联 合 国 E/CN.15/2001/4

经济及社会理事会

Distr.: General
30 March 2001
Chinese
Original: English

预防犯罪和刑事司法委员会
第十届会议
2001 年 5 月 8 日至 17 日，维也纳
临时议程*项目 4
开展国际合作打击跨国犯罪

关于预防和控制高技术犯罪和与计算机有关的犯罪的有效措施的研究报告的结论

秘书长的报告

提要

本报告部分是为了回应经济及社会理事会在其 1999 年 7 月 28 日第 1999/23 号决议中提出的请秘书长就在国家和国际两级为防止和控制与计算机有关的犯罪而可以采取的有效措施进行一次研究的请求。报告对该议题进行了初步审查并建议进行更为详细的研究，作为高度优先的事项将研究结果提交预防犯罪和刑事司法委员会第十一届会议审议。报告还建议委员会第十一届会议审议有关采取进一步行动的一系列选择，包括视可能起草一份打击与计算机有关的犯罪的国际文书，以及有关短期战略的各种选择，包括拟定打击高技术犯罪和与计算机有关的犯罪的联合国全球方案。报告还提供了其他有关的国际组织和政府间组织活动的材料，并力求对个别成员国提出的其些关注作出反应。

* E/CN.15/2001/1。

目录

	段　次	页　次
一. 导言	1	3
二. 背景情况	2－34	3
A. 其他政府间组织或国际组织的审议情况	2－12	3
B. 联合国的活动	13	4
C. 计算机和高技术犯罪的性质：初步分类	14－29	6
D. 评估计算机和高技术犯罪的范围和及其造成的损失	30－34	8
三. 结论和建议：制订预防和控制计算机和高技术犯罪的全球政策	35－55	9
A. 将高技术和计算机犯罪作为一个独立主题处理的必要性	35	9
B. 援助发展中国家的必要性	36－39	9
C. 考虑采取国际、国家和私营部门措施的必要性	40－41	10
D. 联合国的作用	42－49	10
E. 详细研究的要素	50	11
F. 关于计算机和高技术犯罪进一步工作的方案和具体建议	51－55	12

一. 导言

1. 涉及现代计算机、计算机网络和电信技术的犯罪活动问题仍然是成员国刑事司法和执法部门面临的一个严重挑战。如下文所示，可将该挑战视为由若干不同内容构成。

(a) 挑战是全球性的。在过去，现代技术的大多数使用者，因而也可说大多数罪犯和受害者，都在发达国家。为确保全球信息社会成为支持发展的一个因素，而不是妨害发展的另一个障碍，向发展中国家推广使用现代技术已被确定为一个重大优先事项。[1]发展中国家很容易受到计算机和电信犯罪的影响，如果这些国家无法参与控制犯罪政策的拟订和执行，则可能会因为预防犯罪或安全技术而被排除在使用计算机或通信网的机会之外。

(b) 挑战是动态型的。由于新技术的迅猛发展，在犯罪方面的创新做法也发展得很快，技术的全球性造成新的犯罪方法的迅速传播。因此，尤其在技术资源有限的国家，为了能随时在国内和国际上作出反应而对技术的合法发展和在犯罪方面的创新做法进行监督具有至关重要的意义。该进程主要是由技术发展推动的，因而是无止境的。

(c) 挑战是多学科性的。计算机和电信网络技术的发展象征着从涉及劳作和初级商品的社会活动与经济活动向涉及纯信息或知识的社会活动与经济活动的重大转变。这就在人权、可持续社会经济发展等领域产生了重大的影响。将控制犯罪作为这些议程的内容之一是十分重要的，反之亦然。信息技术和计算机与电信网的结构也大体上是私营部门发展的产物，拟订措施打击高技术犯罪和与计算机有关的犯罪必须考虑到商业上的可行性和有关技术在经济上的竞争力等因素。

二. 背景情况

A. 其他政府间组织或国际组织的审议情况

2. 审议这一问题的论坛的数目的增加体现了各国对该问题的性质和规模及在国际上采取有效措施解决该问题的必要性日益关注。

1. 欧洲委员会

3. 欧洲委员会即将完成电脑犯罪公约案文的起草工作，[2] 该公约所处理的是与对系统进行干扰、擅自存取、电子舞弊伪造、令人厌恶的内容及知识产权犯罪等有关的刑事犯罪。案文草案涉及到调查权，包括对通信进行追踪，搜寻、截获并保留电子证据。草案还将界定司法互助和其他形式的国际合作的基本条件与固定的标准。公约如果能顺利完成，标志着为订立打击与计算机有关的犯罪的国际综合文书而作出的首次尝试。各方对已经完成的案文草案反应不一。尽管许多人认为某些比较困难的问题还未得到解决，但总的来说，各国政府，专家和执法机构都将草案视为一个新的积极步骤。许多利益集团认为，不应对国际网络进行管制，这些利益集团攻击该文书是企图在牺牲个人的隐私和其他权益的情况下扩大国内执法权。

4. 关于文书案文的谈判是由电脑空间犯罪问题专家委员会进行的，该委员会是在早些时候对该问题进行了若干研究后于 1997 年 2 月设立的。[3]除了委员会的正式成员外，加拿大、日本和美利坚合众国的专家也应邀参加了会议的讨论，其他国家在谈判期间也参加了会议的讨论。委员会在其于 2000 年 12 月期满的任务授权的范围内先后编写了 25 份案文草案。最后案文已提交给欧洲委员会议会。还将于 2001 年 6 月将其提交欧洲犯罪问题委员会审查，并在得到核准的情况下送交给欧洲委员会部长委员会通过。

2. 8 国集团

5. 经 1995 年 6 月在加拿大哈利法克斯举行的最高级会议上对跨国犯罪所产生的问题进行讨论后，7 个主要的工业化国家与俄罗斯联邦(8 国集团)设立了里昂跨国有组织犯罪问题高级专家组，其中包括与计算机有关的犯罪的专家分组。该分组自 1997 年以来定期举行会议，并提出了若干倡议。该分组所研究的主要问题是跨国界电子查询所造成的问题，通信追踪以及在政府和有关的私营部门之间进行合作的必要性。

6. 8 国集团于 1997 年 12 月通过了有关电脑犯

罪的 10 点行动计划，该行动计划包括对立法进行审

查、采取措施确保能够有训练有素而且装备精良的执法人员、在商定司法援助协议时审议计算机犯罪问题、审议保留电子证据并在外国刑事诉讼中提供这类证据的方法、加强与业界的合作、关于计算机安全的司法标准和其他技术标准、在法律诉讼中使用电子证据等。[4]

7. 1999 年，8 国集团通过了执法机构寻求查阅外国储存的电子数据所应遵循的某些初步的基本原则。[5]8 国集团一般认为，如果数据是公开提供的，例如在开放性网址的情况下或者已获得依法有权查阅并披露数据的人的同意，就可随意查阅这些数据。对没有公开提供的数据，查询者便会遇到困难。如果他们无法很快复制数据，罪犯通常就会将数据删除。如果他们未首先征得所在国的准许而复制该数据，就会产生与所在国主权和对与被截获数据有利害关系的人的权利的保护有关的严重问题。8 国集团所商定的原则涉及到要求加快提供司法互助。将要求数据所在国立即采取步骤以便在得到更多的正式援助之前对这些数据进行保护，以确保能截获这些数据并将这些数据披露给提出请求的国家。这样使用有关司法互助的较为传统的程序和保障措施就可成功地向提出请求的国家传送数据。

8. 关于在计算机网络上对通信进行追踪的基本原则的问题，也在审议之中。大多数服务供应商都保留了电子邮件等通信的来源地和目的地的电子记录，但只是保留为期有限的一段时间。在绝大多数国家，只能通过使用经司法审查的搜寻和截获活动查寻可用于对通信进行追踪并查明所涉系统用户的记录。就对绝大多数国内通信进行追踪而言这并不构成严重的障碍，但如果涉及到跨国通信，由于就对通信进行追踪还需要通过司法互助的渠道提出请求，因此延误会增加。手段巧妙的罪犯了解这一问题，因此这些罪犯会利用这一点，通过在来源地和目的地之间许多不同的国家传输其通信或通过缺乏顺利进行追踪所需要的法律或基础设施的国家传输通信，以便掩盖其通信的实际来源地或目的地。

9. 为便利在跨国情况下各执法机构迅速进行合作，里昂集团建议在各国设立联系网，从而可每周 7 天，每天 24 小时随时待命协助进行有效的调查。该网络最初由 8 国集团的成员国组成，但目前已扩大到包括 19 个国家，具体操作已转交国际刑事警察组织(刑警组织)负责。

10. 为了使政府和私营部门集聚一堂共商大事，8 国集团与业界举行了若干次有关合作的会议。[6]总的来说，业界代表包括开发计算机和电信硬件、软件和其他基础设施元件的公司以及向个别用户提供服务的公司。讨论中审议了与各家公司同执法机构进行合作的意愿和能力、通过让客户了解情况预防犯罪的必要性、将安全成分纳入新开发的技术等有关的问题。

3. 其他国际组织或政府间组织

11. 其他政府间组织和国际组织还将高技术犯罪和与计算机有关的犯罪问题作为一个单独的议题并结合洗钱和跨国有组织犯罪等其他与犯罪有关的因素进行了审议。英联邦是在 1998 年开始审查这些问题的，在 1999 年 5 月英联邦司法部长的一次会议上已将该议题列入议程。这次会议设立了计算机和与计算机有关的犯罪问题的专家工作组，以便为英联邦国家起草示范立法，但有关这一项目的工作被推迟到订立欧洲委员会电脑犯罪公约以后进行。2000 年 7 月又重新开始工作，目前示范立法草案正在起草之中。英联邦还着手将国际上有关这方面的新情况的材料散发给其成员国，对英联邦处理逃犯及进行司法互助的计划进行审查，以确保这类计划能够将种种必要的合作扩大到高技术犯罪的新领域。

12. 刑警组织也十分活跃，设立了有关信息技术犯罪的一系列区域工作队。刑警组织所进行的研究和编写的材料常常能够反映执法部门的需要和关注。用来培训调查人员的材料包括适用于初次从事调查的人员的手册及更为全面的计算机犯罪手册，该手册载有适用于资深调查人员的最佳做法和方法。刑警组织还清楚有必要使用高技术媒体向执法机构传播信息，该组织为此目的而设立了一个万维网址。刑警组织负责维持最初由里昂集团设立的联系网最新名录。刑警组织计划尤其在执法培训方面开展进一步的活动，它将对其他国际组织的活动进行监测或参与这类活动，以便交换信息并避免工作重复。

B. 联合国的活动

13. 联合国继续对与计算机和电信技术有关的犯罪问题进行认真的研究。除根据经社理事会1999年7月28日第1999/23号决议进行的本研究外[7]已采取下述行动处理这一问题：

(a) 大会1990年12月14日第45/109号决议和经济及社会理事会1996年7月23日第1996/11号决议促请会员国使用现代计算机技术更为切实有效地管理刑事司法活动和信息系统。1990年8月27日至9月7日在哈瓦那举行的第八届联合国预防犯罪和罪犯待遇大会建议拟订一项关于刑事司法系统电脑化的国际文书。[8]第九届联合国预防犯罪和罪犯待遇大会期间举行的为期两天的讲习班讨论了这一问题，该讲习班注意到，为及时跟踪这种新形式的犯罪电脑化是有必要的，但是有与会者对隐私权、人权和国家内部及国家之间系统的相互可操作性表示关注。该讲习班还注意到有必要提供以财政资源和技术专长为形式的技术援助。[9]总体上说，该进程的重点是在管理刑事司法和在收集统计资料方面使用计算机的情况，而不是将计算机网络用作一种调查手段或业务工具。最近又将在控制犯罪方面加强使用现代技术的条文纳入了《联合国打击跨国有组织犯罪公约》[10]电子分发文件在谈判进程中发挥了重要作用；

(b) 第八届预防犯罪大会还审议了与计算机有关的犯罪本身的问题，[11]建议采取有关下述方面的一系列措施：

㈠ 修订有关国内犯罪、调查程序、证据规则、没收或赔偿、司法互助和引渡等条款，以便确保能将这些条款适用于涉及与计算机有关的犯罪的情形；

㈡ 提高计算机安全并改进预防犯罪的其他技术措施；

㈢ 在调查、起诉和裁定与计算机有关的犯罪的案件方面对公众进行教育并对官员进行培训；

㈣ 拟订并传播在使用计算机系统方面的道德规则；

㈤ 拟订政策保护计算机有关犯罪的受害者，包括采取措施鼓励举报这类犯罪；

(c) 根据第八届预防犯罪大会在其第9号决议中的建议，联合国于1994年出版了预防和控制与计算机有关的犯罪的手册，[12]供调查人员和政策制定者使用，这份手册已通过因特网广为散发；

(d) 与计算机有关的犯罪问题也已列入2000年4月10日至17日在维也纳举行的第十届联合国预防犯罪和罪犯待遇大会的议程。联合国亚洲和远东预防犯罪和罪犯待遇研究所组织举办了专门讨论这一议题的为期一天的讲习班。[13]该讲习班由四个小组分下述议题进行讨论：与计算机有关的犯罪的犯罪学问题；与在计算机网络上进行查找和缉获有关的问题；与在计算机网络上对通信进行追查有关的问题；执法机构与计算机行业和因特网行业之间的关系。在这一领域的主要专家向与会者简要介绍了当前的问题和欧洲委员会、8国集团和其他论坛所进行的讨论取得的进展情况。除国家派代表与会外，还有若干行业的代表参加了该讲习班。该讲习班作出了若干建议，包括吁请在政府与行业之间加强合作，提高在追查罪犯方面的国际合作，联合国就提供技术合作和援助采取进一步行动。[14]

(e) 由第十届联合国预防犯罪和罪犯待遇大会通过并得到大会2000年12月4日第55/59号决议核可的“关于犯罪与司法：迎接二十一世纪的挑战的维也纳宣言”[15]也涉及到高技术犯罪和与计算机有关的犯罪问题。在维也纳宣言第18段，成员国决定就预防和控制计算机犯罪制定着眼于行动的政策建议，并承诺致力于增进各国预防、调查和检控高技术犯罪及计算机犯罪的能力。宣言请预防犯罪和刑事司法委员会在顾及其他论坛已经进行的工作的情况下着手制定这些政策建议。大会2000年12月4日第55/60号决议随后请委员会继续审议维也纳宣言及第十届预防犯罪和罪犯待遇大会报告中所载的结论和建议，并请秘书长与会员国协商拟订行动计划草案，供委员会第十届会议审议；

(f) 除参与筹备第十届预防犯罪和罪犯待遇大会期间所举行的与计算机网络犯罪有关的讲习班外，联合国亚洲和远东预防犯罪和罪犯待遇研究所举行了一系列会议和讲习班，以查明问题并确定以后活动的议程。该研究所就与计算机有关的犯罪问题对成员国进行了调查，调查结果即将公布，它目前还在对联合国和参加第十届预

防犯罪和罪犯待遇大会讲习班期间的个人所使用的材料进行编纂并计划予以公布。其今后的计划重点是拟订并分发用于调查和检控与计算机有关犯罪的实际资料；

(g) 委员会第十届会议收到秘书长关于“执行《关于犯罪与司法：迎接二十一世纪的挑战的维也纳宣言》行动计划草案”的报告(E/CN.15/2001/5)。秘书长的这份报告也讨论了高技术和计算机犯罪问题，并包含一系列可供采纳的政策建议和具体措施，以便提高国内和国际各级预防、调查和起诉这种犯罪的能力。这些建议和措施依据的是本报告中讨论的材料；

(h) 大会 2000 年 12 月 4 日第 55/63 号决议注意到为打击非法滥用信息技术作出的努力的价值。这种努力包括下列内容：消除犯罪者的庇护所；国际案件的执法合作；交流信息；人员培训与配备；保护机密；保存并快速调取与犯罪调查有关的数据，维持适当的司法互助制度；提高公众对问题的认识；设计能预防犯罪和便利调查的信息系统；在考虑到保护个人自由和隐私权的情况下维护政府打击非法滥用信息技术的能力。大会还决定继续将非法滥用信息技术的问题列入第五十六届会议议程；

(i) 大会 2000 年 11 月 15 日第 55/25 号决议通过了《联合国打击跨国有组织犯罪公约》及两项议定书(第 55/25 号决议附件一至三)。该公约不适用于不涉及严重犯罪的案件，不适用于不涉及有组织犯罪集团的案件，也不适用于所涉任何犯罪不具跨国因素的案件，[16] 不包括某些电子犯罪。但是，该公约适用于犯罪者利用计算机或电信网络支持较传统形式的跨国有组织犯罪的案件。第 29 条第 1 款(h)项特别要求拟订国内措施和技术援助，打击借助计算机、电信网络或其他形式现代技术所实施的跨国有组织犯罪；

(j) 《公约》通过之后，又举行了一次题为“无国界电脑犯罪的挑战”的讲习班。这次讲习班是关于“全球村的法治－主权和普遍性问题”专题讨论会的一部分，是在 2000 年 12 月 12 日至 15 日在意大利巴勒莫举行的《联合国打击跨国有组织犯罪公约》及其议定书高级别政治签署会议框架内举行的。讲习班的议题包括计算机犯罪和其他形式的跨国犯罪，人们越来越认为完全依赖国内法控制这些犯罪已不适当。会议指出，这种犯罪正随着所依赖的技术的扩散而扩展，实施跨国界犯罪也变得更容易了。与会者认为，国家一级的立法和综合性国际文书是解决办法的重要内容，但人们也担心拟订规章有可能为时过早。利用技术警卫等措施、借助教育和拟订使用新技术的道德标准进行预防，也可以在一定程度上解决这个问题。讲习班还建议，电脑犯罪可以分为以下基本类别：未经授权访问计算机或计算机系统，销毁或更改数据，干扰计算机或计算机系统的合法使用，盗窃有形财产，以及通过欺诈获取价值。

C. 计算机和高技术犯罪的性质：初步分类

14. 高技术和计算机犯罪的现象要求人们对全新的一些犯罪进行鉴定并修改现有一些犯罪的定义，以便确保其中包括对新技术的滥用。必须研究有害行为的新形式，以便确定作为一种对策刑法的适用是否适当；究竟是否应该把有关行为定为一种犯罪。国际上对于最严重和最有害行为的实质核心正在形成共识，但是对有些领域，仍然是只有一些国家而不是所有国家认定是犯罪。像擅自复制软件或数据这样的知识产权问题和被称作是冒犯性内容的问题，就是两个主要的例子。

15. 利用新技术从事犯罪活动已经形成全新的犯罪形式。在其他情况下，罪犯采取趋利避险的新方法实施较传统形式的犯罪。第三种犯罪活动基本类型是罪犯较一般地使用技术来进行犯罪活动的组织和联络和逃避监视。建议的其他基本分类领域包括根据下述情况进行的分类：是否罪犯是为经济或物质利益或其他动机而实施犯罪；是否犯罪涉及针对计算机或通信系统或为危害他人而使用这些技术实施的犯罪。

16. 现把高技术和计算机犯罪的基本类型列述于下。

1. 以技术及其用户作为攻击对象而实施的犯罪

(a) 擅自进入计算机或计算机系统

17. 在大多数情况下，出于侵犯合法用户隐私权的考虑，擅自进入计算机或计算机系统被看作是

一种犯罪，因为合法用户的数据可能被检索，擅自进入往往还伴随着其他违法行为或对系统合法使用的干扰。

(b) 擅自使用计算机系统

18. 擅自使用计算机系统和擅自进入计算机系统是同时发生的行为，因为要想进入计算机就必须使用计算机系统。然而一旦进入计算机系统，便也使用计算机系统实施其他犯罪或掩盖犯罪者的真实身份。擅自使用通常被作为一种犯罪，因为计算机

时间和设施的使用是一种珍贵的商品，而罪犯没有为此付费，并且在有些情况下，合法付费的用户却被剥夺了这种使用权。

(c) 擅自阅读、复制或存录数据

19. 正像一般的偷盗一样，擅自阅读、复制或存录数据的危害在于受害者损失价值，而罪犯则不正当地获得价值。然而就数据情况而言，这些方面是不相连的，因为数据可以复制而不消除。此一行为也可作为侵犯隐私权的一种形式加以刑事定罪。

(d) 制作或传播有害程序

20. 计算机病毒、虫和其他程序，干扰系统运作，破坏计算和储存能力。在大多数情况下，此种程序还利用电子邮件或传递受污染的软盘来扩散，因此一旦程序发送出去，罪犯便很快失去对所造成损害范围的控制。许多有害程序还对数据造成实际的损害，消掉或破坏文档。所造成的损害可能是巨大的，这种损害在于系统运作停止，有价值的数据丧失，消除这种有害程序和恢复系统运作耗费资源。

(e) 故意破坏他人计算机

21. 擅自进入他人计算机的罪犯在企图使用系统或掩盖进入计算机这一事实时可有意或无意地进行破坏。经许可进入有关系统的内部人员在有些情况下也可能实施此种犯罪，此种类型的犯罪包括实施攻击切断服务，即罪犯擅自进入大批联网的计算机，通过这些计算机以任意数据“轰炸”目标系统，致使受到攻击的计算机超载并造成停机。这可能是简单的故意破坏行为，或者可能被用作一种遮眼术，通过使技术保障机制失效来掩盖其他犯罪。像病毒这样的有害程序也可被用来实施特定的故意损坏或破坏行为，但能够与罪犯的直接行为分离开来，因为病毒一旦传播出去，通常便会造成肆意的破坏后果。

2. 利用计算机或通信技术实施的常规犯罪

(a) 涉及冒犯内容的犯罪

22. 涉及冒犯内容的犯罪是利用计算机系统制作或者传播应该受到刑事处罚的图像、文件或其他信息。不同国家加以刑事定罪的各种内容类型之间互有不同。大多数国家目前对制作或传播儿童色情文学均加以刑事定罪，但是对于什么材料视作淫秽、色情、诽谤或煽动仇恨看法就不那么一致了。保护人权的宪法原则，包括言论自由，限制了许多国家可对某些形式内容加以刑事定罪的程度。

(b) 与互联网有关的诱拐

23. 恋童癖患者已开始利用互联网作为一种在不暴露自己真实身份的情况下同儿童进行联系和接触的一种方法。对话从电子聊天室开始，一旦取得信任，罪犯便安排亲自会面并诱拐受害人。已有若干罪犯被在互联网上装作儿童的执法人员逮捕。在有些情况下，罪犯诱使受害者删去记录他们谈话的文档以掩盖诱拐证据。

(c) 诈骗

24. 诈骗犯罪类包括大部分这样的犯罪：以电子手段误导划拨资金的去向，或者向技术使用者提供假信息以骗取他们的资金或资产价值。此种犯罪可能是由雇员这样的内部人员实施的，也可能是由擅自进入私人系统或在公共系统上传播假信息的外部人员实施的。随着电子商务的扩大，预计诈骗和其他经济犯罪将会大量增加。在这一领域一个越来越严重的问题是利用技术操纵金融市场。

(d) 工商间谍活动

25. 各公司越来越依赖计算机系统制作和传播信息也已使得它们成为工业间谍活动的目标。进行此种间谍活动的方法可以是从外部擅自进入计算机系统，或外部人员利用技术搜集有价值的信息并把信息秘密地传送给竞争者。

(e) 知识产权犯罪

26. 新技术储存、传送和复制信息的能力使擅自复制信息和使用信息成为令人关切的一个主要领域。然而并不是所有国家都把此种行为作为刑事事项论处。有些国家将之作为直接有关当事方之间的民事事项处理。

(f) 赌博

27. 小规模电子商务基础设施的发展也已使得利用互联网进行赌博成为可能。当在赌博为合法的法域的网址被赌博为犯罪的法域的赌博者利用时，便涉及了刑法问题。除了道德方面的考虑以外，还往往对赌博加以规范管理以创造税收收入，确保进行监督以不让有组织犯罪参与进来，并保护赌博者免受不公平的游戏遭遇。最近，还把利用互联网进行赌博看作是进行洗钱活动的一种可能手段。

(g) 洗钱

28. 利用计算机网络进行电子商务和其他商业活动的情况日益增加，预计这将为洗钱活动开辟众多机会。一般来说，这些技术可以使罪犯隐蔽其真实的身份和所处地点，能够通过利用外国帐户或者多个法域来钻不同法域的空子，并利用像加密这样的技术来掩盖其交易的真实性质。在有些情况下，可能也会涉及像赌博或诈骗这样的其他犯罪。[17]

3. 利用技术支持其他犯罪活动

29. 一般地说，现代计算机和电信网络以及其他此种技术为犯罪组织提供了与向合法商业提供的同样好处。这些好处包括快速、可靠、费用低廉的全球通信。在大多数情况下，这种通信比传统的方法更安全，更难以从外部截获或监视。网络的性质和传送数据较高的速度和数量增加了执法机构截获个人通信的固有困难。专门的安全保障产品像防火墙和加密文件等，就像它们保护合法通信一样同样有效地保护犯罪通信免受截获或干扰。网络技术在某些情况下还可支持一些全新形式的犯罪组织。最常列举的例子是恋童癖患者罪犯，他们可以找到彼此并共赏儿童色情读物或作品而仍保持不透露自己的真实姓名，并可能以犯罪组织现有概念或定义以外的方式进行合作。较常规的犯罪组织也可找到物色其他区域或国家犯罪者并同其进行合作的新机会。

D. 评估计算机和高技术犯罪的范围及其造成的损失

30. 因为计算机和电信网络在范围上已经扩大，在技术上也更完善和先进，所以使用这种网络的人数和依靠这种网络的程度都大大增加。秘书长在提交联合国千年大会的一份报告中指出，互联网自九十年代初开始到 1998 年，其用户达到了 1.43 亿；到 2001 年，预计上网的人数将达到 7 亿。电子商务是较近期出现的现象，到 1996 年，其价值已达到共计 26 亿美元，到 2002 年，预期将超过 3 千亿美元。[18] 现在几乎还没有关于高技术或计算机犯罪的全面统计资料，但是传闻的证据和现有的统计资料显示，随着网上潜在罪犯和受害者的人数日益增加，此种犯罪的程度也正在增加。[19] 犯罪活动的范围看来也在不断扩大，因为技术创造了新的犯罪机会，罪犯找到了利用新的犯罪机会的新方法。目前特别令人关注的是，电子商务和支持电子商务的基础设施的迅速扩展，可能与之伴随的将是与计算机有关的经济犯罪如诈骗、操纵金融市场和洗钱等犯罪的相应增加。

31. 因为对网络依赖程度的增加，刑事犯罪的潜在危害也在增加。大多数工业化国家对网络的依赖程度最大，现在它们都认为计算机和电信网络及其支助基础设施是恐怖主义活动的潜在目标。为战略或政治原因而攻击计算机系统的情况现在仍然很少，但是其他动机的犯罪行为经常造成大规模的损害，其危害程度有时完全超出了罪犯所实际预期的程度。最近的例子包括 1999 年 3 月制作和传播的“Melissa”（美丽莎）病毒，该病毒仅对美利坚合众国造成的直接损失就超过 1

千万美元；2000 年 5 月的“I love you”（我爱你）病毒，估计造成的损失为 70 亿至 100 亿美元，全世界受影响的计算机多达 4,500 万台。另一次事件是一系列切断服务的袭击，以大量毫无意义的数据“轰击”网址，不足两小时便使 1,200 个网址关闭，其中包括一些新闻组织和电子商务网址。在某些事件特别是在某些涉及病毒的事件中，如果其他罪犯复制病毒，并作些改动以对用户或对过滤软件蒙蔽病毒的性质，然后进一步扩散和传播，那么所造成的损失常常会更大。[20]

32. 实际的损失是难以量定的，但是包括修理系统和软件的直接费用、用户进入系统或利用服务的损失以及相应受到的损害、有价值数据的损失和网址运作收入的损失等。由于有此种犯罪，因此便需要开发和采取安全或其他防范措施，这是一项附加的成本要素。此种犯罪的全面增加和某些有关犯罪的惊人性质也产生了要求增加刑法控制、加重处罚和软硬件生产商及向客户提供网络准入的公司必须采取技术防范措施等的巨大而难以预测的政治压力。此种事故造成的进一步的隐性损失是对计算机犯罪的恐惧，此种恐惧可能削弱对计算机技术的使用，使发展中国家的政府和人民不敢最有效地使用这种技术。

33. 对犯罪本身的性质和范围进行可靠分析的研究也是困难的。对于某些形式的行为究竟是否应该加以刑事定罪，如果应该加以刑事定罪，应该如何对这些行为加以界定和分类，这些问题都仍待解决。任何分类办法也都部分地视有关的技术而定。这些有关的技术也存在着如何界定的问题。随着计算机网络使用的扩大和较传统的系统采用数字技术，像计算机网络、有线广播系统、移动和传统电话系统这样的技术正迅速地变得难以区分。这方面当前的一个例子是称作 palm-pilot（掌上向导）的装置，这种装置集移动电话、网络广播和计算机网络服务于一身。这在可预见的未来将对研究人员、政策分析人员和法律起草者提出挑战，并已导致需要使用技术中性的概念和语言，以便确保避免出现漏洞和不一致的情况。

34. 收集准确的统计数据也提出了若干问题，即使在明确确定了犯罪的情况下也是如此。大多数专家认为，人们对普通形式的计算机犯罪报案量大大不足，因为受害者可能没有认识到他们已经受害，没有认识到有关行为是一种犯罪，可能因为难堪或者为了公司的信誉而决定不予告发。像病毒传播这样的犯罪造成的大规模普遍受害现象还引起其他一些问题，因为受害者简直是不计其数，难以逐一清点，还因为此种程序在罪犯被捉拿归案并受到处罚很久之后仍可能继续使更多的人受害。使收集和比较国家犯罪统计数据复杂化的另一因素可能是，根据定义，计算机跨国犯罪是至少在两个国家，有时是在许多国家实施的，或造成后果，从而可能会出现多次报告或者根本就没有报告的现象。

三. 结论和建议：制订预防和控制计算机和高技术犯罪的全球政策

A. 把高技术和计算机犯罪作为一个独立主题处理的必要性

35. 本报告中所谈的犯罪活动由一些基本技术相互联系在一起并具有许多共同的特点。有些犯罪活动是由技术本身产生和界定的新活动，而有些犯罪活动则是受这些技术严重影响的较常规的犯罪形式。许多根本政策问题，如力求在人权和调查权力之间以及在国内利益和国际利益之间的适当平衡，对所有形式的高技术和与计算机犯罪都是共同的。在更实际的层面上，侦查员和公诉人所面临的问题，如找到和确定罪犯、扣押、保存和鉴定计算机或电子证据以及在法庭使用这些证据，大体上都是一样的，不管犯罪本身的性质如何。因此建议，为研究和任何未来的多边讨论目的，把这一领域作为一个独立的主题对待。然而，还应该指出，许多正在出现的令人关切的领域，例如传播儿童色情文学、诈骗和其他金融犯罪，将也需要熟悉有关罪犯和其具体方法的专家的投入。

B. 援助发展中国家的必要性

36. 关于计算机系统和计算机犯罪的许多政策辩论迄今是在高技术部门相当发达的国家内部及其彼此之间进行的。这些国家有很多利益可能受到了计算机犯罪的有害影响。它们有大量的公私营部门对此种技术的投资，也有越来越依靠使用计算机网络的人口。然而，也涉及发展中国家的利益。新技术是促进发展中国家社会、经济和其他利益的一个重大机会，[21] 但是如果发展中国家不能够充分利用这一机会，新技术也可能加大

现有的差距。在这方面，如果发展中国家不能有效地参与讨论，计算机犯罪和发达国家及高技术工业打击此种犯罪的努力可能会成为发展的一种障碍。为了充分确定和阐明发展中国家的利益，为了查明在这一过程的各个阶段的技术和其他援助需要，为了制定在所有社会可行的预防和控制犯罪的措施，并为了充分有效地执行这些措施，需要发展中国家的投入。

37. 将需要几乎普遍地执行有效的犯罪控制措施，因为犯罪分子可以利用新技术而几乎毫不受传统罪犯所受到的那种国界限制。在传统罪犯受到种种因素（如地理距离、海关控制和需要同其受害者实际进行接触等）限制的地方，电子罪犯可以逍遥法外，从远距离或者通过任何缺少适当立法或缺少实施此种立法的意志或能力的法域进行活动。广泛的代表性和有效的参与对确保制定的政策和措施对所有国家都切实可行，确保所有国家愿意并能够有效地执行这些政策和措施将是至关重要的。

38. 确保有效的参与在这一过程的一些阶段将需要发达国家援助。在开始阶段，为了评估发展中国家对技术本身的兴趣，评估此种兴趣如何受到计算机犯罪和控制这种犯罪的努力的影响，将需要发展中国家的投入。因此，最早期阶段的援助特别重要。一些国家已积极地参与了一段时间，但是，对许多国家来说，这些技术还仍然是陌生的，并且对将出现的技术、法律和政策问题还一直没有很多的考虑。即使在帮助下，获得这种专门知识也是需要时间的。因此重要的是，此种援助应尽快开始，并且要保持足够长的时间，以便确保有效地参与所有阶段的讨论。在较长期内，为了保持运作的效能，还将需要经常性的技术援助。技术和依赖技术而实施的犯罪继续在发展变化，这一事实将要求全球进行努力监测新的发展变化，制定有效的对策，并尽快地传播这些新的变化情况和有效的对策，以使执法机构和公诉人即使不走在罪犯的前面，也要不落在罪犯的后面。

39. 因此建议立即作出努力对请求技术援助的发展中国家的技术援助需要进行评估，并尽快地满足这些需要。评估工作应该结合这些国家的电子发展战略，结合全球将技术用于计算机和电信系统以及预防犯罪日益增加的情况来进行。评估工作还应该在与掌管这种技术的私营部门公司协商，并在可能时在它们的帮助下予以进行。从全球角度来讲，评估的重要内容将包括确定关键技术和优先重点。

C. 考虑采取国际、国家和私营部门措施的必要性

40. 专家们普遍认识到，由于现代计算机和电信技术的国际性，已出现了跨国和多国犯罪的新形式。网络空间概念和一个地域的犯罪行为可很容易地影响到另一地域这种情况，使国家和国际措施相结合变得至关重要。没有此种结合，针对犯罪采取的对策便可能是不起作用的，并可能产生意想不到的不利后果，例如使人们不敢使用这些新的技术，损害人权，造成工业竞争力或发展不平衡等。

41. 工业在发展和维持这种技术中所起的突出作用也使得把公营部门的措施和私营部门的措施结合起来非常重要。私营部门一般都支持对犯罪进行有效的控制，但是它们的动机往往出于商业的考虑，而不是政治的考虑，其方法是技术性的而不是法律性的，因此均需要加以协调，在可能时应和政府的国内和国际努力结合起来。

D. 联合国的作用

42. 作为联合国千年大会筹备工作的一部分，曾吁请经济及社会理事会考虑信息技术在发展和国际合作领域中的作用。经社理事会得出结论认为，新的信息技术的发展和传播推广基本上是自行维持的。但是联合国可以很多方式协助推动这一过程。[22] 这包括援助发展中国家跟上新的发展，特别是在市场驱动发展不大可能满足其需要的区域或主题领域；援助它们开发能够带来社会效益但不一定具有商业可行性的特定技术。更一般地说，经社理事会认为，联合国的关键作用在于使这一过程中的利害攸关者，其中包括政府、学术机构和私营部门公司，建立共识和伙伴关系。建立共识的目的是汇集必要的专门知识和资源，以便确保每个人都将有利用新的信息技术并从中受益的机会。

43. 高技术和计算机犯罪是阻碍参与经社理事会称之为全球知识经济并争取从中受益的一个重大障碍。建立共识的任务在控制犯罪领域也同样重要。在拥有重大投资和依靠此种技术的国家

中，对有效控制犯罪措施的必要性也已有了基本的共识，但这仅仅是这一过程的开始。制定具体的措施将需要评估和综合考虑许多经济、社会、文化和法律问题。制定和执行许多控制犯罪措施，要能结果证明行之有效，就必须获得接近于普遍共识的支持，以及几乎每个国家的技术能力达到适当标准。这种共识不仅应该扩及国家与其政府，而且还应扩及大型的多边私营部门。

44. 近期内，重要的是应该收集和传播准确的资料，了解问题的性质和范围以及会员国对解决问题而应做些什么所持的看法，以便使各国考虑各种备选办法，指导联合国应如何进行工作。本文件中所说的政府间组织和一些政府已经开始一般性或结合重大跨国犯罪个案而同其他国家相互交流所获得的立法、检控、技术和执法专门知识。这一工作在范围和涉及的国家数目上均已扩大，但是为此，将需要对现有需求和满足这些需求的现有资源作准确的评估。

45. 因此建议，支持药物管制和预防犯罪厅国际预防犯罪中心对问题进行更详细的研究，以便向预防犯罪和刑事司法委员会第十一届会议提交研究报告。可能的研究主题事项将在下文进一步讨论，但至少应包括调查会员国的基本需要；是否愿意通过提供财政资源和技术专门知识进行援助；会员国对于应如何针对问题制定全球对策以及此一对策应采取什么形式的意见等。

46. 还建议应设立一个开放性政府间专家组，审查上述研究报告并编写备选方案和建议供委员会第十一届会议审议和采取行动。正如上述所指出，在这一过程的所有阶段，各种国家的参与是非常重要的。该专家组的基础应该尽量广泛，特别是应该包括发展中国家的代表。因此建议，其他国家应该尽可能最大程度的以自愿捐款来支助此种参与。

47. 还建议一旦调查研究工作完成并取得专家组的意见，应立即设立一个打击高科技和计算机犯罪的全球方案，有关国家应提供自愿捐款建立和支助此一方案。下文 F 节中详细讨论有关建议。

48. 从较长期看，许多专家认为，只有制定一项打击高科技和计算机犯罪的综合性全球法律文书，才可足以建立有效对付跨国与计算机犯罪所必须的开展国际合作的政策、权力、程序和机制。然而，对于如何能很快地制定出此一文书看法却不一。正如上文 B 节所指出，在这一过程的初期阶段需要让各种各样的国家参与进来。还有一些在起草此一文书中必须加以解决的主要问题，例如，与国家主权、司法和其他人权保障和私营部门在促进计算机安全和犯罪控制措施中的作用等有关的问题。就起草这一文书的过程与其内容可能采取的形式而言，在评估各种备选办法时必须考虑到这些问题。一般地说，包含有较广泛而具有约束力的规定的一项文书可能较为有效，但是要花费较长的时间去谈判，许多国家执行起来证明也较困难和耗费时间。在目前阶段尚未得出任何结论，但是建议应该请专家组考虑关于一项国际文书的程序和实质性备选办法，编制建议作为向委员会第十一届会议报告的一部分。

49. 要考虑的另一因素是，高技术和计算机犯罪看来在发生的频度、地域范围和技术复杂性方面均在迅速增加。伴随着新的计算机、网络和电信媒体的迅速发展和扩大，这一过程看来可能要继续下去。此一前景显示，虽然一项全球性的法律文书可能是一个重要的长期应对办法，但是制订较近期的有效措施可能也是必要的。因此建议也请专家组研拟打击高科技和计算机犯罪的全球短期战略的进一步备选方案。重点放在下列领域：总的和针对个案的法律和技术援助；制定诸如收集、保护、鉴定和展示电子证据的技术标准；建立援助请求联络点。在这方面，应考虑到第二节 A 中所述的各组织中正在开展的工作。

E. 详细研究的要素

50. 就目前的知识水平而言，计算机犯罪领域提出的问题远比解决的多。必须进一步进行研究，以界定这个主题，确定受其影响的利益以及影响方式，并且明确将来的政策选择。这项研究至少应包括下列内容：

(a) 应该调查各国对这个问题性质和范围的看法以及可能的国内和国际对策；

(b) 应该向能体现各种工业、法律、社会和经济特色的国家进行咨询；

(c) 既应该考虑国内犯罪也应该考虑跨国犯罪。虽然许多国家认为某些问题纯属国内问题，但是这些技术的性质打破了国内犯罪和跨国犯罪之间的传统界限。研究人员、决策者和谈判代表常常发现难以区分国内犯罪和跨国犯罪。必须采取统筹办法，尤其是在这个进程的初期阶

段；

(d) 应该研究私营部门人士的看法和提供的援助，突出强调下列方面：

㈠ 这项研究应该审查和考虑开发和运用有关技术的行业的看法和投入，包括计算机硬件和软件以及计算机网络和电信网络等行业的看法和投入；

㈡ 这项研究还应该审查有关非政府组织的看法。致力于言论自由和保护个人隐私的组织对于过去试图建立有效的调查权力始终持批评态度，并已形成了对 8 国集团和欧洲委员会在这一领域努力的政治反对力量；

(e) 这项研究应该考虑犯罪控制以外的问题，例如可持续发展，保护隐私，言论自由和其他基本权利，以及商业和其他利益。这些和其他根本利益同技术发展密切相关。计算机犯罪的增加以及各国政府和国际社会为预防和控制这种犯罪作出的努力都可能对其产生影响；

(f) 这项研究应该评估犯罪的程度，既进行一般评估，也在有关统计因素范围内进行评估，例如具体犯罪形式、地理和其他社会或经济状况。现在已经研究了在收集和分析准确统计资料方面的困难。然而，随着对这个领域的技术范围及其中犯罪类型形成共识，应该能提供更加可靠的数据。此外，随着公众提高对所涉行为类型的认识，并认识到这些行为是犯罪或应以犯罪论处，对这种犯罪报告不够的情况应该减少。收集初步数据对于加强政治支持采取有效的国内和国际行动打击这种犯罪也十分重要；

(g) 这项研究应该考虑高技术和计算机犯罪的定义和分类。本报告使用的分类与这一领域的其他工作相同，可以成为进一步研究的基础，但是必须进行更彻底和严谨的研究，以便形成各国政府、利益集团和这一领域专家统一认识的框架。这是早期的一个优先事项，因为需要进行定义和归类，使进一步政策拟定所依赖的统计数字收集和研究做到统一一致。可行的分类必须考虑到几个主要领域的因素，包括以下内容：

㈠ **相关技术**。高技术和计算机犯罪领域的推动力在很大程度上是相关技术的性质和范围，这些技术正在迅速发展和融合。因此，本报告和关于这个问题的其他工作使用了“高技术和计算机犯罪”这个一般性词语。必须进行研究，对涉及的所有技术进行调查，并提出包含所有技术的概括分类方案。此外，还需要更详细地考虑具体的技术发展变化，以及依赖于这些技术的犯罪活动类型。鉴于这些技术发展迅速，所以不仅应该考虑到当前的技术，而且也应该考虑到潜在的发展变化；

㈡ **犯罪者的性质和动机**。实施新技术犯罪的犯罪人员构成了一个比较新的研究领域。传统犯罪者的动机，例如恋童癖者、诈骗犯或国际毒犯，其动机众所周知。对于这些犯罪者如何适应新的技术，必须从计算机犯罪的角度加以研究；

㈢ **犯罪的地域方面**。与传统犯罪相比，地域方面至少有两点重要的差别。首先是两大“地域范围”相互重叠。犯罪者的实际藏身之处及其具体的环境因素十分重要，例如社会、经济或文化条件。然而，影响犯罪特点的电子地域范围，也就是人们常说的电脑空间因素，也十分重要。

F. 关于高技术和计算机犯罪进一步工作的方案和具体建议

1. 可能制订的打击高技术和计算机犯罪的国际文书

51. 一旦研究结束，建议专家小组应就拟订一项打击高技术和计算机犯罪的国际文书是否可行和可取的有关问题和方案，向委员会提出咨询意见。这些问题将包括以下内容：

(a) 可能制定的文书应该是规范性的还是具有法律约束力的。这项文书可以力求对于刑事犯罪、调查权和国际合作机制等问题作出强制规定，也可以仅提供一些准则，协助各国制定有效措施，并促进法律和程序的国际标准化。如《联合国打击跨国有组织犯罪公约》所显示，可以对这两个方案进行折衷，以文书中的一些条款规定具有约束力的义务，而另一些条款则含有较为一般的准则，或由缔约国酌情加以执行；

(b) 可能制订的新文书与《联合国打击跨国有组织犯罪公约》是什么关系。概括而言，该公约可以成为某些条款的先例，而其他条款对于高技术和计算机犯罪这个主题并不适用。例如，该

公约的范围限制于“有组织犯罪”的活动，会把很大一部分高技术和计算机犯罪排除在外，因为这些犯罪是由公约定义范围以外的个人或群体实施的。[23] 因此，这似乎排除了为公约再制订一项针对此类犯罪的议定书的可能性；[24]

(c) 这项文书一旦缔结，如何不断增补更新。如本报告导言所指出，这个领域的特点是技术和有关犯罪活动演变迅速，必须确保统筹国内和国际措施的任何框架能够跟上变化的步伐。选择方案可以包括，将一部分立法权下放给代表缔约国专门成立的一个专家组，随着新的特别问题的出现，利用议定书来处理这些问题，采用技术中性的措辞或其他措施；

(d) 如何在国际文书中考虑到有关利益，例如隐私、言论自由和其他人权以及商业利益。虽然这个主题要求该文书把重点放在控制和预防犯罪上，但在起草文书及其实质内容过程中，还必须考虑到其他利益。

2. 对付高技术和计算机犯罪的短期战略

52. 如上文指出，高技术和计算机犯罪是个紧迫问题，短期和长期也许都需要一致的国际对策。建议这项研究审查近期内可能采取的措施，由专家小组就短期战略拟订建议，供委员会第十一届会议审议。这项战略可以包含下列要素：

(a) 编制并向所有会员国散发有关高技术和计算机犯罪以及可能采取的对策的资料，以便尽快通报那些尚未参与讨论的会员国。拟议进行的研究将是这套资料的关键内容，但还可以提供其他材料，包括下列内容：

㈠ 可以增补和重新印发1994年发表的《联合国预防和控制计算机犯罪手册》；

㈡ 可以出版和散发第十届联合国预防犯罪和罪犯待遇大会期间举行的计算机网络犯罪讲习班的会议记要和材料；[25]

㈢ 可以更广泛地散发其他政府间组织的材料，特别是欧洲委员会、国际刑警组织和8国集团班成立的里昂集团；

㈣ 可以为有关国家的官员举行讲习班、讨论会或情况介绍会，私营部门的代表也可以参加；

(b) 可以更多地提供侦查员和检察官培训材料。联合国没有编制这种材料，但是一些会员编制了，用于培训自己的官员，在一些情况下也用于涉及其他国家的技术援助项目；

(c) 一些国家需要直接技术援助。这种援助可以包括培训法官、检察官、侦查员和技术专家或法医，其中许多人以后可以培训他人。在一些情况下，这种项目可以并入旨在援助各国为发展而获得和利用新技术的比较一般性的发展项目。如上文指出，如果要避免计算机犯罪对发展的有害影响，就必须把预防和控制犯罪确定为这种项目的构成部分；

(d) 应该鼓励在每个会员国成立协调中心或联络点。这包括用于计算机犯罪调查的直接援助的联络点，[26] 但还包括更广泛的联络，目的是收集各国发展变化的资料以及收发来自国际社会的资料；

(e) 必须承诺大量的财政和技术资源。这种援助的形式可以是向联合国预防犯罪和刑事司法基金自愿捐款，或提供专家或材料，支持打击高技术和计算机犯罪全球方案，或联合国的具体项目。由于这些技术使用普遍，以及很容易被任何地方的犯罪者所利用，因此拥有财政或技术资源的国家愿意援助其他国家。开发和运用计算机和电信网络的行业，也有可以利用的财政和技术资源，以及作出贡献的积极性，因为多种形式的计算机犯罪对其产品的商业前景构成威胁。

3. 建立打击高技术和计算机犯罪的全球方案

53. 有证据显示，在研究和制定政策、法律和技术措施方面已开展大量活动，但对这种活动的总体协调却很少。各国活动的范围各不相同。这个问题涉及一些政府间和非政府组织以及联合国的几个机构和部门，是商业公司和非政府利益集团关切的重大问题。人们的注意力以及资源的调拨，往往集中于直接相关的政府或组织所关切的具体问题，因而造成研究的空白或不一致之处。联合国的全球性使其具有独一无二的地位，可以研究和协调这个领域的活动。建议对会员国的需要和看法一旦调查完毕，即设立打击高技术和计算机犯罪的全球方案。还建议有关国家为成立和运作这样一个全球方案提供自愿捐款。

54. 一旦获得这项研究的结果以及专家小组的意见，委员会第十一届会议就应该审议该全球方案可能的工作范围。该全球方案的任务可以包括上文第 52 段阐述的活动以及下列内容：

(a) 查明确定要求援助的会员国并分析其具体需要；

(b) 编制材料，以援助决策者、立法者、执法机关、检察官以及处理国内和跨国案件的其他有关官员；

(c) 收集、汇编和散发其他方面编制的材料；

(d) 在有足够资源可以提供的情况下，向请求援助的国家提供法律、技术和其他援助；

(e) 编制愿意向请求国提供援助的个人和机构所可以提供的技术专门知识清单；

(f) 与联合国其他机构和部厅协调活动，特别是在人权和发展领域，以期酌情在其他方案中纳入计算机犯罪问题，并确保将其他方案的投入也纳入预防和控制犯罪战略的拟订工作；

(g) 同在打击高技术和计算机犯罪领域积极开展活动的其他政府间组织和个别的政府和机构协调活动；

(h) 与非政府利益集团和私营部门公司协调活动，并从公司筹集资金和汇集技术专门知识，作为打击高技术和计算机犯罪全球战略的组成部分。

4. 待审议的实质问题的初步清单

55. 作为短期和长期战略的要素，也必须考虑许多同样的实质问题。根据先前在联合国和本报告所述其他论坛进行的讨论，下列实质问题必须进行审议：

(a) 查明涉及新技术的有害行为并建立新的罪种或修改现有罪种使之成为刑事犯罪；

(b) 拟订关于处理跨国跟踪通信的原则，包括有权获得、保留和披露往来数据；[27]

(c) 拟订管辖故意和非故意跨界电子搜寻的原则；

(d) 拟订关于处理截获计算机网络和类似媒体上传输通信的共同原则；

(e) 评估各种形式数据存储和传输所固有的保密或隐私利益，以根据这些利益拟订关于扣留和截获的程序控制。例如，大多数国家对于执法部门进入开放的网站或网播通信没有什么限制，但是对于扣留来自不那么公开的私人来源的数据则有限制；

(f) 制订关于查明计算机网络或通信服务个人用户的共同标准或做法，兼顾个人隐私和匿名的需要；

(g) 制定调整法医操作和法律证据规则的共同原则，以确保在刑事诉讼中能保留、鉴定和使用计算机证据；

(h) 在制定打击高技术和计算机犯罪的国际政策和措施方面以及在具体案件中执行这种措施方面，制定保护基本权利的共同原则；

(i) 制定管辖数据保密和完好状况的共同原则，并使这些原则与有效控制犯罪的措施的必要性平衡协调；

(j) 为提出请求的国家拟订技术援助方案和材料，并提供经费。需要利用这种方案和材料协助各国有效参与全球政策的制定，并确保国内当局获得适当的培训和装备，能够迅速有效地对于援助调查跨国计算机犯罪的请求作出响应；

(k) 收集、分析和交流有关新技术发展变化、犯罪者及其技俩的资料，以及预防、调查和起诉犯罪的有效方法的资料；

(l) 为执法专家提供培训、装备和资源，确保有能力在国内案件中进行调查和起诉，并能在跨国界案件中与其他国家有效合作；

(m) 有必要评估和澄清私营部门在国内和国际各级的作用及其与政府的关系。需要考虑这种关系的以下具体要素或方面：

㈠ 必须在有效的犯罪控制措施与这些措施的制定和执行所受到的技术和商业限制之间寻求平衡。工业界在新技术的设计阶段就应该考虑到犯罪控制问题，但是执法部门必须认识到，有些措施在技术上也许不可行，或者措施中提出的变化将造成新技术丧失生产力或竞争力。犯罪控制要求不应该影响新技术的基本可行性或竞争能力，但是犯罪和预防犯罪造成的费用必须成为政府和工业界总体成本收益评估的内容，这些费用

应根据容易发生犯罪的技术所产生的收益酌情加以分摊；

㈡ 政府和工业界必须有效合作，尽量扩大收益，减少付出的代价。这包括查明和开发有效的保障技术和其他预防犯罪技术。在开发阶段尽早将其纳入新技术，并在潜在犯罪者有机会获得这些技术之前，使执法部门和检察机构在新技术方面获得培训和准备。有关行业的技术进步使这些行业对于技术援助方案的成败至关重要，甚至是必不可少的。在许多情况下，商业利益本身就足以成为这些行业参加这种方案的理由；

㈢ 必须制订制度和开展行动，支持有效的刑事侦查和预防犯罪，同时考虑到必须保护这些技术用户的隐私和其他权利。例如能够在合理期限内保留通信证据以备调查之需的制度，以及能够识别客户的需要；

㈣ 必须对私营部门在控制犯罪方面的潜在作用进行全球评估。这是许多服务供应商已经面临的复杂问题，他们也同公众一样关心有效的犯罪控制，但是认识到，如果他们替代或取代国家执法机构，会造成危险和困难。工业界面临着相互冲突的压力：新技术采用商业上不可行的安全措施，还是采用影响到客户基本利益的措施。[28] 他们还面临着政府的压力，要他们控制或排除被认为非法或不适当的内容，或协助国家执法机构进行刑事侦查。这些压力提出了复杂的伦理、法律和政策问题，应该在国家和全球各级加以探讨，以期尽可能实现全球一致。

注

1 见“弥合数字鸿沟”，秘书长致联合国千年大会的报告(A/54/2000，第 150 至 167 段)。另见秘书长关于二十一世纪的发展与国际合作：信息技术在以知识为基础的全球经济中的作用的报告(E/2000/52，第三至第五节)。

2 欧洲犯罪问题委员会，电脑空间犯罪专家委员会，“电脑犯罪公约草案”(PC-CY(2000)，草案，第 25 号，Rev.5)，已经上网，网址为 http://conventions.coe.int/treaty/projets/cybercrime25.htm。

3 研究报告所得出的结论载于欧洲委员会建议 R(89)9 和 R(95)13。专家委员会是由欧洲委员会部长委员会在 1997 年 2 月 4 日举行的部长代表委员会第 583 次会议上设立的。

4 见 1997 年 12 月 10 日在华盛顿举行的 8 国集团司法部长和内政部长会议公报附件。

5 见 1999 年 10 月 19 日至 20 日在莫斯科举行的 8 国集团打击跨国有组织犯罪部长级会议的公报，第 17 段和附件一。

6 2000 年 5 月 15 日至 17 日和 2000 年 10 月 24 日至 26 日分别在巴黎和柏林举行了会议。计划于 2001 年 5 月在东京另外举行一次会议。

7 在第 1999/23 号决议第 14 段，经社理事会请秘书长就国家和国际两级为防止和控制与计算机有关的犯罪而可以采取的有效措施进行一次研究，其中包括审查是否应编拟一些手册、准则和建议，并向预防犯罪和刑事司法委员会第十届会议报告这项研究的结论。

8 见大会 1990 年 12 月 14 日第 45/109 号决议和第 45/121 二十一号决议，及《第八届联合国预防犯罪和罪犯待遇大会，哈瓦那，1990 年 8 月 27 日至 9 月 7 日：秘书处编写的报告》(联合国出版物，出售品编号：E.91.IV.2)，第一章，C 节，第 140 页。

9 见 A/CONF.169/16/Rev.1，第 370 至 385 段。

10 见大会 2000 年 11 月 15 日第 55/25 号决议，附件一，第 18 条，第 8 款。

11 见《第八届联合国预防犯罪和罪犯待遇大会…》，第一章，C 节。

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

13 见大会 1997 年 12 月 12 日第 52/91 号决议和 1998 年 12 月 9 日第 53/110 号决议。另见 A/CONF.187/10 和《第十届联合国预防犯罪和罪犯待遇大会，维也纳，2000 年 4 月 10 日至 17 日：秘书处编写的报告》(联合国出版物，出售品编号：E.00.IV.8)，第 161 至 174 段。

14 见 A/CONF.187/L.10，第 14 段。

15 见《第十届联合国预防犯罪和罪犯待遇大会…》，第一章。

16 见《公约》第 2 条(术语的使用)和第 3 条(适用范围)(第 55/25 号决议附件一)。

[17] 经济合作与发展组织（经合组织）洗钱问题金融行动特别工作组最近审查了此种犯罪。见洗钱问题金融行动特别工作组“2000－2001 年洗钱类型报告”（巴黎，经合组织，2001 年 2 月），第 5－18 段。

[18] A/54/2000，第 152 段。

[19] 例如，美国联邦调查局局长在 2000 年 3 月 28 日对美国参议院司法委员会的关于计算机犯罪的一次讲话中指出，1998－1999 年，联邦调查局承办的案件数增加了一倍，从 547 个增加到 1,154 个，但不清楚是否这是由于犯罪的增加还是报告的次数增加，还是二者兼有之。另见 P. Graboski, “Computer crime: a criminological overview”, Forum on Crime Society，第一卷（2001 年），第 40 页。

[20] 美国一个 31 岁的程序员承认制作了“Melissa”（美丽莎）病毒。加拿大一名 15 岁的男孩对与切断服务的攻击有关的 56 项刑事指控俯首认罪。在“I love you”（我爱你）病毒案件中没有提出任何控罪，但据认为，该病毒来自菲律宾。对这些案件曾流传着各种各样的损害估计，但真正的损失可能永远也确定不了。这里的数字是作为一般规模损失的证据和政治上对此种规模的犯罪所造成的威胁关切程度的证据来引述的。

[21] 见 E/2000/52，第三至第五节。

[22] 见 E/2000/52，第 79－99 段。

[23] 见该公约第 2 条和第 3 条（第 55/25 号决议附件一）。

[24] 现有三项议定书都包含有关公约范围和适用的规定，但都根据具体情况稍有改动。公约的许多条款是根据仅适用于涉及有组织犯罪集团的案件起草的，很难适用于涉及个人实施的计算机犯罪案件。

[25] 组织这次讲习班的联合国亚洲和远东预防犯罪和罪犯待遇研究所目前正在编写这些材料，以供出版。

[26] 8 国集团已经开始进行这项工作，并由国际刑警组织开展后续行动。

[27] “往来数据”一词通常是指服务供应商存储的记录电子通讯来源和目的地的数据。这种数据既可以包括最终来源和目的地，也可以包括计算机网络范围内的临时来源或目的地。与其相关的概念是“订户”或“用户”数据，服务供应商可以用来查明个别的客户。

[28] 最近的一例是，法国一家法院命令互联网公司“雅虎”研究技术办法，阻止该公司在法国的用户访问包含纳粹纪念物的拍卖网站。销售这种物品在法国是违禁的，但在网站所在地是合法的。只要在技术上可行，供应商通常愿意采取这种行动，但条件是主管法院或其他公共当局确定内容本身是非法的。