，也可以成为法律难题（即搜查可能是对位于一地的一办公室中的一台计算机进行的，但是数据却可能储存在位于另一个实际地点的计算机中——尽管对于用户和调查人员来说是“虚拟”存在的）。

43. 在设计程序权力时，区分三种不同种类的信息是有益的：（a）电子通信的实际内容；（b）通信量数据；和（c）用户信息。区分这三种信息是明智的做法，

因为它们可能会带来对隐私或数据保护的不同期待，或引发其他基本人权和自由问题。

44. 第一类法律难题之一是制定“通信量数据”和“用户信息”的定义。例如，欧洲委员会《网络犯罪公约》[32] 将通信量数据定义为：“由构成通信链一部分的计算机系统生成的与采用计算机系统的通信有关的任何计算机数据，这种数据表明了通信的源头、目的地、路径、时间、日期、大小、宽度或基础服务的类型。”公约将用户信息定义为：“服务供应商所掌握的、与其服务的用户相关的除通信量或内容数据之外的计算机数据或其他任何形式的任何信息，通过这种信息可以确定：

“a. 所使用的通信服务类型，所采用的技术规定以及服务期限；

“b. 基于服务协议或安排可以获得的用户的身份、邮件或地理地址、电话和其他访问号码、计费和支付信息；

“c. 基于服务协议或安排可以获得的关于通信设备的安装地点的任何其他信息”（第 18 条，第 3 款）。

45. 联合国《预防和控制与计算机有关的犯罪手册》中考虑了有关定义的问题，[33] 欧盟理事会《关于针对信息系统攻击的框架决定》以及国内立法中也处理了这一问题。[34]

46. 在很多国家的国内立法中，由于诸如“私人通信”和“言论自由”之类的概念，某些内容可能会受到较高程度的宪法保护。如此一来，就有必要在法律上和程序上将某些因特网通信的内容（那些私人的而非公共的）和通信量数据区分开来。在某些情况下，通信量数据和用户信息 [35] 的某些要素可能会和数据保护规定有联系，因为它们组成可能会引起隐私保护的有关简历的核心信息。

47. 应该注意到，数据收集以及随后的保留承担着各种利害关系人相互冲突的利益和价值，可取的办法是在各种合法利益间寻求一种平衡。在一些法域中，根据合理的信息惯例，或有时根据数据保护或隐私立法中的规定，数据收集受到严格的限制，据此，数据只能为了有限的目的收集，只能在知情同意情况下用于所规定的目的，并受到有关适用的其他保障措施的制约（比如对该信息完整性的检查、已知的销毁时间表以及源访问）。[36]

48. 在一些法域中，与搜查和扣押相反，有多个关于实时内容监测的法律机制（比如搭线窃听规定），储存并转发技术一般会给这些法域带来独特的法律问题。在计算机犯罪方面，这可能就是电子邮件的问题，电子邮件在运动时可能需要对内容进行实时监测的授权，而在不动（即储存在电子邮件服务器或终端用户的硬盘驱动器上）的时候又可能需要搜查和扣押令。由于在两种情况下电子邮件信息是基本一样的，由于采用并可能会有两种法律限制的两种不同的法律工具，这可能会引起人们的担心。

49. 已经开发出很多法律手段用来协助与计算机有关的调查，这包括保管令和出示令。保管令是一种加速的机制，它要求服务供应商存储并保存一项交易或一位客户特有的现有数据。这种程序机制在电子证据环境中是重要的，因为这种证据比有形的文件更容易被删除或销毁。从本质上说，保管令就是“不要删除”令。保管令[37]是临时性的，并且是获得必要合法授权的执法机构为获得数据而做出的（比如，扣押该数据的许可令或发布该数据的出示令）。

50. 出示令要求文件的保管人在一段特定的时间向执法机构递交或使其可以获得文件。出示令类似于搜查令，但是发出出示令时，进行搜查的是文件的保管人而非警察。这种令状的破坏性较低，因为保管人更清楚地知道所说的文件的准确位置。在目前的商务环境中，公司通常会把数据储存在它们进行经营的法域之外，这往往是因为那里的数据储存费更便宜。在这种情况下，发出传统的搜查令是不恰当的，而出示令则可以让数据的所有人或其保管人检索这些文件或记录。

六、通过国际合作寻求解决办法

51. 为了有效的回应其他国家寻求协助的要求或为了从其他国家获得协助，可能有必要对国内法进行修改以便处理网络犯罪。在制定处理计算机犯罪的立法时，与其他国家的法律相协调是一个重要的目标。为了尊重各国主权并方便国际合作，最终需要探讨建立像公约之类的正式国际机制的可能性。为了使相互司法协助可以更有效地进行，各法域中的有关不依赖其他罪的独立的犯罪行为和程序权力的规定应该彼此协调。

52. 国际社会现在只是开始面对该领域还在不断出现的多种挑战。使用几个国家中的上百台不受保护的计算机攻击另一国商业网站的大规模阻绝攻击，或者由一种横扫世界三分之二地区的病毒或蠕虫造成的严重损害产生了一些基本问题，比如何处是犯罪地以及由谁进行起诉。另一个关键的问题是有效的行动是否最终会

取决于哪个国家愿意并有能力受托进行调查和起诉。各个法律框架以及刑事司法系统能力的不同会产生漏洞，而跨国计算机犯罪明显准备利用这一漏洞。一些人可能认为这损害了主权，而其他人则认为随着信息社会在全世界开始出现，主权正在发生转变。

53. 这种情况很快使人们注意到引渡这一复杂问题，而引渡本身就可以引起很多问题。例如，在不依赖其他罪的独立的犯罪行为不相兼容的情况下，这种犯罪的定义可能会使双重有罪要求不能被满足。另一方面，越来越多的人都同意，在要求双重有罪的情况下，是基础行为或是犯罪行为的基本因素必须相符，而不仅仅是在相关国家所规定的犯罪行为的形式必须相符。但是，即便在特定案件中双重有罪性没有带来问题，计算机犯罪的类型也可能被认为并不足够严重（例如，根据有关的量刑规定），因而不能引渡。

54. 然而，虽然存在挑战，但从 2000 年第十届联合国预防犯罪和刑事司法大会以来也取得了很多重大的成就，其中包括两个新的法律文书：《欧洲委员会网络犯罪公约》和《联合国打击跨国有组织犯罪公约》，后者的范围是世界性的，间接处理由有组织犯罪集团进行的网络犯罪。

55. 在国际层面上，联合国毒品和犯罪问题办事处、国际刑事警察组织（刑警组织）、经济合作与发展组织（经合发组织）、八国集团等实体，以及欧洲联盟、欧洲委员会、美洲国家组织、东南亚国家联盟和亚洲及太平洋经济合作组织等区域组织为促进国际合作提供了必要的政治和技术专长。和数年前不同，现在有可能讨论关于打击网络犯罪——特别是它经常采用的跨国形式——的国际共识。因此，最终具备了采取一致行动的积极的“道德氛围”，不论这种行动是民事、刑事还是行政措施，这种合作承认社会学家所称的“共同命运共同体”。[38]

56. 《网络犯罪公约》于 2001 年 11 月 23 日开放供各国签署，现在该公约已经获得了 30 个国家的签署和 8 个国家的批准。公约于 2004 年 7 月 1 日生效。它要求缔约国协调各自规定不依赖其他罪的独立的犯罪行为的国内法。这包括：针对计算机数据及系统保密性、完整性和可利用性的犯罪行为，以及伪造和计算机欺诈等与计算机有关的犯罪行为，与侵害版权有关的犯罪行为，和通过计算机系统进行的儿童色情制品犯罪行为。另外，公约设计了一套重要的程序权力，包括出示令和保管令，旨在帮助全球计算机网络环境下的调查和起诉。其中还规定建立一套国际合作的迅速和有效的体系。最后，因特网上的“仇恨犯罪”问题导致《网络犯罪公约》的附加议定书将通过计算机系统进行的种族主义或仇外性质的行为

定为犯罪[39]，该议定书于 2003 年 1 月 28 日开放供签署。它已经获得了 20 个国家的签署和 2 个国家的批准。

57. 2002 年，英联邦法律部长通过了题为《计算机和计算机犯罪法》的示范法。[40]这部示范法和《网络犯罪公约》有相同的框架，它为执法机构提供了打击计算机犯罪的有效和现代的手段。检察官、调查员和立法者可以评估国际上制定的材料，例如指导方针、法律和技术指南、最佳惯例和示范立法以协助有关当局制定国内立法。

58. 从 1990 年第八届联合国预防犯罪和罪犯待遇大会开始，联合国就积极参与处理与计算机有关的发展的各方面问题。[41]1994 年，利用加拿大政府和其他政府和非政府组织的很多专家提供的大量物质和财政帮助，出版了《联合国预防和控制计算机犯罪手册》。[42]

59. 2000 年，在第十届大会期间，举行了“与计算机网络有关的犯罪”讲习班。[43]2001 年，秘书长向预防犯罪和刑事司法委员会提交了关于预防和控制高科技和计算机犯罪的有效措施的研究结论（E/CN.15/2001/4）。

60. 2004 年，作为 2003 年 12 月信息社会世界高峰会议第一阶段的成果，联合国建立了研究垃圾邮件、计算机安全以及其他与因特网有关的问题的工作组，该工作组为 2005 年 11 月在突尼斯进行的世界高峰会议的第二阶段进行准备工作。

61. 计算机犯罪是一个国际性的现象并且需要一个国际解决方案。为了达成这一解决方案，国际社会应该认真回顾其已经使用的方法从而加强国际合作。它还应设法增加对该现象的各种表现、这些表现所带来的挑战以及预防和控制这一现象的可行且理想的途径的认识和了解。

七、计算机犯罪研究中的合作

62. 为今后的政策制定提供证据基础的任务是有挑战性的。对计算机犯罪的研究还处于初级阶段。出于商业、政治或国家安全原因，公共和私营部门中学识渊博的个人和机构可能受到约束，不能和研究人员共享他们的学识。公共记录中的信息往往是不完整或错误的。尽管有这些阻碍，发展知识基础仍是重要的，这样可以使我们缩小数字鸿沟的努力产生效果。

63. 要提供关于各种类型网络犯罪的普遍性和严重性的基本数据，需要使用多种

研究方法和比较办法。此外，通过回顾案例和消耗研究来研究新法律、警察策略和起诉的有效性也是至关重要的。研究不应仅限于警察或法院的数据，而这些来源则往往需要更加确定和统一。受害者和犯罪分子的行为，以及追踪全球立法和执法的发展都是最迫切需要研究的问题。[44]

八、公共和私营部门合作，对付计算机犯罪

64. 政府和私营部门的代表都越来越深地认识到了它们在对付计算机犯罪时进行密切合作的急切需要。没有哪一个政府或政府集团，也没有哪一个公司或工业部门能够依靠自己成功地解决这一问题，而要解决这一问题必须建立一个开放的、双向交流密切的公共和私营部门紧密合作关系。非常明显，私营部门实体已经并且会继续在开发技术以帮助预防和调查网络犯罪中发挥至关重要的作用。但是除了技术解决方案之外，私营部门还可以在帮助决策者确定立法优先问题和解决方案方面发挥重要作用。经验表明，政府和工业界之间积极的伙伴关系可以便于对计算机犯罪分子更有效地执法。

65. 公共和私营部门的伙伴关系正在增加，这是令人鼓舞的。八国集团的成员早就认识到有效地对付网络犯罪需要政府和工业界之间空前的合作，并采取了朝这一方向发展的重大举措，包括通过主持政府和工业界代表会议来讨论共同关心的问题以及可能的解决方案。[45] 联合国、亚太经合组织、经合发组织和其他多边组织在它们日常活动过程中也同样更努力地争取私营部门参与这类活动。

66. 2004 年 12 月，来自很多行业和国际执法机构的代表宣布建立 Digital PhishNet，这一合作执法行动将科技、银行、金融服务和网上拍卖行业的领导者和执法部门团结在一起，以处理“网上钓鱼”这一逐渐增长的有害的网上身份盗窃形式。Digital PhishNet 在工业界和执法机构之间建立了一个单一和统一的交流路线，因此，打击网上钓鱼的关键数据可以实时地进行编辑并提供给执法机构。当其他工业团体还把精力集中在辨别网上钓鱼网站站点和共享最佳做法及案例的信息时，Digital PhishNet 是集中关注帮助刑事执法和协助逮捕和起诉那些通过网上钓鱼对消费者实施犯罪行为的责任人的首批网络之一。Digital PhishNet 网罗了美国十大银行和金融服务提供者中的九家，五大因特网服务供应商中的四家以及五家数字商务和科技公司，并与联邦和国际最高执法机构进行合作。

67. 在过去几年中，很多私营部门实体和香港大学合作举办了很多重要的网络犯罪大会。这些大会将来自亚洲及太平洋的高级司法和执法官员和来自包括联合

国、欧洲委员会、刑警组织和亚太经合组织在内的主要多边组织的著名学者和代表汇聚一堂。讨论的范围包括网络安全挑战、对电子商务的威胁，如垃圾邮件、网络钓鱼以及其他形式的网上诈骗和网上盗版。

68. 世界各地的执法官员在过去几年和很多知名公司合作，对网上诈骗犯和其他网络犯罪分子进行调查和起诉，其中包括一些世界上最著名的垃圾邮件发送者。

69. 尽管取得了这一进展，但是为了进一步提高政府和工业界之间的协作水平，并为公共和私人部门之间对话及合作提供更广阔的架构并使其具有更强的规律性，还有更多工作需要做。

九、建议

70. 韩国犯罪学协会在汉城主持的两次专家会议中确定了以下建议，第十一届大会似宜在考虑第十一届大会区域筹备会议的相关建议的情况下审议这些建议：

（a）处理计算机犯罪问题需要一个广泛的、具有包容性的中心，它超出了刑法、刑事程序和执法的范围。这一中心应该包括，网络经济安全运行以优化商业信心和个人隐私的要求，以及促进和保护信息和通信技术的创新和财富创造潜力及机会的策略，包括在发生网络攻击时的预警和反应机制。在预防和起诉计算机犯罪的背后，隐约显露出创建网络安全的全球文化所带来的更大的挑战，这需要处理所有社会的需要，其中包括信息技术结构新近兴起但仍然脆弱的发展中国家；

（b）应该进一步发展各个层次的国际合作。由于其世界性的特点，联合国系统应该利用大会所要求的经过改进的内部协调机制在确保网络空间的运行和保护的政府间活动中起主导性作用，从而使其不被犯罪分子或恐怖主义分子滥用或利用。特别是，联合国系统应该有助于促进采取全球方案打击网络犯罪及采取国际合作程序，从而避免和减少网络犯罪对关键基础设施、可持续发展、隐私保护、电子商务、银行业和贸易的消极影响；

（c）应鼓励所有国家尽快地更新它们的刑法，以便对付网络犯罪的特殊性质。至于通过使用新技术进行的传统形式的犯罪，这种更新的完成可以通过阐明或废除不再完全适当的法律，比如不能解决毁损或盗窃无形物体的成文法，或通过制定关于新型犯罪如未经授权访问计算机或计算机网络的新规定。这种更新还

应该包括程序法，例如关于追踪通信的程序法，以及比如迅速保存数据的司法互助法律、协议或安排。在确定新立法的强度时，应鼓励各国借鉴欧洲委员会《网络犯罪公约》的规定；

（d）政府、私营部门和非政府组织应该相互合作，以缩小数字鸿沟、唤起公众对网络风险和适当对策的注意并增强包括执法人员、检察官和法官在内的刑事司法专业人员的能力。为了这一目的，国内司法行政部门和法律教学机构应在其教学计划中包含关于计算机犯罪的综合课程；

（e）第十一届大会应大力重视建立、改进和扩大目前打击网络犯罪所使用的有关国际信息共享、预警和反应机制、限制损害措施的实用工具，例如国际刑警组织，八国集团 24/7 警报机制、《网络犯罪公约》、计算机应急小组以及事故反应和安全队论坛（FIRST）， 这些手段仍只限于一些国家，其中大部分是发达国家。应该使全世界都可以使用这些手段，从而共享关于识别、保护、避免和处理新型网络犯罪的知识和信息，并且将有效的反应机制告知公众。另外，应该特别强调使发展中国家获得这些实用工具并提供相关的培训；

（f）计算机犯罪政策应该以证据为基础，并接受严格的评估，从而确保其效率和有效性。因此，国际上应该做出一致和协调的努力，以建立筹资机制，促进实用研究，并控制许多类新出现的网络犯罪。然而，确保在国际上协调研究工作以及广泛分享研究同样重要。

（g） 第十一届大会期间将举行关于采取措施打击计算机犯罪的讲习班，毒品和犯罪问题办事处应将讲习班的成果提请将于 2005 年在突尼斯举行的信息社会世界高峰会议第二阶段审议。

注

1 D. B. Parker, S. Nycum and S. S. Oüra, *Computer Abuse*（ Menlo Park, California, Stanford Research Institute, 1973）。

2 Donn B. Parker, *Computer Crime: Criminal Justice Research Manual* （Washington, D. C. , United States Department of Justice, 1979）。

3 Donn B. Parker, *Computer Crime: Criminal Justice Research Manual* （Washington, D. C. , United States Department of Justice, 1989）。

4 Russell G. Smith, Peter N. Grabosky and Gregor f. Urbas, *Cyber Criminals on Trial* （Cambridge, Cambridge University Press, 2004）。

[5] 欧洲委员会，《欧洲条约汇编》，第 185 号。

[6] 在一些国家，因特网居民用户使用无线局域网，没有安全保护措施的局域网被用来擅自访问因特网，以达到各种目的。这往往和“驾驶攻击”（使用汽车上的便携式电脑来定位和登陆无线接入点或“热点”）联系在一起。

[7] 在一些国家，“盗窃”这一概念仅仅涉及有形商品，包括使一个人丧失其有形物品；因此，它的范围并不延伸至盗窃无形商品，也不包括复制数据文件。一些国家不是通过刑事或惩罚性制裁来处理这些行为，而是将其视为属于民法包括版权制度的范畴。

[8] Bram Cohen 的 BitTorrent 对等软件越来越多地被用于共享大型数据文件，有的是出于合法目的（比如分发来源公开的软件、电脑游戏或电视节目的“实时放映”），有的是出于视频盗版目的。视频盗版的概况见 Clive Thompson 载于 2005 年 1 月 13 日的 Wired 的“The Bit Torrent effect”；以及 Jeff Howe 载于 2005 年 1 月 13 日的 Wired 的“The shadow Internet”。

[9] *IC3 2003 Internet Fraud Report*：2003 年 1 月 1 日—2003 年 12 月 31 日（美国国家白领犯罪中心和联邦调查局）。

[10] 见 Michael D. Mehta, Don Best and Nancy Poon., “Peer-to-peer sharing on the Internet: an analysis of how Gnutella networks are used to distribute pornographic material”。 *Canadian Journal of Law and Technology*, 第 1.1 卷，第 1 号（2002 年 1 月）；以及美国总审计署，*File Sharing Programs: Peer-to-peer Networks Provide Ready Access to Child Pornography*，GAO-03-351（华盛顿特区，2003 年 2 月）。

[11] Dick Thornburgh and Herbert S. Lin eds.，*Youth, Pornography and the Internet*（Washington, D. C., National Academy Press, 2003）。

[12] 有关 24 个国家处理种族主义、仇外和反犹太人材料的法律的概况，见 2004 年 4 月 28 日至 29 日在柏林举行的欧洲安全与合作组织打击反犹太主义会议审议的关于本主题的文件（CIO.GAL/25/04/Rev.1）。

[13] Scott Berinato, “The truth about cyberterrorism”, *CIO Magazine*, 15 March 2002。

[14] 关于可以在市场上获得的那些使用量子密码术将基于光纤的系统或无线网络上的数据加密，见 Gary Stix,“Best-kept secrets”，*Scientific American*, 2005 年 1 月。

[15] 关于对《千年发展目标》信息和通信技术方面的分析，见国际电信联盟，*World Telecommunication Development Report 2003: Access Indicators for the Information Society*，第七版（2003 年）。该研究对与信息和通信技术相关的千年发展目标作了有趣的评估，而新的数字存取索引尤其有前景。

[16] 中国因特网网络信息中心关于中国因特网发展的第 15 次统计调查报告（2005 年 1 月）（www.cnnic.net.cn)（2005 年 1 月 25 日访问）。

[17] Internet Systems Consortium（http://www.isc.org）。

[18] 源自国际电信联盟，《世界电信指标数据库》，第八版（2004 年）。

[19] 《2000 年世界经济和社会概览》（联合国出版物，出售品编号：E.00.II.C.1）。

[20] 有关对数字鸿沟的复杂性的统计分析，见 George Sciadas 编辑的 *Monitoring the Digital Divid…… and Beyond* （2003 年）中所提出的概念性框架。

21 人们已经注意到，具有讽刺意义的是，在正要缩小“数字鸿沟”的当口，这些情况又在不同层面重造了这种鸿沟，并可能会损害当地的商业信心或对投资的最初吸引力。

22 匿名服务和假名服务的主要区别在于，假名服务在一段特定的时间内会保存一个身份（化名或“名”）（因此假名身份、用户身份和“真实世界”中身份之间也许会有更强的联系）。另一方面，最纯正的匿名服务基本上是一种一次性或单一交易服务。有各种各样的匿名和假名服务，其中大部分是为获得一种或多种典型的因特网服务（比如电子邮件重邮程序、网上冲浪、因特网多线交谈或用户网新闻组）而提供代理人、链接或 mix-nets。也有不同程度的匿名和假名，不仅取决于基础加密和认证软件等因素，而且取决于提供匿名服务的服务器或服务器网络，生成“名”的程序以及支付服务中的计账机制。

23 David H. Crocker 修订的 *Standard for the Format of ARPA Internet Text Messages*, RFC 822（1982 年 8 月 13 日）。

24 在八国集团关于网络空间安全和信心的政府/业界对话（2000 年 10 月，柏林）期间举行的数据保留讲习班中，确定了以下有关数据保留的成本问题：系统日志的储存容量；有关数据的检索；设计和发展；管理、操作和培训成本；提供安全和隐私；为执法进行处理及交付的责任；以及与机会及消费者信赖有关的费用。

25 由于经营模式、服务和技术的不同，服务供应商保存数据的时间长度也可能各不相同。一些数据是为了记账而保存的，其他数据是为系统性能核查保存的。根据国内立法，要求或允许为执法以外目的而保留的时间范围从几秒钟到更长一段时间不等。不同类型的通信量数据所保存的时间也不一样，例如网络访问记录，RADIUS 或 TACACS+有不同于 NNTP 记录的商业和数据储存要求，因此在一些情况下，可能会保存更长的时间。内容一般是不保留的或不可获得的。

26 *Recommendations for Tracing Networked Communications across National Borders in Terrorist and Criminal Investigations*（http://canada.justice.gc.ca/en/news/g8/doc2.html）。

27 见计算机应急小组协调中心，2003 年年度报告（www.cert.org），以及事故反应和安全小组论坛（www.first.org）。

28 Ulrich Sieber, *Legal Aspects of Computer-Related Crime in the Information Society: COMCRIME Study*（1 January 1998）。

29 Russell G. Smith、Peter N. Grabosky 和 Gregor F. Urbas 所著 《在审的网络犯罪分子》（剑桥，剑桥大学出版社，2004 年）将 Sieber 关于国内立法的六种潮流模型应用于澳大利亚的经验。

30 经济发展与合作组织，*Computer-Related Crime: Analysis of Legal Policy,* ICCP 汇编第 10 号（1986 年）；又见欧洲委员会部长委员会于 1989 年 9 月 13 日通过的第 R（89）9 号建议。

31 向 2002 年 11 月 11 日至 13 日在汉城召开的亚洲及太平洋计算机犯罪和信息安全会议提交的“中国国家报告”，这次会议由亚洲及太平洋经济社会委员会和大韩民国信息和通信部举办。鉴于 2001 年至 2004 年 5 月在北京一个区（海淀区检察院）就有 52 名嫌疑犯被捕，犯罪分子的数量可能会很多——其中 48.4%是黑客攻击。

32 欧洲委员会，《欧洲条约汇编》，第 185 号。

33 《国际刑事政策评论》，第 43 和 44 号（联合国出版物，出售品编号：E.94.IV.5）。

34 联合王国的《规范调查权力法案》（2000 年）在第 2.9 条提出了通信量数据的定义，尽管这一定义也包括用户信息。联合国关于“笔录记录器”和“截留和追踪设备”的定义中包含了通信

量数据的概念（美国法典，标题 18，第 3127 条），并通过《提供打击与防止恐怖主义所需的适当工具以团结并强化美国法案》（《爱国者法案》）进行了更新（2001 年）。

35 至于用户信息，一些国家在电话领域可能已经存在现行规定（消费者、名称和地址信息）。

36 相关的国际文书包括，例如，1981 年欧洲委员会《关于在自动处理个人数据方面保护个人的公约》（欧洲委员会，《欧洲条约汇编》，第 108 号）或 1980 年经合发组织《调整隐私和个人数据跨国界流动保护的指导方针》。这些文书试图建立一些原则，据此个人信息必须正当地获得；只能用于最初指定的目的；对目的而言适当、相关而且不超过该目的；准确并随时更新；可以为主体获得；保持安全；并在使用后销毁。在一些法域进一步加强了义务的强度，例如，欧洲议会和欧盟委员会数据保护指示（95/46/EC 号指示和 97/66/EC 号指示）。随后，很多欧洲国家实施了更有力的数据保护法以履行它们的法律义务，满足指示的标准。在欧洲之外，也存在有关个人数据的类似规定的文书，比如，加拿大的《个人信息保护和电子文件法》。

37 注意“数据保存”确保有关特定用户的现有特定信息不被删除。相反，“数据保留”是旨在强制性要求所有因特网服务供应商收集和保留关于所有用户的一系列数据的一般要求。

38 Roderic Broadhurst, “Content crimes: criminality and censorship in Asia”, paper presented at Octopus Interface: the Challenge of Cybercrime, Strasbourg, France, 15-17 September 2004。

39 欧洲委员会，《欧洲条约汇编》，第 189 号。

40 该示范法可以在英联邦秘书处法律和宪法事务司的网页上找到：http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/{DA109CD2-5204-4FAB-AA77-86970A639B05}_Computer%20Cri-me.pdf。

41 第八届大会举行了“刑事司法管理电脑化”讲习班（A/CONF.144/14）。1992 年，本组织就制作了“刑事司法信息系统电脑化指南”（联合国出版物，出售品编号：E.92.X VII.6）。1995 年第九届联合国预防犯罪和罪犯待遇大会期间，举行了“刑事司法系统管理的国际合作和协助：刑事司法活动的电脑化和刑事司法信息的发展、分析和政策使用”讲习班（A/CONF.169/13）（又见：联合国预防犯罪和罪犯待遇亚洲和远东研究所，《高科技犯罪的全球挑战：与计算机网络有关的犯罪讲习班，第十届联合国预防犯罪和罪犯待遇大会，2000 年 4 月 15 日，奥地利维也纳》（2001 年 4 月，东京）。

42 《国际刑事政策评论》，第 43 和 44 号（联合国出版物，出售品编号：E.94.IV.5）。

43 见“与计算机网络有关的犯罪”讲习班的背景文件（A/CONF.187/10）。

44 Peter Grabosky 和 Roderic Broadhurst，“The future of cyber-crime in Asia”， Cybercrime: the Challenge in Asia, Roderic Broadhurst and Peter Grabosky eds, (Hong Kong University Press, 2005,) pp347-360。

45 见“八国集团柏林会议：关于网络空间安全和信心的对话（摘要和评价）”（载于 http://www.mofa.go.jp/ policy/economy/summit/2000/lyon.htm）；以及 Kuriko Miyake, “八国集团结束东京高科技犯罪 2 犯罪会议“（载于 http://archives.cnn. com/2001/TECH/internet/05/31/g8.cyber.crime.idg）。