COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

《欧洲条约集》第 185 号

《网络犯罪公约》

2001 年 11 月 23 日，布达佩斯

序言

欧洲委员会成员国及其他签署国，

考虑到欧洲委员会的目标是实现成员国之间更大的团结一致；

确认促进与本公约其他缔约国合作的价值；

深信有必要作为优先事项，特别是通过适当的立法和促进国际合作，推行共同的刑事政策以保护社会免受网络犯罪之害；

注意到计算机网络的数字化、融合和持续全球化带来的深刻变化；

关注计算机网络和电子信息也可能被用于实施刑事犯罪，而与这些犯罪有关的证据有可能被这些网络储存和转移的风险；

认识到国家和私营企业有必要在打击网络犯罪方面开展合作，有必要保护使用和发展信息技术的合法利益；

相信有效打击网络犯罪在刑事问题上需要扩大、迅速和良好的国际合作；

深信本公约对于阻止破坏计算机系统、网络和计算机数据的保密性、完整性和可用性的行为以及对滥用此类系统、网络和数据的行为实为必要，方法是将本公约所述的此类行为确定为犯罪，采用足以有效打击此类刑事犯罪的权力，并通过在国家和国际两级促进对此类刑事犯罪的侦测、调查和起诉，以及通过为快速和可靠的国际合作做出安排；

铭记有必要确保执法利益与尊重基本人权之间的恰当平衡，后者庄严载于 1950 年欧洲委员会《保护人权和基本自由公约》、1966 年联合国《公民及政治国际公约》和其他适用的国际人权条约，这些条约重申人人有权持有见解和言论自由的权利而不受干扰，包括不分国界寻求、接受和传递各种信息和思想的自由，以及有关尊重隐私的权利；

又铭记保护个人数据的权利，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》所赋予的权利；

考虑到 1989 年联合国《儿童权利公约》和 1999 年国际劳工组织《最恶劣形式的童工劳动公约》；

考虑到欧洲委员会关于刑法领域合作的现有公约，以及欧洲委员会成员国与其他国家之间存在的类似条约，强调本公约旨在补充这些公约，以便使针对计算机系统和数据有关的刑事犯罪的刑事调查和诉讼更为有效，并能以电子形式收集刑事犯罪的证据；

欢迎最近的事态发展进一步推动了国际间在打击网络犯罪方面的理解与合作，包括联合国、经合组织、欧洲联盟和八国集团所采取的行动；

回顾部长委员会关于在拦截电信的调查委托书方面实际应用《欧洲刑事事项互助公约》的第(85)10 号建议、关于版权和邻接权领域盗版问题的第(88)2 号建议、关于规范警察部门使用个人数据的第(87)15 号建议、关于保护电信服务领域特别是电话服务中个人数据的第(95)4 号建议，以及有关计算机犯罪的第(89)9 号建议(它为国家立法机构提供了某些计算机犯罪定义的指南)，以及与信息技术有关的刑事诉讼法问题的第(95)13 号建议；

考虑到欧洲司法部长在第二十一届会议(1997 年 6 月 10 日至 11 日，布拉格)通过的第 1 号决议——该决议建议部长委员会支持欧洲犯罪问题委员会开展的关于网络犯罪的工作，以便使国内刑法规定更加接近，并能使用有效手段调查此类犯罪，以及欧洲司法部长第二十三届会议(2000 年 6 月 8 日至 9 日，伦敦)通过的第 3 号决议——该决议鼓励谈判方继续努力，以期找到适当的解决办法，使尽可能多的国家成为本公约的缔约国，并承认有必要建立一个迅速和有效的国际合作体制，其中恰当考虑到打击网络犯罪的具体要求；

还考虑到欧洲委员会国家元首和政府首脑在第二次首脑会议(1997 年 10 月 10 日至 11 日，斯特拉斯堡)上通过的《行动计划》，以寻求在欧洲委员会的标准和价值观基础上对新的信息技术的发展拟订共同对策；

兹议定如下：

第一章 术语的使用

第 1 条 定义

在本公约中：

(a) “计算机系统”系指任何装置或一组相互连接或关联的装置，其中一个或多个装置按照一种程序对数据进行自动处理；

(b) “计算机数据”系指以适合在计算机系统中处理的形式对事实、信息或概念的表述，包括适合于计算机系统执行某种功能的程序；

(c) “服务供应商”系指：

(1) 向其服务的用户提供通过计算机系统进行通信能力的任何公共或私人实体，以及

(2) 代表这种通信服务或这种服务的用户处理或存储计算机数据的任何其他实体。

(d) “流量数据”系指与通过计算机系统进行通信有关的任何计算机数据，它由构成通信链中一部分的计算机系统产生，表明通信的来源、目的地、路径、时间、日期、大小、持续时间或基础服务类型。

第二章　国家一级应采取的措施

第 1 节　实质性刑法

篇目 1　破坏计算机数据和系统的保密性、完整性和可用性的犯罪行为

第 2 条　非法访问

各缔约国均应采取必要的立法和其他措施，根据其国内法将无权故意擅自访问计算机系统的全部或任何部分定为刑事犯罪。缔约国可规定犯罪行为必须是通过违反安全措施，意图获取计算机数据或其他不诚实的意图，或涉及到与另一计算机系统相连的计算机系统所实施的。

第 3 条　非法截取

各缔约国均应采取必要的立法和其他措施，根据其国内法将故意实施的、通过技术手段无权截取的、向计算机系统、从计算机系统或在计算机系统内进行的非公开传输的计算机数据，包括携带此类计算机数据的计算机系统的电磁辐射定为刑事犯罪。缔约国可规定该罪行是以不诚实的意图实施的，或涉及与另一计算机系统相连的计算机系统。

第 4 条　数据干扰

1　各缔约国均应采取必要的立法和其他措施，根据其国内法将故意破坏、删除、恶化、更改或压制计算机数据的行为定为刑事犯罪。

2　缔约国可保留权利要求第 1 款所述行为造成严重的损害。

第 5 条　系统干扰

各缔约国均应采取必要的立法和其他措施，根据其国内法将无权故意通过输入、传输、破坏、删除、恶化、更改或压制计算机数据的方式严重妨碍计算机系统的运作定为刑事犯罪。

第 6 条　滥用设备

1　各缔约国均应采取必要的立法和其他措施，根据其国内法将下列无权故意实施的行为定为刑事犯罪：

(a) 生产、销售、采购以供使用、进口、分发或以其他方式提供：

(1) 主要为实施根据第 2 条至第 5 条确定的任何犯罪目的而设计或改装的装置，包括计算机程序，

(2) 能够访问整个计算机系统或其任何部分的计算机密码、访问代码或类似数据，

意图将其用于实施第 2 条至第 5 条确定的任何犯罪目的；和

(b) 拥有上文(a)项(1)目或(2)目所述物品，意图将其用于实施第 2 条至第 5 条确定的任何犯罪目的。缔约国可依据法律要求在承担刑事责任之前拥有若干此类物品。

2 本条第 1 款所述的生产、销售、采购以供使用、进口、分发或以其他方式提供或拥有，如果不是为了实施按照本公约第 2 条至第 5 条确定的犯罪目的，如经授权测试或保护计算机系统，则不应将本条解释为对其施加刑事责任。

3 各缔约国可保留不适用本条第 1 款的权利，但该保留不涉及本条第 1 款(a)项(2)目所指物品的销售、分发或以其他方式提供。

篇目 2 与计算机有关的犯罪行为

第 7 条 与计算机有关的伪造

各缔约国均应采取必要的立法和其他措施，根据其国内法将下列行为定为犯罪：无权故意输入、传输、损坏、删除、恶化、更改或取消计算机数据，造成失真数据，意图使其在法律上被视为真实数据或出于法律目的对其采取行动，无论该数据是否直接可读和可以理解。在承担刑事责任之前缔约国可要求有欺诈意图，或类似的不诚实意图。

第 8 条 与计算机有关的欺诈

各缔约国均应采取必要的立法和其他措施，根据其国内法将以下无权故意造成他人财产损失的行为定为刑事犯罪：

(a) 对计算机数据的任何输入、更改、删除或压制，

(b) 对计算机系统运行的任何干扰，

出于欺诈或者不诚实意图擅自为本人或者他人牟取经济利益。

篇目 3 与内容有关的犯罪行为

第 9 条 与儿童色情制品有关的犯罪行为

1 各缔约国均应采取必要的立法和其他措施，根据其国内法将下列无权故意实施的行为定为刑事犯罪：

(a) 制作儿童色情制品，以便通过计算机系统传播；

(b) 通过计算机系统推送或提供儿童色情制品；

(c) 通过计算机系统散发或传播儿童色情制品；

(d) 通过计算机系统为本人或者他人获得儿童色情制品；

(e) 在计算机系统或计算机数据存储介质中存储儿童色情制品。

2 就上述第 1 款而言，“儿童色情制品”一词应包括以视觉方式描绘以下内容的色情材料：

(a) 由未成年人从事露骨的性行为；

(b) 由貌似未成年人从事露骨的性行为；

(c) 反映由未成年人从事露骨的性行为的真实图像。

3 就上述第 2 款而言，“未成年人”一词应包括所有未满 18 周岁的人。然而，缔约国可以要求降低年龄限制，但不得低于 16 岁。

4 各缔约国均可保留全部或部分不适用第 1 款(d)项和(e)项以及第 2 款(b)项和(c)项的权利。

篇目 4 有关侵犯版权和相关权利的犯罪行为

第 10 条 有关侵犯版权和相关权利的犯罪行为

1 各缔约国均应采取必要的立法和其他措施，按照其在 1971 年 7 月 24 日关于《伯尔尼保护文学和艺术作品公约》的《巴黎修订案文》、《与贸易有关的知识产权协定》和《世界知识产权组织版权条约》下所承担的义务，根据其国内法将侵犯该缔约国法律界定的版权行为定为刑事犯罪，但这些公约赋予的任何精神权利除外，这类行为是通过计算机系统以商业规模任意实施的。

2 各缔约国均应采取必要的立法和其他措施，按照其在《保护表演者、唱片制作者和广播组织国际公约》(罗马公约)、《与贸易有关的知识产权协定》和《世界知识产权组织表演和唱片条约》下所承担的义务，根据其国内法将侵犯该缔约国法律界定的相关权利的行为定为刑事犯罪，这些公约赋予的任何精神权利除外，这类行为是通过计算机系统以商业规模任意实施的。

3 缔约国可以保留在有限的情况下不对本条第 1 款和第 2 款规定的刑事责任进行追究的权利，但必须有其他有效的补救措施，而且这种保留不得减损本条第 1 款和第 2 款所述国际文书中规定的缔约国的国际义务。

篇目 5 附带责任和制裁

第 11 条 企图和协助或教唆

1 各缔约国均应采取必要的立法和其他措施，根据其国内法将故意实施、协助或教唆实施按照本公约第 2 条至第 10 条确立的任何犯罪并企图实施这种犯罪的行为定为刑事犯罪。

2 各缔约国均应采取必要的立法和其他措施，根据其国内法将故意实施按照本公约第 3 条至第 5 条、第 7 条、第 8 条和第 9 条第 1 款(a)项和(c)项确立的任何犯罪的企图定为刑事犯罪。

3 各缔约国可保留全部或部分不适用本条第 2 款的权利。

第 12 条 法人责任

1 各缔约国均应采取必要的立法和其他措施，以确保法人能够对按照本公约确立的由任何自然人为其利益实施的刑事犯罪承担责任，该自然人以个人身份或作为法人单位的一部分行事，属于在法人单位中担任领导职务的人，所依据的是:

(a) 法人代表权；

(b) 代表法人作出决定的权力；

(c) 在法人内部行使控制权。

2 除本条第 1 款已经规定的情况外，各缔约国均应采取必要的措施，确保在第 1 款所述自然人因缺乏监督或控制，致使在其授权下行事的自然人有可能为该法人的利益实施按照本公约确立的刑事犯罪时，可追究法人的责任。

3 依照缔约国的法律原则，法人的责任可以是刑事责任、民事责任或行政责任。

4 此种责任不影响实施犯罪的自然人的刑事责任。

第 13 条 制裁和措施

1 各缔约国均应采取必要的立法和其他措施，确保按照第 2 条至第 11 条确定的刑事犯罪可受到有效、相称和劝阻性的制裁，包括剥夺自由。

2 各缔约国均应确保按照第 12 条承担责任的法人受到有效、相称和劝阻性的刑事或非刑事制裁或措施，包括罚款制裁。

第 2 节 程序法

篇目 1 通用条款

第 14 条 程序性规定的范围

1 各缔约国均应采取必要的立法和其他措施，确立本节规定的权力和程序，以便开展具体的刑事调查或诉讼。

2 除第 21 条另有明确规定外，各缔约国均应将本条第 1 款所述的权力和程序适用于：

(a) 按照本公约第 2 条至第 11 条所确定的刑事犯罪；

(b) 利用计算机系统实施的其他刑事犯罪；和

(c) 以电子形式收集刑事犯罪的证据。

3 (a) 各缔约国可以保留仅对其保留中指明的犯罪或犯罪类别适用第 20 条所述措施的权利，但此类犯罪或犯罪类别的范围不得比其适用第 21 条所述措施的犯罪范围更窄。各缔约国均应考虑对这种保留加以限制，以便能够最广泛地适用第 20 条所述的措施。

(b) 如果一缔约国由于本公约通过时受其现行立法的限制，不能对服务供应商的计算机系统内传输的通信适用第 20 条和第 21 条所述的措施，而该系统：

(1) 是为封闭式用户群的利益运营的，并且

(2) 不使用公共通信网络，也不与其他公共或私人计算机系统连接，

该缔约国可保留不将这些措施适用于此类通信的权利。各缔约国均应考虑限制这种保留，以便能够最广泛地适用第 20 条和第 21 条所述的措施。

第 15 条--条件和保障

1 各缔约国均应确保本节规定的权力和程序的设立、执行和适用遵守其国内法规定的条件和保障，其中应规定充分保护人权和自由，包括其根据 1950 年欧洲委员会《保护人权和基本自由公约》、1966 年联合国《公民及政治权利国际公约》和其他适用的国际人权文书所承担的义务而产生的权利，并应纳入相称性原则。

2 鉴于有关程序或权力的性质，此类条件和保障应酌情包括司法或其他独立监督、适用的理由以及对这种权力或程序的范围和期限的限制。

3 在符合公共利益，特别是健全司法的前提下，各缔约国均应考虑本节中的权力和程序对第三方的权利、责任和合法利益的影响。

篇目 2 加快保存已存储的计算机数据

第 16 条 加快保存已存储的计算机数据

1 各缔约国均应采取必要的立法和其他措施，使其主管机构能够命令或以类似方式迅速保存通过计算机系统储存的特定计算机数据，包括流量数据，特别是在有理由相信计算机数据特别容易丢失或被修改的情况下。

2 如果一缔约国通过命令某人保存其拥有或控制的特定存储的计算机数据来实施上述第 1 款，该缔约国应采取必要的立法和其他措施，责成此人在必要的时间内(最长不超过 90 天)，保存和维护该计算机数据的完整性，以便主管机构能够寻求披露该数据。缔约国可规定该命令随后可以延长。

3 各缔约国均应采取必要的立法和其他措施，责成保管人或其他负责保存计算机数据的人在国内法规定的期限内对此类程序的运作保密。

4 本条所指的权力和程序应遵守第 14 条和第 15 条的规定。

第 17 条 加快保存和部分披露流量数据

1 各缔约国均应根据第 16 条就保存的流量数据采取必要的立法和其他措施，以便:

(a) 确保无论是否一个或多个服务供应商参与该通信的传输，都可以加快保存流量数据；和

(b) 确保迅速向缔约国主管机构或该主管机构指定的人披露足够数量的流量数据，使缔约国能够识别通信的服务商和传输路径。

2 本条所指的权力和程序应遵守第 14 条和第 15 条的规定。

篇目 3 出示令

第 18 条 出示令

1 各缔约国均应采取必要的立法和其他措施，授权其主管机构命令：

(a) 在其领土上的人提交其所拥有或控制的、储存在计算机系统或计算机数据存储介质中的特定计算机数据；以及

(b) 在缔约国境内提供服务的服务供应商，提交该服务供应商拥有或控制的与此类服务有关的用户信息。

2 本条所指的权力和程序应遵守第 14 条和第 15 条的规定。

3 就本条而言，“用户信息”一词是指以计算机数据形式或任何其他形式存在的、由服务供应商掌握的、有关其服务的用户(除流量或内容数据外)的任何信息，通过这些信息可以确定:

(a) 所使用的通信服务类型、所采用的技术规范和服务期限；

(b) 基于服务协议或安排可获得的用户身份、邮政或地理地址、电话和其他接入号码、账单和支付信息；

(c) 基于服务协议或安排可获得的有关通信设备安装地点的任何其他信息。

篇目 4 搜查和扣押存储的计算机数据

第 19 条 搜查和扣押存储的计算机数据

1 各缔约国均应采取必要的立法和其他措施，授权其主管机构搜查或以类似方式访问：

(a) 计算机系统或其中的一部分以及其中存储的计算机数据；和

(b) 在其领土上可存储计算机数据的计算机数据存储介质。

2 各缔约国均应采取必要的立法和其他措施，以确保其主管机构根据第 1 款(a)项搜查或以类似方式访问特定计算机系统或其部分的情况下，并有理由相信所寻找的数据存储在其境内的另一计算机系统或其部分中，且这种数据可合法地从初始系统访问或获得，该主管机构应能迅速扩大搜查或以类似方式访问另一系统。

3 各缔约国均应采取必要的立法和其他措施，授权其主管机构扣押或以类似方式保护根据第 1 款或第 2 款访问的计算机数据。这些措施应包括以下权力：

(a) 扣押或以类似方式保护计算机系统或其中一部分或计算机数据存储介质；

(b) 制作并保留这些计算机数据的一份副本；

(c) 维护相关存储的计算机数据的完整性；

(d) 使被访问的计算机系统中的计算机数据不能再访问或将其移除。

4 各缔约国均应采取必要的立法和其他措施，授权其主管机构命令任何了解计算机系统运作或用于保护其中的计算机数据的措施的人，合理提供必要的信息，以便能够采取第 1 款和第 2 款所述的措施。

5 本条所指的权力和程序应遵守第 14 条和第 15 条的规定。

篇目 5 实时收集计算机数据

第 20 条 实时收集流量数据

1 各缔约国均应采取必要的立法和其他措施，授权其主管机构命令：

(a) 通过在该缔约国领土上应用技术手段收集或记录，以及

(b) 强制服务供应商在其现有技术能力范围内：

(1) 通过在该缔约国领土上应用技术手段收集或记录，以及或

(2) 配合并协助主管机构收集或记录

在其领土上通过计算机系统传输的与特定通信有关的实时流量数据。

2 如果一缔约国由于其国内法律制度的既定原则不能采取第 1 款(a)项所述措施，则可以采取必要的立法和其他措施，确保通过在该国领土上应用技术手段，实时收集或记录与其境内传输的特定通信有关的流量数据。

3 各缔约国均应采取必要的立法和其他措施，责成服务供应商对本条规定的任何权力的行使和与之有关的任何信息予以保密。

4 本条所指的权力和程序应遵守第 14 条和第 15 条的规定。

第 21 条 截取内容数据

1 各缔约国均应针对国内法确定的一系列严重犯罪行为，采取必要的立法和其他措施，授权其主管机构:

(a) 在该缔约国领土上通过应用技术手段收集或记录，以及

(b) 强制服务供应商在其现有技术能力范围内：

(1) 在该缔约国领土上通过应用技术手段收集或记录，以及

(2) 配合并协助主管机构收集或记录，

在其领土上通过计算机系统传输的特定通信的实时内容数据。

2 如果一缔约国由于其国内法律制度的既定原则不能采取第 1 款(a)项所述措施，可以采取必要的立法和其他措施，确保通过在该国领土上应用技术手段，实时收集或记录其领土上特定通信的内容数据。

3 各缔约国均应采取必要的立法和其他措施，责成服务供应商对本条规定的任何权力的行使和与之有关的任何信息予以保密。

4 本条所指的权力和程序应遵守第 14 条和第 15 条的规定。

第 3 节 管辖权

第 22 条--管辖权

1 各缔约国均应采取必要的立法和其他措施，以确立对按照本公约第 2 条至第 11 条确定的任何犯罪的管辖权，倘若犯罪发生在：

(a) 其领土上；或

(b) 悬挂该缔约国国旗的船只上；或

(c) 根据该缔约国法律注册的航空器上；或

(d) 由其国民所为，而根据犯罪行为发生地刑法应受到惩罚，或者如果犯罪行为发生在任何国家领土管辖范围以外。

2 各缔约国均可保留不适用或仅在特定情况或条件下适用本条第 1 款(b)项至(d)项规定的管辖权规则或其任何部分的权利。

3 各缔约国均应采取必要措施，以确立对本公约第 24 条第 1 款所指罪行的管辖权，如果被指控的犯罪人出现在其领土上，并且在另一缔约国提出引渡请求后，该缔约国不会仅以其国籍为由将其引渡给另一缔约国。

4 本公约不排除缔约国根据其国内法行使的任何刑事管辖权。

5 当一个以上缔约国声称对按照本公约确定的一项指控罪行拥有管辖权时，有关缔约国应酌情进行协商，以期确定最合适的起诉管辖权。

第三章 国际合作

第 1 节 一般原则

篇目 1 关于国际合作的一般原则

第 23 条 关于国际合作的一般原则

各缔约国均应根据本章的规定，通过适用有关刑事事项国际合作的国际文书、在统一或对等立法基础上商定的安排和国内法，尽可能广泛地相互合作，以便调查或审理与计算机系统和数据有关的刑事犯罪，或收集刑事犯罪的电子证据。

篇目 2 有关引渡的原则

第 24 条 引渡

1 (a) 本条适用于缔约国之间对按照本公约第 2 条至第 11 条确定的刑事犯罪进行的引渡，条件是根据缔约双方的法律，这些犯罪可处以剥夺自由最长至少一年，或处以更严厉的刑罚。

(b) 如果根据在统一或对等立法或引渡条约基础上商定的安排适用不同的最低刑罚，包括适用于两个或两个以上缔约国的《欧洲引渡公约》(《欧洲条约集》第 24 号)，则应适用此类安排或条约规定的最低刑罚。

2 本条第 1 款所述的刑事犯罪应被视为包括在缔约国之间现有的任何引渡条约中的可引渡罪行。各缔约国承诺将此类罪行作为可引渡的罪行纳入彼此之间将要缔结的任何引渡条约。

3 以订有条约为引渡条件的缔约国，如果收到与之未订有引渡条约的另一缔约国的引渡请求，可将本公约视为就本条第 1 款所述任何刑事犯罪进行引渡的法律依据。

4 不以订有条约为引渡条件的缔约国，应承认本条第 1 款所述的刑事犯罪为彼此之间的可引渡犯罪。

5 引渡须符合被请求方的法律或适用的引渡条约所规定的条件，其中包括被请求方可拒绝引渡的理由。

6 如果仅以被请求引渡者的国籍为由拒绝就本条第 1 款所述的刑事犯罪进行引渡，或者被请求方认为其对该犯罪具有管辖权，则被请求方应根据请求方的要求将案件提交其主管机构进行起诉，并应在适当时候向请求方报告最终结果。主管机构应以与该缔约国法律规定的任何类似性质的犯罪相同的方式作出决定，并进行调查和诉讼。

7 (a) 各缔约国均应在签署时或交存批准书、接受书、核准书或加入书时，向欧洲委员会秘书长通报在没有条约的情况下负责提出或接受引渡或临时逮捕请求的每一主管机构的名称和地址。

(b) 欧洲委员会秘书长应设立并随时更新关于缔约国指定机构的名册。各缔约国均应确保该名册上的详细材料始终准确无误。

篇目 3 有关互助的一般原则

第 25 条 有关互助的一般原则

1 缔约国应尽最大可能相互协助，以便对与计算机系统和数据有关的刑事犯罪进行调查或诉讼，或收集刑事犯罪的电子形式的证据。

2 各缔约国还应采取必要的立法和其他措施，以履行第 27 条至第 35 条规定的义务。

3 在紧急情况下，各缔约国可通过快速通信手段，包括传真或电子邮件，提出相互协助或相关的通信请求，只要这种手段提供适当的安全和认证(必要时包括使用加密)，并在被请求方要求时随后加以正式确认。被请求方应通过任何此类快速通信手段接受并答复请求。

4 除本章各条另有具体规定外，相互协助须符合被请求方的法律或适用的互助条约所规定的条件，包括被请求方可拒绝合作的理由。被请求方不得以其认为请求仅涉及属于财政犯罪为由，而就第 2 至第 11 条所述犯罪行为行使拒绝互助的权利。

5 如根据本章的规定，被请求方以存在双重犯罪为条件准许提供互助，则不论被请求方的法律是否将该罪行列为同一类罪行，或以与请求方相同的用语界定该罪行，如果寻求协助的犯罪目标所涉行为在其法律中属于刑事罪，则应视为满足了这一条件。

第 26 条 自发提供的信息

1 缔约国如果认为披露如下信息可能有助于接受方发起或开展关于按照本公约确立的刑事犯罪的调查或诉讼，或可能导致该缔约国依照本章提出合作请求，可以在其国内法的范围内，不经事先请求，向另一缔约国提供其本身调查中获得的信息。

2 在提供此类信息之前，提供方可要求对其保密，或仅在有条件的情况下使用。如果接收方不能满足这一请求，则应通知提供方，然后由提供方决定是否仍提供该信息。如果接收方按照条件接受信息，则应受其约束。

篇目 4 在无适用的国际协议的情况下提出互助请求的程序

第 27 条 在无适用的国际协议的情况下提出互助请求的程序

1 如果请求方与被请求方之间没有以统一或对等立法为基础的互助条约或安排，应适用本条第 2 款至第 9 款的规定。如果存在此类条约、安排或立法，则本条的规定不适用，除非有关缔约国同意适用本条其余所有或任何部分予以代替。

2 (a) 各缔约国均应指定一个或多个中央机关，负责发送和答复互助请求、执行此类请求或将其转交主管机构执行；

(b) 中央机关应彼此直接沟通；

(c) 各缔约国均应在签署时或交存批准书、接受书、核准书或加入书时，将根据本款指定的中央机关的名称和地址通知欧洲委员会秘书长；

(d) 欧洲委员会秘书长应设立并随时更新一份缔约国指定的中央机关名册。各缔约国均应确保该名册上的详细材料始终准确无误。

3 除非与被请求方的法律不符，否则按照本条提出的互助请求应依照请求方确定的程序执行。

4 除第 25 条第 4 款规定的拒绝理由外，被请求方在下列情况下可以拒绝提供协助：

(a) 请求涉及被请求方认为是政治罪或与政治罪有关的犯罪，或

(b) 被请求方认为，执行这一请求可能损害其主权、安全、公共秩序或其他基本利益。

5 如果采取行动会妨碍其主管机关进行的刑事调查或诉讼，被请求方可推迟对请求采取行动。

6 在拒绝或推迟协助之前，被请求方应在适当情况下，与请求方协商后，酌情考虑是否可部分准许该项请求，或附加其认为必要的条件。

7 被请求方应将协助请求的执行结果迅速通知请求方。应说明拒绝或推迟请求的理由。被请求方还应将任何导致请求无法执行或可能严重拖延执行的原因告知请求方。

8 请求方可要求被请求方对按照本章提出的任何请求之事及其内容予以保密，但为执行请求所需的情况除外。如果被请求方不能遵守保密要求，应立即通知请求方，由请求方决定是否仍执行请求。

9 (a) 在紧急情况下，请求方的司法机关可直接向被请求方的司法机关发出互助请求或相关的信函。在任何此种情况下，应同时通过请求方的中央机关向被请求方的中央机关发送一份副本。

(b) 根据本款发出的任何请求或信函，可通过国际刑事警察组织(国际刑警组织)发出。

(c) 如果按照本款(a)项提出请求，而有关部门无权处理这一请求，则应将该请求上交国家主管机构，并直接通知请求方已这样处理。

(d) 按照本款提出的不涉及强制行动的请求或信函，可由请求方主管机构直接转交被请求方的主管机构。

(e) 各缔约国在签署时或交存批准书、接受书、核准书或加入书时，可通知欧洲委员会秘书长，出于效率考虑，按照本款提出的请求应向其中央机关提出。

第 28 条 保密和使用限制

1 如果请求方和被请求方之间没有以统一或对等立法为基础的互助条约或安排，则应适用本条的规定。如果存在此类条约、安排或立法，则本条的规定不适用，除非有关缔约国同意适用本条其余所有或任何部分予以代替。

2 被请求方应请求提供的信息或材料可视下列条件而定：

(a) 保密，如果缺乏这一条件即不能满足相互法律协助的请求，或

(b) 不得用于请求中所述以外的调查或诉讼。

3 如果请求方不能遵守第 2 款所述的条件，应立即通知对方，由对方决定是否仍提供该项材料。一旦请求方接受该条件，即应受该条件的约束。

4 在符合第 2 款所述条件的情况下，提供信息或材料的任何缔约国可要求对方针对这一条件解释使用此类信息或材料的用途。

第 2 节 具体规定

篇目 1 关于临时措施方面的互助

第 29 条 迅速保全存储的计算机数据

1 一缔约国可要求另一缔约国命令或以其他方式迅速保全位于另一方境内通过计算机系统存储的数据，而请求方打算就该数据的搜查或类似访问、扣押或类似保全或披露提出互助请求。

2 根据第 1 款提出的保全请求应具体说明：

(a) 寻求保全的主管机构；

(b) 作为刑事调查或诉讼对象的罪行和相关事实的简要说明；

(c) 需要保全的存储的计算机数据及其与犯罪行为的关系；

(d) 任何可以确定存储的计算机数据的保管人或计算机系统位置的信息；

(e) 保全的必要性；以及

(f) 该缔约国打算就搜查或类似访问、扣押或类似保全或披露存储的计算机数据提交互助请求。

3 被请求方接获另一缔约国的请求后，须采取一切适当措施，按照其国内法迅速保全指定的材料。为了回应请求，不应要求将双重犯罪作为提供这种保全的条件。

4 要求将双重犯罪作为条件以答复搜查或类似访问、扣押或类似保全或披露存储数据互助请求的缔约国，对于按照本公约第 2 条至第 11 条所确定的罪行以外的罪行，如果有理由认为在披露时不能满足双重犯罪的条件，可保留拒绝本条下的保全请求的权利。

5 此外，只有在下列情况下，才可拒绝保全请求：

(a) 请求涉及被请求方认为是政治罪或与政治罪有关的犯罪，或

(b) 被请求方认为执行该项请求可能损害其主权、安全、公共秩序或其他基本利益。

6 如果被请求方认为保全数据不能确保其今后的可用性，或将威胁到请求方调查的保密性，或以其他方式损害请求方的调查，则应立即将此种情况通知请求方，然后由请求方决定是否应执行该请求。

7 为回应第 1 款所述的请求进行的任何保全，其期限不得少于 60 天，以便请求方能提出搜查或类似访问、扣押或类似保全或披露数据的请求。在收到这种请求后，在对该请求作出决定之前，应继续保存这些数据。

第 30 条 加快披露保存的流量数据

1 在执行根据第 29 条提出的保全与某一特定通信有关的流量数据的请求过程中，如果被请求方发现有另一国的服务供应商参与该通信的传输，被请求方应尽快向请求方披露足够数量的流量数据，以查明该服务供应商和通信传输的路径。

2 只有在下列情况下，才可以拒绝按照第 1 款披露流量数据：

(a) 请求涉及被请求方认为是政治罪或与政治罪有关的犯罪；或

(b) 被请求方认为执行该项要请求可能损害其主权、安全、公共秩序或其他基本利益。

篇目 2 关于调查权的互助

第 31 条 关于访问存储的计算机数据的互助

1 一缔约国可要求另一缔约国搜查或以类似方式访问、扣押或以类似方式保全通过位于被清求方境内的计算机系统存储的数据，包括根据第 29 条保全的数据。

2 被请求方可适用第 23 条所述的国际文书、安排和法律，并依照本章其他有关规定，对请求给予答复。

3 在下列情况下，应迅速对请求给予答复：

(a) 有理由相信相关数据特别容易丢失或被修改；或

(b) 第 2 款所述的文书、安排和法律对快速合作另有规定。

第 32 条　经同意或在可公开获得的情况下跨境访问存储的计算机数据

一方可未经另一方授权可以：

(a) 访问可公开获得的(开放源码)存储的计算机数据，无论数据位于何处；或

(b) 通过其境内的计算机系统访问或接收存储在另一缔约国的计算机数据，前提是该缔约国获得有合法权力通过该计算机系统向该缔约国披露数据的人的合法、自愿同意。

第 33 条　实时收集流量数据方面的互助

1　缔约国应相互协助实时收集其境内通过计算机系统传输的特定通信的相关流量数据。在符合第 2 款规定的情况下，此类协助应受国内法规定的条件和程序的管辖。

2　各缔约国均应至少对在国内类似案件中可实时收集流量数据的刑事犯罪提供这种协助。

第 34 条 截取内容数据方面的互助

缔约国应在各自适用的条约和国内法允许的范围内，在实时收集或记录通过计算机系统传输的特定通信内容数据方面相互提供协助。

篇目 3　全天候网络

第 35 条 全天候网络

1　各缔约国均应指定一个每周 7 天每天 24 小时随时可用的联络点，以确保为有关计算机系统和数据的刑事犯罪调查或诉讼，或为收集刑事犯罪的电子形式的证据提供即时援助。此类协助应包括提供便利，或在其国内法律和惯例允许的情况下，直接执行下列措施：

(a) 提供技术咨询；

(b) 按照第 29 条和第 30 条保存数据；

(c) 收集证据，提供法律信息和确定嫌疑人的位置。

2　(a) 一缔约国的联络点应有能力快速与另一缔约国的联络点进行联系。

(b) 如果缔约国指定的联络点不是该缔约国负责国际互助或引渡的某个或多个机构的一部分，该联络点应确保能够迅速与上述一个或多个机构进行协调。

3　各缔约国均应确保备有训练有素、装备齐全的人员以方便这一网络的运行。

第五章 最后条款

第 36 条 签署和生效

1 本公约开放供欧洲委员会成员国和参与其制定的非成员国签署。

2 本公约须经批准、接受或核准。批准书、接受书或核准书应交存欧洲委员会秘书长。

3 本公约自五个国家，其中包括至少三个欧洲委员会成员国按照第 1 款和第 2 款的规定，表示同意受其约束之日起三个月期满后的下个月的首日生效。

4 对于其后表示同意受本公约约束的任何签署国，本公约应在其按照第 1 款和第 2 款的规定，表示同意受本公约的约束之日起三个月期满后的下个月的首日生效。

第 37 条 加入公约

1 本公约生效后，欧洲委员会部长委员会在与本公约缔约国协商并征得其一致同意后，可邀请任何非欧洲委员会成员国且未参与本公约制定的国家加入本公约。该决定应由《欧洲委员会章程》第 20 条(d)款规定的多数缔约国和有权参加部长委员会的缔约国代表一致表决作出。

2 对于按照上述第 1 款加入本公约的任何国家，本公约应于其向欧洲委员会秘书长交存加入书之日起三个月期满后的下个月的首日生效。

第 38 条 适用领土

1 任何国家在签署时或交存批准书、接受书、核准书或加入书时，均可指明本公约适用的一个或多个领土。

2 任何国家均可在以后任何日期通过致欧洲委员会秘书长的声明，将本公约的适用范围扩大到声明中规定的任何其他领土。就该领土而言，本公约应于秘书长收到声明之日起三个月期满后的下个月的首日生效。

3 根据上述两款针对其中所指明的领土作出的声明，可通过致欧洲委员会秘书长的通知撤销。撤销应在秘书长收到通知之日起三个月期满后的下个月的首日生效。

第 39 条 公约的效力

1 本公约的目的是补充缔约国之间适用的多边或双边条约或安排，包括下列规定：

-《欧洲引渡公约》(1957 年 12 月 13 日在巴黎开放供签署,《欧洲条约集》第 24 号)

-《欧洲刑事事项互助公约》(1959 年 4 月 20 日在斯特拉斯堡开放供签署,《欧洲条约集》第 30 号)

-《欧洲刑事事项互助公约附加议定书》(1978 年 3 月 17 日在斯特拉斯堡开放供签署,《欧洲条约集》第 99 号)。

2 如果两个或两个以上缔约国已经就本公约所涉事项缔结了协定或条约，或以其他方式就此类事项建立了关系，或者如果今后会这样做，它们也应有权适用这种协定或条约或相应调整这些关系。但是，如果缔约国就本公约所处理的事项而非其规定的事项建立关系，则应以不违背本公约目标和原则的方式进行。

3 本公约的任何规定均不影响缔约国的其他权利、限制、义务和责任。

第 40 条 声明

任何国家均可在签署时或交存批准书、接受书、核准书或加入书时，向欧洲委员会秘书长发出书面通知，声明愿意利用第 2 条、第 3 条、第 6 条第 1 款(b)项、第 7 条、第 9 条第 3 款和第 27 条第 9 款(e)项规定的补充要件的可能性。

第 41 条 联邦条款

1 联邦国家可保留根据本公约第二章承担义务的权利，但须符合其关于中央政府与各组成州或其他类似领土实体之间关系的基本原则，但前提是它仍能根据第三章进行合作。

2 联邦国家在根据第 1 款提出保留时，不得以适用这种保留的条款来排除或大幅减少其对第二章规定的措施的义务。总体而言，它应就这些措施提供广泛有效的执法能力。

3 对于本公约的条款，如果其适用属于各组成州或其他类似领土实体的管辖范围，而这些州根据联邦宪法制度没有义务采取立法措施，联邦政府应将其赞成的意见通知这些州的主管机构，鼓励它们采取适当行动使这些条款生效。

第 42 条 保留

任何国家在签署时或交存批准书、接受书、核准书或加入书时，均可向欧洲理事会秘书长发出书面通知，声明其适用第 4 条第 2 款、第 6 条第 3 款、第 9 条第 4 款、第 10 条第 3 款、第 11 条第 3 款、第 14 条第 3 款、第 22 条第 2 款、第 29 条第 4 款和第 41 条第 1 款规定的保留。

第 43 条 保留的地位和撤回

1 根据第 42 条提出保留的缔约国可以通过向欧洲理事会秘书长发出通知，全部或部分撤回保留。这种撤回应于秘书长收到通知之日起生效。如果通知说明撤回保留将于通知中指定的日期生效，而该日期晚于秘书长收到通知的日期，则撤回应在这一较晚日期生效。

2 已作出第 42 条所述保留的缔约国，一旦情况允许，应立即全部或部分撤回该保留。

3 欧洲委员会秘书长可定期向已作出第 42 条所述的一项或多项保留的缔约国询问撤回此种保留的前景。

第 44 条 修正

1 本公约的修正案可由任何缔约国提出，并应由欧洲委员会秘书长通知欧洲委员会成员国、参与本公约制定的非成员国，以及根据第 37 条的规定已加入或获邀加入本公约的任何国家。

2 缔约国提出的任何修正案应送交欧洲犯罪问题委员会(犯罪问题委员会)，该委员会应向部长委员会提交对该拟议修正案的意见。

3 部长委员会应审议拟议的修正案和犯罪问题委员会提交的意见，并在与本公约非成员国协商后可通过修正案。

4 部长委员会根据本条第 3 款通过的任何修正案的文本应转交各缔约国接受。

5 根据本条第 3 款通过的任何修正案应在所有缔约国通知秘书长表示接受修正案后的第 30 天生效。

第 45 条 争端的解决

1 应随时向犯罪问题委员会通报本公约的解释和适用情况。

2 如果缔约国在本公约的解释或适用方面发生争端，应寻求通过谈判或其选择的任何其他和平方式解决争端，包括经有关各方同意，将争端提交犯罪问题委员会，或其裁决对当事各方具有约束力的仲裁法庭，或提交国际法院。

第 46 条 缔约国协商

1 缔约国应酌情定期协商，以期促进：

(a) 有效利用和实施本公约，包括发现其中的任何问题，以及根据本公约作出的任何声明或保留的效果；

(b) 交流与网络犯罪和以电子形式收集证据有关的重大法律、政策或技术发展方面的信息；

(c) 审议对本公约可能的补充或修正。

2 应定期向犯罪问题委员会通报第 1 款所述协商的结果。

3 犯罪问题委员会应酌情为第 1 款所述的协商提供便利，并采取必要的措施协助缔约国努力补充或修正本公约。最迟在本公约生效三年后，犯罪问题委员会应与缔约国合作，对公约的所有条款进行审查，并在必要时提出任何适当的修正案。

4 除欧洲委员会承担的费用外，执行第 1 款规定所发生的费用应由各缔约国按照其确定的方式承担。

5 各缔约国均应在欧洲委员会秘书处的协助下履行本条规定的职责。

第 47 条 退约

1 任何缔约国均可在任何时候向欧洲委员会秘书长发出通知宣布退出本公约。

2 此种退约应在秘书长收到通知之日起三个月期满后的下个月的首日生效。

第 48 条 通知

欧洲委员会秘书长应向欧洲委员会成员国、参与本公约制定的非成员国以及已加入或获邀加入本公约的任何国家通报下列情况：

(a) 任何签署；

(b) 任何批准书、接受书、核准书或加入书的交存；

(c) 根据本公约第 36 条和第 37 条的任何生效日期；

(d) 根据第 40 条作出的任何声明或根据第 42 条提出的任何保留；

(e) 与本公约有关的任何其他行为、通知或通信函。

下列签署人经正式授权在本公约上签字，以昭信守。

本公约于 2001 年 11 月 23 日在布达佩斯签署，用英文和法文写成，两种文本具有同等效力，一式两份，存放在欧洲委员会档案馆。欧洲委员会秘书长应将经过核证的副本转发给欧洲委员会各成员国、参与本公约制定的非成员国以及应邀加入本公约的任何国家。

《欧洲条约集》第 185 号

关于《网络犯罪公约》的解释性报告

2001 年 11 月 23 日，布达佩斯

一. 本公约及其解释性报告由欧洲委员会部长委员会第 109 届会议(2001 年 11 月 8 日)通过，本公约 2001 年 11 月 23 日于布达佩斯网络犯罪问题国际会议之际开放供签署。

二. 本解释性报告的内容尽管性质上可能有助于公约所载规定的适用，但不构成对本公约作出权威性解释的文书。

一. 导言

1. 信息技术革命已经从根本上改变了社会，并且在可预见的未来会继续这种改变。许多任务变得更容易处理了。在信息技术的帮助下，最初只有一些特定的社会部门实现了工作程序的合理化，而如今几乎没有任何社会部门不受其影响。信息技术以各式各样的方式几乎渗透到人类活动的方方面面。

2. 信息技术的一个显著特点是它已经并将继续对电信技术的发展产生影响。涉及人类语音传输的传统电话技术已被海量数据的交换所取代，这些数据包括语音、文本、音乐以及静态和动态图像。这种交流不再仅仅发生在人与人之间，也发生在人与计算机之间，以及计算机相互之间。电路交换连接已被分组交换网络取代。是否可以建立直接连接已不再重要，只要将数据输入到含有目的地址的网络中，或者让任何想要访问数据的人都可以访问它，就足够了。

3. 电子邮件的普遍使用和通过互联网访问众多网站就是这类发展的例子。它们深刻地改变了我们的社会。

4. 计算机系统所含信息的易获取性和可搜索性，加之其交流和传播的几乎无限可能性，无论地理距离远近，都导致了可获得的信息量和从中可获得的知识的爆炸性增长。

5. 这些发展带来了前所未有的经济和社会变革，但也产生了阴暗面：出现了新的犯罪类型，以及通过新技术实施传统犯罪行为。此外，犯罪行为的后果可能比以前更深远，因为它们不受地理限制或国界的限制。最近有害的计算机病毒在世界各地的蔓延就证明了这一现实。保护计算机系统的技术措施需要与预防和阻止犯罪行为的法律措施同时实施。

6. 新技术挑战现有的法律概念。信息和通信在世界各地更容易流通。边界也不再是这种流通的边界。罪犯越来越多地出现在其行为影响地以外的地方。然而，国内法通常局限于特定的领土。因此，必须由国际法来处理所面临问题的解决办法，这就需要通过适当的国际法律文书。本公约旨在应对这一挑战，并在新的信息社会中妥善尊重人权。

二. 筹备工作

7.根据(C)(D)P(C)/103/211196 号决定，欧洲犯罪问题委员会(犯罪问题委员会)于 1996 年 11 月决定成立一个专家委员会来处理网络犯罪问题。犯罪问题委员会的决定基于以下理由：

8.“信息技术领域的快速发展对现代社会的各个方面都产生了直接影响。电信和信息系统的整合，使得各种通信的存储和传输不受距离限制，开辟了一系列新的可能性。信息高速公路和网络(包括互联网)的出现加速了这些发展，借助它们，几乎任何人都可以获得任何电子信息服务，无论其所处世界何处。通过连接通信和信息服务，用户创建了一种称为“网络空间”的公共空间，这种空间可用于合法目的，但也可能被滥用。这类“网络空间犯罪”要么破坏了计算机系统和电信网络的完整性、可用性和保密性，要么包括利用这些网络的服务实施传统犯罪。这类犯罪的跨界性质，例如通过互联网实施的犯罪，与国家执法当局的属地性相冲突。

9.因此，刑法必须跟上这类技术发展的步伐，这类技术发展为滥用网络空间设施和损害合法利益提供了错综复杂的机会。鉴于信息网络的跨境性质，需要国际社会齐心协力对付这种滥用行为。虽然第(89)9 号建议使各国对某些形式的计算机滥用的概念趋于一致，但只有具有约束力的国际文书才能为打击这类新现象确保必要的效率。在本文书的框架内，除了国际合作措施外，还应解决实体法和程序法问题，以及与使用信息技术密切相关的问题。”

10.此外，犯罪问题委员会考虑了应其请求由(H).W.K.卡斯珀森教授编写的报告，该报告的结论是“……应当寻求另一种比建议更具参与性的法律文书，例如公约。这样一项公约不仅应处理刑事实体法事项，还应处理刑事程序问题以及国际刑法程序和协定。”[1]关于实体法的建议(R(89)9 号)[2]和关于与信息技术有关的程序法问题的建议(R(95)13 号)[33] 所附的报告已经得出类似的结论。

11. 新的委员会的具体职权范围如下：

(一)“参照关于计算机犯罪的第 R(89)9 号建议和关于与信息技术有关的刑事诉讼法问题的第 R(95)13 号建议，特别审查以下专题：

(二)网络空间犯罪，特别是通过使用电信网络(如互联网)实施的犯罪，如非法货币交易、提供非法服务、侵犯版权，以及侵犯人的尊严和损害对未成年人的保护；

(三)其他实质性刑法问题，为此可能需要采取共同办法已达国际合作目的，例如网络空间行为者(包括互联网服务供应商)的定义、惩罚和责任；

(四)使用，包括跨界使用的可能性，以及强制权力在技术环境中的适用性，例如截取通信和电子监视信息网络，例如通过互联网，搜查和扣押信息处理系统(包括互联网站)，使非法材料无法获取，并要求服务供应商遵守特殊义务，同时考虑到特定信息安全措施(如加密)造成的问题；

[1] 关于计算机相关犯罪的建议(R(89)9 号)的执行情况，(H).W.K.卡斯珀森博士编写的报告(doc. CDPC (97) 5 和 PC-CY (97) 5，第 106 页)。

[2] 见与计算机相关的犯罪，欧洲犯罪问题委员会的报告，第 86 页。

[3] 见与信息技术有关的刑事诉讼法问题，第 R(95)13 号建议，第 17 条原则。

(五)与信息技术犯罪有关的管辖权问题，例如确定犯罪发生的地点(犯罪地点)和相适用的法律，包括在多重管辖权的情况下一罪不二审的问题，以及如何解决积极管辖权冲突和如何避免消极管辖权冲突的问题；

(六)与在刑事领域欧洲公约执行情况专家委员会(刑事公约专家委)密切合作，讨论在调查网络空间犯罪方面的国际合作问题。

该委员会应尽可能就项目(一)至(五)起草一份具有约束力的法律文书，特别强调国际问题，并酌情就具体问题提出附带建议。该委员会可应对科技发展，就其他事项提出建议。”

12. 继犯罪问题委员会的决定之后，部长委员会根据部长代表第 583 次会议(1997 年 2 月 4 日举行)通过的第(C)M/(D)(e)1/(D)(e)(c)(97)583 号决定，成立了新的委员会，称为“网络空间犯罪问题专家委员会”(网络犯罪专家委)。该委员会于 1997 年 4 月开始工作，并就一项关于网络犯罪的国际公约草案进行了谈判。根据其原来的职权范围，该委员会应在 1999 年 12 月 31 日前完成工作。由于届时委员会未能完全结束关于公约草案中某些问题的谈判，部长代表第(C)M/(D)(e)1/(D)(e)(c)(99)679 号决定将其职权范围延长至 2000 年 12 月 31 日。欧洲各国司法部长就谈判两度表示支持：第 21 届会议(1997 年 6 月，布拉格)通过的第 1 号决议，建议部长委员会支持犯罪问题委员会在网络犯罪方面开展的工作，以便使各国国内刑法条款更加趋同，并能够使用有效的手段调查此类犯罪；第 23 届欧洲司法部长会议(2000 年 6 月，伦敦)通过的第 3 号决议，鼓励谈判各方继续努力，以期找到适当的解决办法，使尽可能多的国家成为本公约缔约国，并承认需要一个方便有效的国际合作体制，该体制应妥善考虑到打击网络犯罪的具体要求。欧洲联盟成员国借助 1999 年 5 月通过的“联合立场”表示支持网络犯罪专家委的工作。

13. 1997 年 4 月至 2000 年 12 月期间，网络犯罪专家委举行了 10 次全体会议和 15 次不限成员名额的起草小组会议。在延长的任务期限到期后，专家们在犯罪问题委员会的主持下又举行了三次会议，以最后敲定解释性备忘录草案，并根据欧委会议会大会的意见审查了公约草案。部长委员会于 2000 年 10 月请议会大会就公约草案发表意见，议会大会于 2001 年 4 月第二期全体会议上通过了公约草案。

14. 在网络犯罪专家委作出决定之后，2000 年 4 月解密并发布了公约草案的早期版本，随后在每次全体会议之后发布了嗣后的草案，以便使谈判国能够与所有感兴趣的各方进行协商。事实证明，这一协商过程是颇具裨益的。

15. 经修订和定稿的公约草案及其解释性备忘录于 2001 年 6 月提交犯罪问题委员会第 50 次全体会议批准，随后公约草案文本提交部长委员会通过并开放供签署。

三. 公约

16. 本公约“的主要目的是(1)协调网络犯罪领域的国内刑事实体法要件和相关规定；(2)规定调查和起诉此类犯罪以及通过计算机系统实施的其他犯罪或电子形式证据所需的国内刑事程序法权力；(3)建立一种快速有效的国际合作制度。

17. 因此，公约包含四章：(一)术语的使用；(二)在国内一级应采取的措施--实体法和程序法；(三)国际合作；(四)最后条款。

18. 第二章第一节(实体法问题)涵盖了计算机犯罪或与计算机有关的犯罪领域的刑事定罪条款和其他相关条款:它首先界定了分为 4 个不同类别的 9 种犯罪，然后论述了附带责任和制裁。本公约界定了下列犯罪：非法访问、非法截取、干扰数据、干扰系统、滥用设备、与

计算机有关的伪造、与计算机有关的欺诈、与儿童色情制品有关的犯罪以及与版权和邻接权有关的犯罪。

19. 第二章第二节(程序法问题)首先确定了适用于本章中所有程序权力的共同条件和保障措施，其范围超出了第 1 节中定义的犯罪，因为它适用于通过计算机系统实施的任何犯罪或其证据为电子形式。而后，它规定了以下程序性权力：加快保存已存储的数据，加快保存和部分披露流量数据，出示令，搜查和扣押计算机数据，实时收集流量数据；截取内容数据。第二章最后是关于管辖权的规定。

20. 第三章包括关于传统犯罪和与计算机犯罪有关的互助以及引渡规则的规定。它涵盖了两种情况下的传统互助：缔约国之间不存在法律依据(条约、对等立法等)——在这种情况下适用该章下的条款；若存在法律依据--在这种情况下，现行安排也适用于本公约下的协助。计算机或与计算机有关的犯罪的专项协助适用于这两种情况，并在附加条件的情况下涵盖第二章所界定的相同程序权力范围。此外，第三章载有一项关于跨境访问存储的计算机数据的特定类型的规定，该规定不需要相互协助(在征得同意或公开可获得的情况下)，并规定建立一个全天候网络，以确保缔约国之间迅速提供协助。

21. 最后，第四章包含最后条款，这些条款除了某些例外，重复了欧洲委员会条约中的标准条款。

对本公约条款的评述

第一章　术语的使用

第 1 条 定义介绍

22. 起草者认为，根据本公约，缔约国没有义务将第 1 条界定的四个概念逐字复制到其国内法中，只要这些法律以符合本公约原则的方式涵盖这些概念并为其实施提供同等的框架即可。

第一条(a)项　计算机系统

23. 本公约规定的计算机系统是一种由硬件和软件组成的设备，用于自动处理数字数据。它可能包括输入、输出和存储设施。它可以是独立的，也可以在网络中与其他类似的设备连接。“自动”意味着无需直接人工干预，“数据处理”意味着计算机系统中的数据是通过执行计算机程序来操作的。“计算机程序”是一组可由计算机执行以达到预期结果的指令。一台计算机可以运行不同的程序。计算机系统通常由不同的设备和外围设备组成，这些设备被区分为处理器或中央处理器。外围设备是与处理单元交互执行某些特定功能的设备，例如打印机、显示屏、光盘读取器/写入器或其他存储设备。

24. 网络是两个或多个计算机系统之间的互连。这些连接可以是接地的(例如，电线或电缆)、无线的(例如，无线电、红外或卫星)或两者兼有。网络可以在地理上局限于小区域(局域网)，或者可以跨越大区域(广域网)，并且这类网络本身可以互连。互联网是由许多互连的网络组成的全球网络，所有这些网络都使用相同的协议。存在其他类型的网络，无论是否连接到互联网，都能够在计算机系统之间传送计算机数据。计算机系统可以作为端点或作为辅助网络的通信手段连接到网络。最重要的是数据是通过网络交换的。

第一条(b)项　计算机数据

25. 计算机数据的定义建立在国际标准化组织数据定义的基础上。该定义包含术语“适合加工”。这意味着数据以一种可以被计算机系统直接处理的形式存在。为了明确本公约中的

数据必须理解为电子形式或其他可直接处理的形式的数据，采纳了“计算机数据”这一概念。自动处理的计算机数据可能是本公约所界定的一项刑事犯罪的目标，也可能是适用本公约所界定的一项调查措施的对象。

第一条(c)项　服务供应商

26.术语“服务供应商”包括在计算机系统上的数据通信或处理方面发挥特殊作用的广泛类别的人员(参见第二节的评述)。根据该定义第(1)目，它明确表明，为用户提供相互通信能力的公共和私人实体都包括在内。因此，用户是否形成一个封闭的群体，或者供应商是否向公众提供服务，无论是免费还是收费，都无关紧要。封闭群可以是，例如由公司网络向其提供服务的私有企业的员工。

27.根据该定义的第(2)目，“服务供应商”一词亦包括那些代表第(1)目所述人士储存或以其他方式处理数据的实体。此外，该术语还包括代表第(1)目所述服务的用户存储或以其他方式处理数据的实体。例如，根据该定义，服务供应商既包括提供托管和缓存等的服务，也包括提供网络连接的服务。然而，如果仅仅是内容提供者(例如，与网络托管公司签约托管其网站的人)而不提供通信或相关数据处理服务，则不属于该定义旨在包括的范围。

第 1 条(d)项　流量数据

28.就本公约而言，第 1 条(d)项所定义的流量数据是受特定法律制度管辖的一类计算机数据。这类数据是由通信链中的计算机生成的，以便将通信从起点路由到目的地。因此，它对通信本身是辅助的。

29.在调查与计算机系统有关的刑事罪行时，需要流量数据以追查通讯来源，作为收集进一步证据的起点，或作为犯罪证据的一部分。流量数据可能只持续短暂时间，因此有必要对其进行快速保存。因此，为了在删除之前收集更多证据或识别嫌疑人，可能有必要快速披露它，以辨别通信的路线。因此，收集和披露计算机数据的普通程序可能是不够的。此外，流量数据的收集在原则上被认为是侵扰行较小的，因为它并不披露被认为更敏感的通信内容。

30.该定义详尽地列出了本公约中特定制度处理的流量数据类别：通信来源、目的地、路径、时间(格林威治标准时间)、日期、大小、持续时间和基本服务类型。并非所有这些类别在技术上都是可用的，能够由服务供应商提供，或者是特定刑事调查所必需的。“来源”指的是服务供应商向其提供服务的通信设施的电话号码、网际协议(IP)地址或类似标识。“目的地”指的是通信被发送到的通信设施的类似指示。术语“基础服务类型”指的是网络内正在使用的服务类型，例如文件传输、电子邮件或即时通信。

31.这一定义允许各国立法机构有权根据流量数据的敏感性在法律保护方面采取差别化。在这方面，第 15 条规定缔约国有义务提供足以保护人权和自由的条件和保障。这意味着，除其他外，适用调查权的实质性标准和程序可能会因数据的敏感性而异。

第二章　国家一级应采取的措施

32.第二章(第 2 至 22 条)包括三节：实体法(第 2 至 13 条)、程序法(第 14 至 21 条)和管辖权(第 22 条)。

第 1 节　实体刑法

33. 本公约第 1 节(第 2 至 13 条)的目的是通过确定有关犯罪的共同最低限度标准，改进预防和制止计算机或与计算机有关的犯罪的手段。这种协调减轻了在国家和国际层面打击此类犯罪方面的难度。国内法的对应性可以防止滥用行为转移到以前标准较低的缔约国。因此，也可以加强在实际处理案件中交流有用的共同经验。国际合作(特别是引渡和司法互助)得到促进，例如关于双重犯罪的要求。

34. 所列罪行清单代表了不排除国内法延伸的最低共识。它在很大程度上依据的是欧洲委员会关于计算机犯罪的第 R(89)9 号建议以及其他公共和私营国际组织(经合组织、联合国、国际刑法协会)的工作制定的准则，但也考虑到当代应对不断扩大的滥用电信网络方面的经验。

35. 本节分为五个篇目。篇目 1 包括计算机相关的核心犯罪，即破坏计算机数据和系统的保密性、完整性和可用性的犯罪行为，反映了在关于计算机和数据安全的讨论中确定的电子数据处理和通信系统面临的基本威胁。该篇目描述了涵盖的犯罪类型，即未经授权访问和非法篡改系统、程序或数据。篇目 2 至 4 包括其他类型的“与计算机有关的犯罪”，这些犯罪在实践中所起的作用更大，计算机和电信系统被用作攻击某些合法利益的手段，而这些利益大多已经受到刑法的保护，不会受到使用传统手段的攻击。遵循欧洲委员会第 R(89)9 号建议准则中的建议，增加了篇目 2 犯罪(与计算机有关的欺诈和伪造)。篇目 3 涵盖了“利用计算机系统非法制作或传播儿童色情制品有关的犯罪行为”，这是近年来最危险的作案方式之一。公约起草委员会讨论了将其他与内容有关的罪行包括在内的可能性，例如通过计算机系统传播种族主义宣传。然而，委员会无法就此类行为的刑事定罪达成共识。虽然有很大一部分人赞成将此列为刑事犯罪，但一些代表团以言论自由为由对列入这一条款表示强烈关切。考虑到问题的复杂性，委员会决定将起草一项公约附加议定书的问题提交犯罪问题委员会处理。

篇目 4“有关侵犯版权和相关权利的犯罪行为”之所以被列入公约，是因为侵犯版权是最普遍的计算机或与计算机有关的犯罪形式之一，其恶化之势正在引起国际的关注。最后，篇目 5 包括关于企图、协助或教唆以及制裁和措施的补充规定，它们符合近年来国际文书关于法人责任的规定。

36. 虽然实体法条款涉及使用信息技术的犯罪，但本公约使用了技术中性的语言，以便实质性刑法罪行既可以适用于当前涉及的技术，也可以适用未来涉及的技术。

37. 本公约起草者认为，缔约国可以将轻微或微不足道的不当行为排除在实施第 2 至 10 条所界定的罪行之外。

38. 所列罪行的一个具体特点是明确要求涉及的行为是“无权”实施的。它反映了这样一种观点，即所描述的行为本身并非一向应受到制裁，不仅在传统的法律辩护适用的情况下，如同意、自卫或必要性，而且在其他原则或利益导致排除刑事责任的情况下，可能是合法或正当的。“无权”一词的含义来源于使用它的上下文。因此，在不限制缔约国如何根据其国内法实施这一概念的情况下，它可以指未经授权(无论是立法、政府、行政、司法、合同还是双方同意)实施的行为，或者国内法中已确立的法律辩护、借口、理由或相关原则未涵盖的行为。因此，本公约没有影响根据合法政府权力采取的行为(例如，在缔约国政府采取行动维护公共秩序、保护国家安全或调查刑事犯罪时)。此外，网络设计中固有的合法和常见的活动，或合法和常见的运营或商业做法不应被定为犯罪行为。下文解释性备忘录的相应案文针对具体罪行提供了这种刑事定罪例外情况的具体例子。应由缔约国决定如何在其国内法律体系中(根据刑法或其他法律)实施此类豁免。

39. 本公约所载的所有罪行都必须是“故意”实施的，才能适用刑事责任。在某些情况下，额外的特定故意要件构成犯罪的一部分。例如，在关于计算机相关欺诈的第 8 条中，获取

经济利益的意图是犯罪的一个构成要件。本公约起草者一致认为，“故意”的确切含义应由各国解释。

40. 该节的某些条款允许国内法在执行本公约时增加限定情况。在其他情况下，甚至允许有保留的可能性(参见第 40 和 42 条)。在刑事定罪方面，这些限制性更强的不同方式反映了对所涉行为的危险性或使用刑法作为反措施的必要性的不同评估。这种做法为各国政府和议会在决定在这一领域的刑事政策提供了灵活性。

41. 起草确定这类罪行的法律应尽可能明确和具体，以便对将导致刑事制裁的行为类型提供足够的可预见性。

42. 在起草过程中，起草者审议了将第 2 至 11 条界定的行为以外的行为定为刑事犯罪的可取性，包括所谓的网络抢注，即注册的域名要么与已经存在且通常为人们熟知的实体名称相同，要么与产品或公司的商号或商标相同。网络抢注者无意积极使用该域名，并试图通过迫使有关实体(即使是间接的)支付域名所有权转让费来牟利。目前，这一行为被认为是与商标有关的问题。由于商标侵权不受本公约管辖，起草者认为不宜处理将此类行为定为刑事犯罪的问题。

篇目 1--破坏计算机数据和系统的保密性、完整性和可用性的犯罪行为

43. 第(2 至 6)条界定的刑事犯罪旨在保护计算机系统或数据的保密性、完整性和可用性，而不是将网络设计中固有的合法和常见活动，或合法和常见的操作或商业做法定为刑事犯罪。

非法访问(第 2 条)

44. “非法访问”包括对计算机系统和数据的安全(即保密性、完整性和可用性)的严重威胁和攻击这一基本罪行。保护的需要反映了组织和个人以不受干扰和不受限制的方式管理、操作和控制其系统的利益所在。纯粹未经授权的入侵，即“黑客入侵”、“破解”或“计算机入侵”，原则上本身就是非法的。这可能会给系统和数据的合法用户造成障碍，并可能导致更改或破坏，造成高昂的重建费用。这种入侵可能会让黑客获得机密数据(包括密码、目标系统的信息)和秘密，造成无偿使用系统，甚至鼓励黑客实施与计算机相关的更危险的犯罪，如计算机相关的欺诈或伪造。

45. 当然，防止未授权访问的最有效方法是引入和开发有效的安全措施。然而，全面的应对措施还必须包括威慑和使用刑法措施。禁止未经授权访问的刑事禁令能够在早期阶段对系统和数据提供额外的保护，防止上述危险。

46. “访问”包括进入计算机系统的全部或任何部分(硬件、组件、已安装系统的存储数据、目录、流量数据和与内容相关的数据)。但它不包括仅向该系统发送电子邮件或文件。“访问”包括进入通过公共电信网络连接的另一计算机系统，或进入同一网络上的计算机系统，例如一个组织内的局域网(LAN)或内部网(Intranet)。通信方式(例如，远距离，包括通过无线链路或近距离)并不重要。

47. 该行为也必须是“无权”实施的。除了以上对此表述的解释外，这意味着没有将系统或其部分的所有者或其他权利持有人经授权的访问(例如为了授权测试或保护有关的计算机系统)定为刑事犯罪。此外，访问允许公众免费开放访问的计算机系统并不构成犯罪，因为这种访问是“有权的”。

48.特定技术工具的应用可能导致根据第 2 条直接或通过超文本链接访问网页，包括深度链接或应用“浏览记录(cookies)”或“机器人(bots)”来查找和检索代表通信的信息。使用这些工具的本身并非“无权”。公共网站的维护意味着网站拥有者同意任何其他网站用户都可以访问该网站。在通常应用的通信协议和程序中提供的标准工具的应用本身并非是“无权”的，特别是当被访问系统的权利持有者已视为接受了这种应用软件，例如在不拒绝初始安装或不移除安装“浏览记录”的情况下。

49.许多国家的法律已经包含了关于“黑客”犯罪的规定，但范围和构成要件差别很大。第 2 条首句中宽泛的刑事定罪方式并非无可争议。反对意见源于这种情况，即仅仅入侵并没有造成危险，甚至黑客行为也导致了对系统安全漏洞和弱点的检测。这导致许多国家采取了一种要求附加限定条件的较窄方法，这也是第(89)9 号建议和经合组织工作组 1985 年的建议所采用的方法。

50.根据第 2 条第一句，缔约国可以采取较宽泛的方法，将单纯的黑客行为定为犯罪。或者，缔约国可以附上第二句中列出的所有或任何限定要件:违反安全措施、获取计算机数据的特殊意图、证明刑事责任的其他不诚实意图，或犯罪与远程连接到另一个计算机系统的计算机系统有关的要求。最后一种选择允许缔约国排除一个人在不使用另一个计算机系统的情况下实际访问一台独立计算机的情况。缔约国可将将犯罪局限于非法访问联网计算机系统这一范围(包括电信服务提供的公共网络和专用网络，如内联网或外联网)。

非法截取(第 3 条)

51.该条款旨在保护数据通信的隐私权。这一犯罪行为与传统窃听和记录人与人之间的口头电话交谈一样，是对通信隐私的侵犯。通信隐私权载于《欧洲人权公约》第 8 条。第 3 条确定的犯罪行为将这一原则适用于所有形式的电子数据传输，无论是通过电话、传真、电子邮件还是文件传输。

52.该条文的内容主要取自建议(89)9 所载的“未经授权截取”犯罪。在本公约中，已经明确规定，在下列情况下，所指的通信涉及“计算机数据的传输”以及电磁辐射。

53.通过"技术手段"进行的截取涉及监听、监测或监视通信内容，直接通过访问和使用计算机系统获取数据内容，或间接通过使用电子窃听或窃听装置获取数据内容。截取也可能涉及录音。技术手段包括固定在传输线路上的技术设备以及收集和记录无线通信的设备。它们可能包括软件、密码和代码的使用。使用技术手段这一要求是避免过度定罪的限制性条件。

54.该罪行适用于计算机数据的“非公开”传输。术语“非公开”限定了传输(通信)过程的性质，而不是传输的数据的性质。所传送的数据可能是公开的信息，但当事方希望以保密方式传送。或者，数据可能出于商业目的在付服务费之前保密，如同付费电视一样。因此，“非公共”一词本身并不排除通过公共网络进行通信。根据第 3 条，员工之间的通信，无论是否出于商业目的，构成“计算机数据的非公开传输”，也受到保护，不得在无权情况下被截取(见“欧洲人权法院对哈福德诉英国案的判决”，1997 年 6 月 25 日，20605/92)。

55.计算机数据传输形式的通信可以发生在单个计算机系统内部(例如，主机与屏幕或打印机之间)、属于同一人的两个计算机系统之间、两台计算机之间相互通信、或者一台计算机与人之间(例如，通过键盘)。尽管如此，缔约国可要求在远程连接的计算机系统之间传输通信作为附加要件。

56.应当指出的是，“计算机系统”的概念可能也包括无线电连接，但这并不意味着缔约方有义务将截取任何无线电传输的行为定为刑事犯罪，因为这种传输即使是“非公开”的，也是以相对公开和容易获取的方式进行的，因此可以截取，例如无线电业余爱好者所为。

57. 设定与“电磁辐射”有关的犯罪行为将确保范围更为全面。计算机在运行过程中可能会发出电磁辐射。根据第 1 条的定义，这类发射不被视为“数据”。然而，从这种发射中可以重建数据。因此，根据这项规定，从计算机系统电磁辐射中截取数据属于犯罪行为。

58. 要追究刑事责任，非法截取必须是“故意”和“无权”实施的。例如，如果截取者有权这样做，如果他按照传输参与者的指示或授权采取行动(包括参与者同意的授权测试或保护活动)，或者如果为了国家安全或侦察机关侦查犯罪而合法授权进行监视，那么这种行为是正当的。另据了解，对使用常见的商业做法，如利用“浏览记录”，无意将其定为刑事犯罪，因为这不属于“无权”截取。关于受第 3 条保护的员工之间的非公开通信(见上文第 54 段)，国内法可为合法截取此类通信提供理由。根据第 3 条，在这种情况下进行的截取将被视为“有权”进行。

59. 在一些国家，截取可能与未经授权访问计算机系统的犯罪密切相关。为了确保使禁止与适用法律相一致，那些要求具备不诚实意图，或要求根据第 2 条所实施的犯罪涉及某一计算机系统连接到另一个计算机系统的国家，也可以要求在本条中附加刑事责任的类似限定要件。这些要件应与犯罪的其他要件，例如“故意”和“无权”，一起解释和适用。

数据干扰(第 4 条)

60. 这项规定的目的是为计算机数据和计算机程序提供类似于有形物体享有的保护，防止故意造成损害。这里受保护的合法利益是存储的计算机数据或计算机程序的完整性和正常运行或使用。

61. 在第 1 款中，“破坏”和“恶化”作为重叠的行为，特别涉及对数据和程序的完整性或信息内容的有害改变。“删除”数据相当于毁掉一个有形物。它毁掉了数据，使数据无法辨认。压制计算机数据是指任何阻止或终止有权访问计算机的人或存储数据的数据载体可使用数据的行为。术语“更该”是指对现有数据的修改。因此，输入恶意代码(如病毒和特洛伊木马)以及由此引起的数据修改均为本款所涵盖。

62. 上述行为只有在“无权”情况下才会受到制裁。网络设计或常见的运营或商业惯例中固有的经常活动，例如由其所有者或运营商授权的对计算机系统的安全性或其保护的测试，或者当系统的运营商安装新软件(例如，允许访问互联网的软件而禁用先前安装的类似程序)时发生的计算机操作系统的重新配置，都属于合法行为，因此本条没有将它们定为刑事犯罪。为方便匿名通信(如匿名转发系统的活动)而修改流量数据，或为安全通信(如加密)而修改数据，原则上应被视为对隐私的合法保护，因此，应被视为有权行为。然而，缔约国可能希望将某些与匿名通信有关的滥用行为定为刑事犯罪，例如，为了隐瞒犯罪人的身份而更改数据包报头的信息。

63. 此外，违法者的行为一定是“故意”而为的。

64. 第 2 款允许缔约国就该罪行提出保留，它们可以要求该行为造成了严重损害。对什么构成这种严重损害的解释由国内立法决定，但如果利用这一保留的可能，缔约国应将其解释通知欧洲委员会秘书长。

系统干扰(第 5 条)

65. 在建议(89)9 中它被称为计算机破坏行为。该条款旨在将通过使用或影响计算机数据而故意妨碍合法使用计算机系统包括电信设施的行为定为犯罪。受保护的合法权益是指计算机或电信系统的运营商和用户能够使其正常运行的权益。该文本是以中性的方式制定的，因此所有类型的功能都可以受到它的保护。

66. 术语“妨碍”是指干扰计算机系统正常运行的行为。这种妨碍必须通过输入、传输、损坏、删除、更改或压制计算机数据来实现。

67. 此外，妨碍必须是“严重的”，才能引发刑事制裁。各缔约国均应自行决定必须满足哪些标准才能将妨碍视为“严重”。例如，缔约国可能要求造成最低限度的损害，才能视为严重妨碍。起草者认为，向特定系统发送数据的形式、大小或频率对所有者或运营商使用该系统或与其他系统通信的能力有重大有害影响(例如，通过生成“拒绝服务”的攻击程序、阻止或大幅减缓系统运行的病毒等恶意代码，或向接收者发送大量电子邮件以阻止系统的通信功能的程序)，都被认为是“严重的”。

68. 妨碍必须是“无权”的。网络设计中固有的常见活动或常见的运营做法或商业惯例都是有权的。这些包括例如由其所有者或运营商授权的对计算机系统的安全性或其保护的测试，或者当系统的运营商安装新软件而禁用先前安装的类似程序时发生的计算机操作系统的重新配置。因此，即使这种行为造成严重妨碍，本条也未将其定为刑事犯罪。

69. 出于商业或其他目的，未经请求发送电子邮件可能会对收件人造成滋扰，特别是当大量发送或频繁发送此类信息时(“垃圾邮件”)。起草人认为，只有在故意和严重妨碍通信的情况下，才应将此类行为定为刑事犯罪。尽管如此，缔约国可能根据其法律对妨碍采取不同的做法，例如将特定的干涉行为定为行政违法行为，或以其他方式加以制裁。条文让缔约国决定应在多大程度上(部分或全部、暂时或永久)妨碍系统的运作算达到损害门槛，因而依照法律有理由施以行政或刑事制裁。

70. 犯罪必须是故意的，即行为人必须具有严重妨碍的意图。

滥用设备(第 6 条)

71. 该条款将故意实施针对某些设备或访问数据的具体非法行为定为单独和独立的刑事犯罪，这些设备或访问数据被滥用于实施上述破坏计算机系统或数据的保密性、完整性和可用性的犯罪。由于犯下这些罪行往往需要拥有访问手段(“黑客工具”)或其他工具，因此有强烈的动机为犯罪目的获取这些工具，这可能导致在这些工具的生产和分销中形成一种黑市。为了更有效地打击这种危险，刑法应在第 2 至第 5 条所述犯罪实施之前，从源头上禁止特定的潜在危险行为。在这方面，该条款借鉴了欧洲委员会(《关于对基于或包含有条件获取的服务进行法律保护的欧洲公约》--《欧洲条约集》第 178 号)和欧洲联盟内部近年来的发展(欧洲议会和欧洲委员会 1998 年 11 月 20 日“关于基于或由有条件准入构成的服务的法律保护”的第 98/84/(E)(C)号指令)以及一些国家的相关规定。1929 年日内瓦《防止伪造货币国际公约》也采取了类似的方法。

72. 第 1 款(a)项(1)目将主要为实施本公约第 2 至第 5 条确定的任何犯罪目的而设计或改装的装置，包括计算机程序的生产、销售、采购以供使用、进口、分发或以其他方式提供定为犯罪行为。“分发”是指主动将数据转发给他人，而“提供”是指将设备放在网上供他人使用。该术语还旨在涵盖创建或编译超链接以方便访问此类设备。列入“计算机程序”指的是，例如为更改或甚至破坏数据或干扰系统操作而设计的程序，诸如病毒程序，或者设计成或适合于进入计算机系统的程序。

73. 起草者对这些装置是否应仅限于专门为犯罪而设计的装置，进而排除双重用途的装置开展了深入讨论。这被认为覆盖面过窄。这可能会导致刑事诉讼中难以克服的举证困难，使该条款实际上不适用，或者只在极少数情况下适用。备选办法是将即便合法生产和分发的所有设备都包括在内，但这种选择也被拒绝了。只有意图从事计算机犯罪的主观要件才成为是否加以制裁的决定条件，在伪造货币方面尚未采用这种做法。本公约作为一种合理的折衷办法，将其范围限于主要为了犯罪而客观设计或改装设备的情况。仅此一项通常就会排除双重用途设备。

74. 第 1 款(a)项(2)目将生产、销售、采购以供使用、进口、分发或以其他方式提供计算机密码、访问码或类似数据(借助它们可以访问整个计算机系统或其任何部分)的行为定为刑事犯罪。

75. 第 1 款(b)项将拥有第 1 款(a)项(1)目或(2)目所列的物品定为犯罪。根据第 1 款(b)项的最后一句，允许缔约国依法要求拥有若干此类物品。拥有的物品数量直接证明了犯罪意图。承担刑事责任所需的物品数量由各缔约国自行决定。

76. 这项罪行的要求是无权且故意实施的。为了避免过度定罪的危险，即出于合法目的生产设备并将其投放市场，例如反击对计算机系统的攻击，增加了进一步的限定犯罪的要件。除了一般意图要求之外，还必须有具体(即直接)的意图，即该设备用于实施本公约第 2 至第 5 条所确立的任何犯罪行为。

77. 第 2 款明确规定，为授权测试或保护计算机系统而开发的工具不在该条款的涵盖范围之内。这一概念已经包含在“无权”的表述中。例如，工业界为控制其信息技术产品的可靠性或测试系统安全性而设计的测试设备(“破解设备”)和网络分析设备都是为合法目的而生产的，故被视为“有权”。

78. 由于对第 2 至第 5 条中所有不同类型的计算机犯罪行为适用“滥用设备”罪的必要性有不同意见，第 3 款允许在保留的基础上(参见第 42 条)在国内法中限定该项罪行。然而，各缔约国有义务至少将第 1 款(a)项(2)目所述的销售、分发或提供计算机密码或访问数据定为犯罪。

篇目 2--与计算机有关的犯罪行为

79. 第 7 至第 10 条涉及常常通过使用计算机系统实施的普通犯罪。大多数国家已经将这些普通犯罪定为刑事犯罪，其现行法律有可能足够宽泛，也有可能不够宽泛，无法扩展到涉及计算机网络的情况(例如，一些国家的现行儿童色情制品法可能无法扩展到电子图像)。因此，在执行这些条款的过程中，各国必须审查其现行法律，以确定它们是否适用于涉及计算机系统或网络的情况。如果现有的罪行已经涵盖这种行为，就没有必要修改现有的罪行或颁布新的罪行。

80. “与计算机有关的伪造”和“与计算机有关的欺诈”涉及某些与计算机有关的犯罪，即与计算机有关的伪造和与计算机有关的欺诈，作为操纵计算机系统或计算机数据的两种具体类型。将它们列入承认了这样一个事实，即在许多国家，某些传统合法利益没有受到充分保护，难以免受新形式的干扰和攻击。

与计算机有关的伪造(第 7 条)

81. 该条的目的是确立与伪造有形文件类似的罪行。它旨在填补刑法中与传统伪造有关的空白，传统伪造要求文件中包含的陈述或声明具有视觉可读性，而不适用于电子存储的数据。如果第三方因此受到误导，操纵此类具有证据价值的数据可能会产生与传统伪造行为相同的严重后果。与计算机有关的伪造涉及未经授权创建或更改存储的数据，以便在合法交易过程中获得不同的证据价值，这取决于数据中包含的信息的真实性，它会被欺骗。受保护的合法权益是可能对法律关系产生影响的电子数据的安全性和可靠性。

82. 应当指出的是，各国对伪造的概念差异很大。一种概念是基于文档作者的真实性，而其他概念则是基于文档中所含陈述的真实性。然而，各方一致认为，关于真实性的欺骗至少

是指数据的发布者，而不理会数据内容的正确性或真实性。缔约国可以更进一步在“真实”一词下包括数据的真实性。

83. 这项规定涵盖等同于具有法律效力的公共或私人文件的数据。未经授权“输入”正确或不正确的数据会导致相当于伪造文件的情况。随后的更改(修改、变更、部分改正)、删除(从数据介质中删除数据)和抑制(保留、隐藏数据)通常相当于伪造真实文档。

84. “出于法律目的”一词也指法律上相关的合法交易和文件。

85. 该条款的最后一句允许缔约国在国内法审判犯罪时，在附加刑事责任之前，另外要求有欺诈意图或类似的不诚实意图。

与计算机有关的欺诈(第 8 条)

86. 随着技术革命的到来，实施诈骗(包括信用卡诈骗)等经济犯罪的可能成倍增加。在计算机系统中代表或管理的资产(电子基金、存款)已经像传统形式的财产一样成为被操纵的目标。这些犯罪主要包括输入操纵，即向计算机输入不正确的数据，或通过程序操纵和其他干扰数据处理过程的方式。该条的目的是将数据处理过程中任何意图非法转移财产的不当操纵行为定为犯罪。

87. 为确保涵盖所有可能的相关操作，第 8 条(a)项中的“输入”、“更改”、“删除”或“抑制”的构成要件由第 8 条(b)项中“对计算机程序或系统运行的任何干扰”的一般行为加以补充。“输入、更改、删除或抑制”的要件与前几条中的含义相同。第 8 条(b)涵盖了诸如硬件操作、抑制打印输出的行为以及影响数据记录或流动或程序运行顺序的行为。

88. 如果计算机欺诈操作造成他人财产的直接经济损失或占有损失，并且肇事者的行为意图是为本人或他人非法牟取经济收益，则计算机欺诈操作行为被定为犯罪。“财产损失”是一个广义的概念，包括金钱、有形资产和具有经济价值的无形资产的损失。

89. 犯罪必须是“无权”实施的，经济利益必须是无权获得的。当然，旨在获取经济利益的通行合法商业做法因有权从事，并不包括在本条确定的犯罪行为中。例如，根据受影响人员之间的有效合同开展的活动是有权进行的(例如，根据合同条款有权禁用网站)。

90. 犯罪必须是“故意”实施的。一般意图要件是指造成他人财产损失的计算机操纵或干扰。该罪行还要求有特定的欺诈或其他不诚实意图，以便为本人或他人牟取经济利益或其他利益。因此，例如，可能对一人造成经济损害并使另一人受益，但并非出于欺诈或不诚实意图从事的与市场竞争有关的商业行为，不应包括在本条确定的犯罪行为中。例如，使用信息收集程序在互联网上进行比较购物(“机器人”)，即使没有得到“机器人”访问的网站的授权，也不会被定罪。

篇目 3--与内容有关的犯罪行为

与儿童色情制品有关的犯罪行为(第 9 条)

91. 关于儿童色情制品的第 9 条旨在加强对儿童的保护措施，包括保护他们免受性剥削，方法是更新刑法条款，更有效地限制使用计算机系统对儿童实施性犯罪。

92. 这项规定回应了欧洲委员会国家元首和政府首脑在其第二次首脑会议(1997 年 10 月 10 日至 11 日，斯特拉斯堡)的行动计划(项目三.4)中表达的关注，并符合寻求禁止儿童色情

制品的国际趋势，最近通过的《<联合国儿童权利公约>关于买卖儿童、儿童卖淫和儿童色情制品的任择议定书》和欧洲委员会最近“关于打击对儿童的性剥削和儿童色情制品倡议”(C)OM2000/854)就是证明。

93.该条款将儿童色情制品的电子制作、拥有和传播的各个方面定为犯罪。大多数国家已经将儿童色情制品的传统制作和实物散发定为刑事犯罪，但随着越来越多地使用互联网作为交易这类材料的主要工具，人们强烈认为，国际法律文书中的具体规定对于打击这种新形式的对儿童的性剥削和危害至关重要。人们普遍认为，这种材料和网上做法，例如在恋童癖者之间交流想法、幻想和建议，在支持、鼓励或便利针对儿童的性犯罪方面发挥了作用。

94.第 1 款(a)项将为通过计算机系统达到传播目的制作儿童色情制品定为犯罪。为了从源头上消除上述危险，这一规定是必要的。

95.第 1 款(a)项将为传播目的通过计算机系统制作儿童色情制品定为犯罪。“推送”意在涵盖引诱他人获取儿童色情制品。这意味着推送材料的人实际上可以提供材料。“提供”意在涵盖将儿童色情物品放在网上供他人使用，例如通过创建儿童色情网站的方式。该款还旨在涵盖创建或编辑指向儿童色情网站的超链接，以方便访问儿童色情网站。

96.第 1 款(c)项将通过计算机系统散发或传播儿童色情制品定为犯罪。“散发”是材料的主动传播。通过计算机系统向他人发送儿童色情制品将被定为“传播”儿童色情制品罪。

97.第 1 款(d)项中的“为本人或他人获得”一词系指主动获取儿童色情制品，例如通过下载。

98.第 1 款(e)项将在计算机系统或诸如软盘或光盘等数据载体上拥有儿童色情制品定为犯罪。拥有儿童色情制品刺激了对此类材料的需求。遏制儿童色情制品生产的一个有效方法是对从生产到拥有这一链条中每个参与者的行为订立刑事后果。

99.第 2 款中的“色情材料”一词适用国家标准对淫秽物品、不符合公共道德的物品或类似的腐败物品作出的分类。因此，具有艺术、医学、科学或类似价值的材料可被视为非色情材料。视觉描绘包括存储在计算机磁盘或其他电子存储装置中的数据，这些数据能够转换成视觉图像。

100.“露骨的性行为”至少包括真实或模拟的性行为：(a)同性或异性之间的性交，包括未成年人之间或成年人与未成年人之间的生殖器与生殖器、口腔与生殖器、生殖器与肛门或口腔与肛门之间的性交；(b)兽交；(c)手淫；(d)性虐待狂虐待或受虐狂虐待；或(e)对未成年人性器官或耻骨区的任何猥亵展示。描述的行为真实还是模拟无关紧要。

101.为触犯第 1 款所载罪行而由第 2 款界定的三类材料涵盖：对儿童进行性虐待的真实描述(第 2 款(a)项)；描绘貌似未成年人进行露骨性行为的色情图片(第 2 款(b)项)：以及最后，看似“真实”，但实际上并不涉及真的儿童进行露骨性行为的图像(第 2 款(c)项)。后一种情况包括被修改过的图片，例如自然人的变形图像，甚至完全由计算机生成的图像。

102.在第 2 款涵盖的三种情况下，受保护的合法权益略有不同。第 2 款(a)项更直接地侧重于防止虐待儿童。第 2 款(b)项和(c)项旨在提供保护，防止某些行为，这些行为虽然不一定会对材料中描述的"儿童"造成伤害，因为虽然没有真实的儿童，但可能会被用来鼓励或引诱儿童参与此类行为，从而成为助长虐待儿童的亚文化的一部分。

103.“无权”一词并不排除在特定情况下免除某人责任的法律辩护、借口或类似的相关原则。因此，“无权”一词允许缔约国考虑基本权利，如思想自由、言论自由和隐私。此外，缔约国可为与具有艺术、医学、科学或类似价值的“色情材料”有关的行为提供免责辩护。

关于第 2 款(b)项，“无权”的提法也可以允许，例如，缔约国可规定，如果确定所描绘的人不是本规定意义上的未成年人，则免除其刑事责任。

104. 根据联合国《儿童权利公约》(第 1 条)中"儿童"的定义，第 3 款将儿童色情制品中的"未成年人"定义为所有 18 岁以下的人。制定统一的国际年龄标准被视为一个重要的政策问题。需要注意的是，年龄是指使用(真实的或虚构的)儿童作为性对象的年龄，与同意发生性关系的年龄是分开的。然而，认识到某些国家在关于儿童色情制品的国家立法中要求有较低的年龄限制，第 3 款最后一句允许缔约国要求不同的年龄限制，但不得低于 16 岁。

105. 该条列出了与儿童色情有关的不同类型的非法行为，如第 2 至 8 条所述，缔约国有义务将"故意"实施的行为定为刑事犯罪。根据这一标准，任何人除非有意推送、提供、散发、传播、制作或拥有儿童色情制品，否则不承担法律责任。各缔约国可采用更具体的标准(例如，参见涉及服务供应商责任的欧洲共同体适用法律)，在这种情况下，以该标准作准。例如，如果“了解和控制”传输或存储的信息，就可能要承担责任。例如，在特定情况下，如果缺少国内法规定的意图，服务供应商充当包含此类材料的网站或新闻编辑室的渠道或宿主是不够的。此外，不要求服务供应商为避免刑事责任监控行为。

106. 第 4 款允许缔约国对第 1 款(d)项和(e)项以及第 2 款(b)项和(c)项作出保留。可以部分或全部动用不适用本条款上述部分的权利。根据第 42 条，任何此类保留应在缔约国签署时或交存批准书、接受书、核准书或加入书时向欧洲委员会秘书长申明。

篇目 4--有关侵犯版权和相关权利的犯罪行为

有关侵犯版权和相关权利的犯罪行为(第 10 条)

107. 侵犯知识产权，特别是侵犯版权，是互联网上最常见的犯罪行为，引发版权所有人和从事计算机网络专业工作者的担忧。未经版权人许可，在互联网上复制和传播受保护作品的情况极为频繁。受保护的作品包括文学、摄影、音乐、音像等作品。由于数字技术和在电子网络环境下复制和传播的规模之大，未经授权的拷贝很容易被复制和传播，因此有必要列入关于刑法制裁的规定，并加强这一领域的国际合作。

108. 各缔约国均有义务将故意侵犯由本条所列协议引起的版权和相关权(有时称为邻接权)的行为定为刑事犯罪，这些侵权行为是通过计算机系统和商业规模实施的。第 1 款规定了对通过计算机系统侵犯版权行为的刑事制裁。在几乎所有的国家，侵犯版权均属于一种犯罪行为。第 2 款涉及通过计算机系统侵犯相关权利的问题。

109. 侵犯版权和相关权利的行为是按照各缔约国的法律并根据该缔约国对某些国际文书承担的义务来界定的。虽然要求各缔约国将这些侵权行为确定为刑事犯罪，但各国国内法中对此类侵权行为的确切界定方式可能各所不同。然而，本公约规定的刑事定罪义务不包括第 10 条明确处理的知识产权侵权行为，因此排除了与专利或商标有关的侵权行为。

110. 关于第 1 款，提到的协定是指 1971 年 7 月 24 日关于《保护文学和艺术作品伯尔尼公约》的《巴黎修订案文》、《与贸易有关的知识产权协定》和《世界知识产权组织版权条约》。关于第 2 款，援引的国际文书有《保护表演者、唱片制作者和广播组织国际公约》(《罗马公约》)、《与贸易有关的知识产权协定》和《世界知识产权组织表演和唱片条约》。两款中“根据其所承担的义务”一词的使用表明，本公约的缔约国没有义务适用其未加入的协定；此外，如果缔约国作出了其中一项协定允许的保留或声明，则该保留可限制其根据本公约所承担的义务的范围。

111. 在缔结本公约时，《知识产权组织版权条约》和《知识产权组织表演和录音制品条约》尚未生效。尽管如此，这些条约仍然很重要，因为它们大大更新了知识产权的国际保护(特别是关于在互联网上“按需提供”受保护材料的新的权利)，并改进了打击全球侵犯知识产权行为的手段。但是，有一项理解是，在这些条约对一缔约国生效之前，根据本公约，侵犯这些条约确立的权利不必然就是刑事犯罪。

112. 根据国际文书中所承担的义务将侵犯版权和相关权利定为犯罪的义务并不延伸至所述文书赋予的任何精神权利(如《伯尔尼公约》第 6 条之二和《世界知识产权组织版权条约》第 5 条)。

113. 侵犯版权和相关权利的行为必须“任意”才能适用刑事责任。与本公约所有其他实体法条款不同的是，第 1 款和第 2 款中都使用了“任意”一词，而不是“故意”，因为这是《与贸易有关的知识产权协定》(第 61 条)中使用的术语，管辖将侵犯版权定为犯罪的义务。

114. 这些条款旨在规定对“以商业规模”的侵权行为和通过计算机系统实施的刑事制裁。这符合《与贸易有关的知识产权协定》第 61 条，该条规定，只有在“具有商业规模的盗版”情况下，才需要在版权问题上进行刑事制裁。然而，缔约国可能希望超越“以商业规模”这一界限，将其他类型的侵犯版权行为也定为刑事犯罪。

115. 由于“侵犯”一词已经表示未经授权使用受版权保护的材料，因此在本文中省略了视为多余的“无权”一词。相反，少了“无权”一词并不意味着排除适用与本公约其他条款中“无权”一词有关的刑法辩护、理由和排除刑事责任的原则。

116. 第 3 款允许缔约国在“有限的情况下”(例如平行进口、租赁权)，只要有其他有效的补救措施，包括民事和(或)行政措施，即不追究第 1 款和第 2 款下的刑事责任。这一规定基本上允许缔约国有限地免除施加刑事责任的义务，只要它们不减损《与贸易有关的知识产权协定》第 61 条规定的义务，这是最低限度的现有刑事定罪要求。

117. 本条不得解释为将给予作者、电影制片人、表演者、录音制品制作者、广播组织或其他权利持有人的保护扩大到不符合国内法或国际协定规定的资格标准的人。

篇目 5--附带责任和制裁

企图和协助或教唆(第 11 条)

118. 本条的目的是确定与企图和协助或教唆实施本公约所界定的罪行有关的其他罪行。如下文进一步讨论的那样，不要求缔约国将实施本公约确立的每一项犯罪的企图定为犯罪。

119. 第 1 款要求缔约国将协助或教唆实施第 2 至 10 条所列任何罪行定为刑事犯罪。如果实施本公约所确立的犯罪的人得到另一个也有意实施犯罪的人的帮助，则产生协助或教唆的责任。例如，虽然通过互联网传输有害内容数据或恶意代码作为渠道需要服务供应商的协助，但根据本节没有犯罪意图的服务供应商不能承担责任。因此，服务供应商没有义务为避免根据本条款承担刑事责任主动监控内容。

120. 关于企图犯罪的第 2 款，本公约中界定的一些犯罪或这些犯罪的要件在概念上被认为难以企图(例如，推送或提供儿童色情制品的要件)。此外，一些法律制度对企图犯罪的制裁进行了限制。因此，只需就企图从事第 3、4、5、7、8、9 条 1 款(a)和(c)项确立的犯罪定为刑事犯罪。

121. 如同根据本公约确立的所有犯罪一样，企图和协助或教唆必须是故意实施的。

122. 增加第 3 款是为了解决缔约国在第 2 款方面可能遇到的困难，因为不同立法中的概念千差万别，尽管第 2 款将某些方面排除在企图条款之外。缔约国可声明保留全部或部分不适用第 2 款的权利。这意味着，对该条款作出保留的任何缔约国都没有义务将企图定为犯罪，或者可以选择它将对企图施加刑事制裁的犯罪或犯罪部分。这项保留旨在使本公约得到尽可能广泛的批准，同时允许缔约国保留其一些基本法律概念。

法人责任(第 12 条)

123 第 12 条涉及到法人的责任。它与当前承认法人责任的法律趋势相一致。它旨在规定公司、协会和类似的法人对其内部担任领导职务的人为该法人的利益而采取的犯罪行为负有责任。第 12 条还考虑到，如果该领导人员未能监督或控制法人的雇员或代理人，而这种失误又为该雇员或代理人实施本公约规定的某项罪行提供了便利，则应承担责任。

124. 根据第 1 款，需要满足四个条件才能承担赔偿责任。第一、必须犯下本公约所述的某项罪行。第二、该罪行必须是为法人的利益而实施的。第三、担任领导职务的人必须实施了该罪行（包括协助和教唆）。“担任领导职务的人”是指在组织中担任高级职务的自然人，如董事。第四、担任领导职务的人必须根据这些权力之一行事——代表权或作出决定的权力或行使控制权——这表明这种自然人是在其权力范围内行事，从而使法人承担责任。总而言之，第 1 款规定缔约方有能力只对这种主要人员犯下的罪行追究法人的责任。

125. 此外，第 2 款规定，如果犯罪不是由第 1 款所述的领导者实施的，而是由在法人授权下行事的另一人实施的，即在其权限范围内行事的该法人的一名雇员或代理人，则缔约国有义务追究法人的责任。承担责任必须具备的条件是：(1)法人的雇员或者代理人犯罪，(2)犯罪是为了法人的利益而实施的；(3)领导者因没有监督雇员或者代理人使犯罪成为可能。在这种情况下，未能监管应被解释为没有采取适当和合理的措施，防止雇员或代理人代表法人从事犯罪活动。这种适当和合理的措施可以由各种因素决定，例如企业的类型、规模、标准或既定的企业最佳做法等。这不应被解释为要求对雇员通信有一套全面监控制度(另见第 54 段)。服务供应商不会因为客户、用户或其他第三方在其系统上犯罪而承担责任，因为“在其授权下行事”一词仅适用于在其授权范围内行事的雇员和代理人。

126. 本条规定的责任可以是刑事、民事或行政责任。只要制裁或措施符合第 13 条第 2 款的标准，即属于“有效、相称和劝阻性的”，并包括罚款，各缔约国都可以根据各自的法律原则灵活选择规定所有或任何此类形式的责任。

127. 第 4 款澄清了法人责任不排除个人责任。

制裁和措施(第 13 条)

128. 这一条与第 2 至 11 条密切相关，这些条款定义了各种计算机或与计算机有关的犯罪，根据刑法这些犯罪应该受到制裁。依据上述条款规定的义务，该条规定缔约国有义务通过规定“有效、相称和劝阻性的”刑事制裁使这些犯罪依其严重性而引发后果，对于自然人，还有可能判处监禁。

129. 根据第 12 条确定其责任的法人也应受到“有效、相称和劝阻性的”制裁，这些制裁可以是刑事、行政或民事性质的。根据第 2 款，缔约国必须规定对法人实施货币制裁的可能性。

130. 该条保留了其他制裁或措施的可能性，以反映罪行的严重性，例如，措施可能包括禁令或没收。该条将自由裁量权留给缔约国，以建立一种与其现有国家法律制度相称的刑事犯罪和惩罚制度。

第 2 节　程序法

131. 本节中的条款介绍了在国家一级为对第 1 节规定的犯罪、通过计算机系统实施的其他刑事犯罪以及收集刑事犯罪的电子形式的证据进行刑事调查而采取的某些程序性措施。根据第 39 条第 3 款，本公约的任何规定均未要求或请缔约国设立本公约所载权力或程序以外的权力或程序，也不阻止缔约国这样做。

132. 技术革命包括“电子高速路”，使众多形式的通信和服务通过共享公共传输媒体和载体而相互关联和相互连接，也改变了刑法和刑事诉讼的领域。不断扩大的通信网络既为传统犯罪也为新技术犯罪打开了新的犯罪活动大门。不仅实体刑法必须跟上这些新的滥用行为的变化，刑事诉讼法和侦查技术也必须跟上其变化。同样，也应调整或发展保障措施，以跟上新的技术环境和新的程序权力的变化。

133. 打击网络环境中的犯罪的主要挑战之一是难以查明犯罪人并评估犯罪行为的程度和影响。另一个问题是电子数据变化无常，这些数据可能在几秒钟内就被更改、移走或删除。例如，控制数据的用户可以使用计算机系统来抹掉作为刑事调查对象的数据，从而销毁证据。速度和保密有时往往对调查的成功至关重要。

134. 本公约使搜查和扣押等传统程序措施适应新的技术环境。此外，还制定了新的措施，如加快保存数据，以确保传统的收集措施，如搜查和扣押，在瞬息万变的技术环境中仍然有效。由于新技术环境中的数据并非总是静态的，而可能是在通信过程中流动的，因此也对与电信有关的其他传统收集程序进行了调整，如实时收集流量数据和截取内容数据，以便能够收集通信过程中的电子数据。其中一些措施载于欧洲委员会关于与信息技术有关的刑事诉讼法问题的第 R(95)13 号建议。

135. 本节提到的所有规定旨在允许为具体的刑事调查或诉讼目的获取或收集数据。本公约的起草者讨论了公约是否应规定服务供应商有义务在某一固定时间范围内定期收集和保留流量数据，但由于缺乏共识，没有列入任何此类义务。

136. 该程序通常指所有类型的数据，包括三种特定类型的计算机数据(流量数据、内容数据和用户数据)，它们可以以两种形式存在(存储或在通信过程中)。其中一些术语的定义见第 1 条和第 18 条。程序对特定类型或形式的电子数据的适用性取决于数据的性质和形式以及程序的性质，具体见每一条。

137. 在使传统的程序法适应新的技术环境时，本节规定中出现了何种术语适当的问题。选择包括保持传统语言(“搜查”和“扣押”)，使用新的和更注重技术的计算机术语(“访问”和“复制”)，正如其他国际论坛关于该主题的文本(如八国集团高科技犯罪分组)所采用的那样，或者采用一种折中的混合语言(“搜查或类似的访问”，以及“扣押或类似的保全”)。由于有必要反映电子环境中概念的演变，并确定和保持其传统根源，因此采用了灵活的方法，允许各国使用 ″搜查和扣押 ″的旧概念或 ″获取和复制 ″的新概念。

138. 本节中的所有条款都提到“主管机构”以及为具体刑事调查或诉讼的目的应赋予它们的权力。在某些国家，只有法官才有权命令或授权收集或出示证据，而在其他国家，检察官或其他执法人员则被赋予相同或类似的权力。因此，“主管机构”是指国内法授权的司法、行政或其他执法机关，它们有权命令、授权或承担执行程序措施，以收集或出示与具体刑事调查或诉讼有关的证据。

篇目 1--通用条款

139. 本节一开始有两项一般性规定，适用于所有与程序法有关的条款。

程序性规定的范围(第 14 条)

140. 各缔约国有义务根据其国内法和法律框架，采取必要的立法和其他措施，确立本节所述的权力和程序，以便进行“具体的刑事调查或诉讼”。

141. 除两种例外情况外，各缔约国均应将根据本节确立的权力和程序适用于：(一)根据本公约第一节确立的刑事犯罪；(二)利用电脑系统所犯的其他刑事罪行；(三)以电子形式收集刑事犯罪的证据。因此，为了具体刑事调查或诉讼的目的，本节所指的权力和程序应适用于根据本公约确定的犯罪、通过计算机系统实施的其他刑事犯罪，并适用于以电子形式收集刑事犯罪证据。这确保了可以通过本节规定的权力和程序获得或收集任何刑事犯罪的电子证据。它确保获得或收集计算机数据的能力与非电子数据的传统权力和程序相同或平行。本公约明确规定，缔约国应在其法律中列明以数字或其他电子形式包含的信息可以在刑事诉讼中在法庭上作为证据，而不论起诉的刑事犯罪的性质如何。

142. 这一适用范围有两个例外。首先，第 21 条规定，截取内容数据的权力应仅限于由国内法律确定的一系列严重犯罪。许多国家认识到口头通信和电信的隐私性以及这一调查措施的侵扰性，将截取口头通信或电信的权力限制为一系列严重罪行。同样，本公约只要求缔约国就一系列严重罪行确立截取特定计算机通信内容数据的权力和程序，这些权力和程序将由国内法律确定。

143. 第二，缔约国可保留将第 20 条(实时收集流量数据)中的措施仅适用于保留中规定的犯罪或犯罪类别的权利，前提是此类犯罪或犯罪类别的范围不超过其适用第 21 条所述截取措施的犯罪范围。一些国家认为，就隐私和侵扰性而言，收集流量数据等同于收集内容数据。保留权将允许这些国家将实时收集流量数据的措施适用范围限制在与其适用实时截取内容数据的权力和程序相同的犯罪范围。然而，许多国家认为，就隐私权和侵扰程度而言，截取内容数据和收集流量数据并不等同，因为仅收集流量数据并不能收集或披露通信内容。由于实时收集流量数据对于追踪计算机通信的来源或目的地可能非常重要(从而有助于识别罪犯)，因此本公约请行使保留权的缔约国限制其保留，以便能够最广泛地运用所提供的权力和程序实时收集流量数据。

144. (b)项为以下国家规定了一项保留：这些国家由于在本公约通过时其国内法的现有限制，不能截取为封闭的用户群的利益而运行的，并且不使用公共通信网络，也不与其他计算机系统连接的计算机系统中的通信。术语“封闭的用户群”指的是，例如受与服务供应商的关联限制的用户群，诸如公司为其提供使用计算机网络使之有能力彼此间进行通信的公司雇员。“不与其他计算机系统连接”一词是指，在根据第 20 条或第 21 条发出命令时，正在传输通信的系统与另一计算机网络没有物理或逻辑连接。“不使用公共通信网络”一词不包括使用公共计算机网络(包括互联网)、公共电话网络或其他公共电信设施传输通信的系统，无论这种使用对用户是否明显。

条件和保障(第 15 条)

145. 公约该节规定的权力和程序的设立、执行和适用应遵守各缔约国国内法规定的条件和保障。虽然缔约国有义务在其国内法中引入某些程序法规定，但如何在其法律体系中确立和实施这些权力和程序，以及在具体案件中如何适用这些权力和程序，由各缔约国的国内法和程序决定。正如下文具体描述的，这些国内法律和程序应包括宪法、立法、司法或其

他方面可以规定的条件或保障。其方式应包括增加某些要件，作为平衡执法要求与保护人权和自由的条件或保障。由于本公约适用于众多有不同法律制度和文化的缔约国，不可能详细规定每项权力或程序的适用条件和保障。缔约国应确保这些条件和保障对人权和自由提供充分的保护。本公约缔约国必须遵守一些共同标准或最低保障。这些标准或最低保障包括缔约国根据适用的国际人权文书承担的义务而产生的标准或最低保障。这些文书包括 1950 年《欧洲保护人权与基本自由公约》及其关于欧洲缔约国的第 1、4、6、7 和 12 号附加议定书(《欧洲条约集》第 5[1]、9、46、114、117 和 177 号)。它还包括对世界其他地区的国家适用的其他人权文书(如 1969 年《美洲人权公约》和 1981 年《非洲人权和人民权利宪章》)，以及更普遍批准的 1966 年《公民及政治权利国际公约》。此外，大多数国家的法律也提供了类似的保护措施。

146. 本公约的另一项保障措施是，权力和程序应“纳入相称性原则”。各缔约国根据其国内法的相关原则执行相称性原则。对欧洲国家来说，这源自 1950 年欧洲委员会《保护人权和基本自由公约》的原则、其适用的判例以及国家立法和判例，即权力或程序应与犯罪的性质和情况相称。其他国家将适用其法律的相关原则，如对出示令超范围的限制以及搜查和扣押的合理性要求。另外，第 21 条明确限制了有关截取措施的义务是针对一系列由国内法确定的严重罪行，这是适用相称性原则的一个明显例子。

147. 在不限制可适用的条件和保障类型的情况下，本公约特别要求，鉴于权力或程序、司法或其他独立监督的性质，此类条件和保障应酌情包括适用权力或程序的正当理由以及对其范围或期限的限制。国家立法机构在适用具有约束力的国际义务和既定的国内原则时，必须确定哪些权力和程序带有足够的侵扰性，需要执行特定的条件和保障措施。如第 215 段所述，鉴于截取的侵扰性，缔约国应明确适用诸如截取方面的条件和保障措施。与此同时，例如，这些保障措施不必同样适用于保存。国内法应处理的其他保障措施包括免于自证其罪的权利，以及作为措施适用对象的个人或场所的法律特权和特殊性。

148. 关于第 3 段中讨论的事项，最重要的是考虑“公共利益”，特别是“健全的司法”利益。在符合公众利益的范围内，缔约国应考虑其他因素，例如有关权力或程序对因执法措施而招致的第三方(包括服务供应商)的“权利、责任和合法权益”的影响，以及是否可以采取适当的方法减轻这种影响。总而言之，初步考虑的是健全的司法和其他公共利益(例如公共安全和公共卫生以及其他利益，包括受害者的利益和对私人生活的尊重)。在符合公众利益的范围内，通常也会考虑以下问题：尽量减少对消费者服务的干扰、保护本章规定的披露或便利披露而免于责任，或保障所有权利益。

篇目 2--加快保存已存储的计算机数据

149. 第 16 条和第 17 条中的措施适用于已经由数据持有者(如服务供应商)收集和保存的存储数据。它们不适用于对未来流量数据的实时收集和保存，也不适用于对通信内容的实时访问。这些问题在篇目 5 中作了阐述。

150. 条款中描述的措施仅在计算机数据已经存在且目前正在存储的情况下才发挥作用。由于许多原因，与刑事调查有关的计算机数据可能不存在或不再被存储。例如，可能没有收

[1] 根据 1970 年 9 月 21 日生效的第 3 号议定书(《欧洲条约集》第 45 号)、1971 年 12 月 20 日生效的第 5 号议定书(《欧洲条约集》第 55 号)和 1990 年 1 月 1 日生效的第 8 号议定书(《欧洲条约集》第 118 号)的规定，对本公约内容作出了修正，并包括第 2 号议定书《欧洲条约集》第 44 号)的案文，根据第 5 条第 3 款，该议定书是本公约的一个有机组成部分。自 1998 年 11 月 1 日生效之日起，本议定书修订或增加的所有条款均由第 11 号议定书(《欧洲条约集》第 155 号)取代。自该日起，1994 年 10 月 1 日生效的第 9 号议定书(《欧洲条约集》第 140 号)被废止，第 10 号议定书(《欧洲条约集》第 146 号)失去了其目的。

集和保留准确的数据，或者没有维护收集的数据。数据保护法可能确定地要求销毁重要数据，此后人们才意识到这些数据对刑事诉讼的重要性。有时可能没有收集和保留数据的商业理由，例如客户为服务支付统一费用或服务属于免费的情况。第 16 条和第 17 条没有解决这些问题。

151.“数据保存”必须与“数据保留”区分开来。虽然它们在通用语言中有相似的含义，但在计算机使用方面却有不同的含义。保存数据意味着保护已经以存储形式存在的数据，使其不受任何可能导致其当前质量或条件改变或恶化的影响。保留数据意味着将目前正在生成的数据保留到将来。数据保留意味着在当前积累数据，并将其保持或拥有至未来某一时间。数据保留是存储数据的过程。而数据保存是保持存储的数据安全可靠的活动。

152.第 16 条和第 17 条只提到数据保存，而不是数据保留。这两条并不强制要求收集和保留服务供应商或其他实体在其活动过程中收集的所有数据甚至部分数据。保存措施适用于“通过计算机系统存储的”计算机数据，其前提是该数据已经存在、已被收集和存储。此外，正如第 14 条所述，本公约第 2 节要求建立的所有权力和程序都是“为了特定的刑事调查或诉讼的目的”，这就限制了这些措施对特定案件的调查的适用。此外，如果缔约方通过命令的方式实施保全措施，该命令是针对 ″个人拥有或控制的特定存储计算机数据″（第 2 款）。因此，这些条款只规定了在随后根据其他法律权力披露数据之前，在具体的刑事调查或诉讼中要求保存现有存储数据的权力。

153.确保数据保存的义务并不是要求缔约国限制提供或使用不定期收集和保留某些类型的数据(如流量或用户数据)的服务，作为其合法商业惯例的一部分。该义务也不要求缔约国为了这样做而实施新的技术能力，例如保存短暂的数据，这些数据可能在系统中存在很短的时间，以至于无法根据请求或命令进行合理的保存。

154.有些国家的法律要求，由特定类型的持有者持有的某些类型的数据，如个人数据，不得保留，如果保留数据不再有商业目的，则必须删除。在欧盟，一般原则由第 95/46/(E)(C)号指令实施，在电信部门的特定情况下，由第 97/66/(E)(C)号指令实施。这些指令规定，一旦不再需要存储数据时有义务立即删除数据。然而，成员国可以通过立法，规定在必要时为预防、调查或起诉刑事犯罪可以豁免。这些指令并不妨碍欧盟成员国根据其国内法设立权力和程序，为具体调查保存特定数据。

155.对大多数国家来说，数据保存在国内法中是一种全新的法律权力或程序。这是对付计算机和计算机相关犯罪，特别是通过互联网实施的犯罪的一个新的重要调查工具。首先，由于计算机数据的波动性，数据很容易受到操纵或更改。因此，有价值的犯罪证据很容易因粗心大意的处理和存储做法、旨在销毁证据的故意操纵或删除或例行删除不再需要保留的数据而丢失。保护其完整性的一种方法是由主管机构搜查或以类似方式访问、扣押或以类似方式保护数据。然而，如果数据的保管者是值得信赖的，如一个有信誉的企业，那么通过保存数据的命令，可以更快地保证数据的完整性。对合法企业而言，保全令对其正常活动和声誉的破坏程度，可能对其场所的搜查和扣押要小。第二，计算机和与计算机有关的犯罪在很大程度上是通过计算机系统传输通信而发生的。这些通信可能包含非法内容，如儿童色情制品、计算机病毒或其他导致干扰数据或计算机系统正常运行的指令，或实施其他犯罪的证据，如贩毒或欺诈。确定这些过去通信的来源或目的地有助于确定犯罪者的身份。为了追踪这些通信以确定其来源或目的地，需要有关这些过去通信的流量数据(见下文第 17 条对流量数据重要性的进一步解释)。第三，如果这些通信包含非法内容或犯罪活动证据，并且这些通信的副本由服务供应商保留，如电子邮件，那么为了确保关键证据不丢失，保存这些通信是非常重要的。获取这些过去通信的副本(例如，已经发送或接收的存储的电子邮件)可以揭示犯罪的证据。

156.加快保存计算机数据的权力就是为了解决这些问题。因此，缔约国需要引入一项权力，作为一项临时措施，命令保存特定的计算机数据，据此，数据将在必要的时间内得到保存，

最长不超过 90 天。缔约国可规定随后更新该命令。这并不意味着在保存时就向执法部门披露这些数据。要做到这一点，必须采取额外的披露措施或进行搜查。关于向执法部门披露保存的数据，见第 152 和 160 段。

157. 同样重要的是，在国家一级制定保存措施，以便使缔约国能够在国际一级相互协助，加快保存位于其境内的储存数据。这将有助确保关键数据不会在通常耗时的传统司法协助程序中丢失，而这些程序使被请求方能够实际获得有关数据，并向请求方披露数据。

加快保存已存储的计算机数据(第 16 条)

158. 第 16 条旨在确保国家主管机构能够命令或以类似方式迅速保存与特定刑事调查或诉讼有关的储存的特定计算机数据。

159. 保存数据意味着保护已经以存储形式存在的数据，使其不受任何可能导致其目前质量或条件改变或恶化的影响。它要求数据安全，不会被修改、变质或删除。保存并不一定意味着数据被“冻结”(即无法访问)，合法用户不能使用该数据或其副本。根据命令的确切规定，命令对象仍可访问数据。该条没有具体说明应该如何保存数据。由各缔约国决定恰当的保存方式，以及在某些适宜情况下，保存数据是否也应包括“冻结”。

160. 提及“命令或以类似方式获得”意在允许使用其他法律方法来实现保全，而不仅仅是通过司法或行政命令或指令(如出自警察或检察官的命令)。在一些国家，诉讼法中不存在保全令，只能通过搜查和扣押或出示令来保全和获取数据。使用“或以其他方式获得”这一短语的目的是具有灵活性，以允许这些国家通过使用这些手段执行本条。然而，建议各国考虑设立权力和程序，以便实际命令该命令的接收者保存数据，因为此人迅速采取行动可以在特定情况下更迅速地执行保存措施。

161. 以下命令或以类似方式要求迅速保存指定计算机数据的权力适用于任何类型的存储计算机数据。这可以包括命令中指定的任何类型的数据。例如，可以包括商业、健康、个人或其他记录。这些措施将由缔约国制定，以供“特别是在有理由相信计算机数据特别容易丢失或被修改的情况下”使用。这可能包括数据只需短时间保留的情况，例如有一项商业政策规定在一段时间后删除数据，或者当存储介质用于记录其他数据时，原有数据通常被删除。它还可以提及数据保管人的性质或数据存储的不安全方式。然而，如果保管人不值得信赖，以搜查和扣押的方式进行保全，会比下达保全命令(可能不服从)更为安全。第 1 款具体提到“流量数据”，是为了表明该款特别适用于这类数据，如果它们由服务供应商收集和保留，通常只保留很短的一段时间。提及"流量数据"也为第 16 条和第 17 条中的措施提供了联系。

162. 第 2 款规定，如果一缔约国通过一项命令要求保全，该保全命令仅与“某人保存其拥有或控制的特定存储的计算机数据”有关。因此，存储的数据可能实际上由该人拥有，或者可能存储在其他地方，但受该人控制。收到命令的人有义务“在必要的时间内(最长不超过 90 天)，保存和维护该计算机数据的完整性，以便主管机构能够寻求披露该数据”。一缔约国的国内法应对根据某项命令必须保存数据的最长期限作出规定，而该命令应对数据的确切保存期限作出具体规定。该期限应视需要而定，最长不超过 90 天，以便允许主管机构采取其他法律措施，如搜查和扣押，或类似的访问或保全，或发布出示令，以获得数据披露。一缔约国可规定该命令而后延长。在这方面，应提及第 29 条，该条涉及就迅速保全计算机系统存储的数据提出的互助请求。该条规定，为答复互助请求而实行的保全“其期限不得少于 60 天，以便请求方能提出搜查或类似的访问、扣押或类似的保全或披露数据的请求”。

163. 第 3 款规定，保管人或其他负责保存计算机数据的人在国内法规定的期限内对此类程序的运作保密。这要求缔约国采取保密措施，加快保存存储的数据，并对保密期设定时限。

这一措施满足了执法的需要，从而使被调查的嫌疑人不知晓调查的情况，也保护了个人的隐私权。对于执法机关来说，加快保存数据是初步调查的一部分，因此，在这一阶段，隐蔽性可能很重要。保存是在采取其他法律措施获取数据或披露数据之前的初步措施。为了不让其他人试图篡改或删除数据需要保密。对于命令收件人、数据主体或数据中可能提及或指明的其他人，对措施的时间长短需有明确的限制。保持数据安全和安保以及对已采取保存措施之事进行保密的双重义务，有助于保护数据主体或其他可能在该数据中被提及或识别的人的隐私。

164. 除上述限制外，第 16 条所述权力和程序也受第 14 条和第 15 条规定的条件和保障的制约。

加快保存和部分披露流量数据(第 17 条)

165. 该条对第 16 条下保存流量数据的具体义务作了规定，并规定迅速披露某些流量数据，以查明参与了特定通信传输的其他服务供应商。“流量数据”的定义见第 1 条。

166. 获得与以往通信相关联的存储的流量数据对于识别过去通信的源头或目的地可能至关重要，它对于识别以下人员也至为关键，例如，散发儿童色情制品者、作为欺诈计划的一部分散发欺诈性虚假介绍者、散发计算机病毒者、非法访问计算机系统未遂或得逞者、或将通信传输到计算机系统进而干扰系统中的数据或系统正常运行者。然而，由于旨在保护隐私的法律可能会禁止长期存储此类数据，或市场力量可能会阻止长期存储此类数据，所以通常只能短期存储此类数据。因此，采取保存措施以确保这类数据的完整性十分重要(见上文关于保存的讨论)。

167. 在通信传输中，通常可能涉及多个服务供应商。每个服务供应商可以拥有与特定通信的传输相关的一些流量数据，这些流量数据或者是由该服务供应商在通信经过其系统时生成并保留的，或者是由其他服务供应商提供的。有时，出于商业、安全或技术目的，在通信传输中涉及的服务供应商之间共享流量数据或至少某些类型的流量数据。在这种情况下，服务供应商中的任何一个都可能拥有确定通信源头或目的地所需的关键流量数据。然而，通常没有一个服务供应商拥有足够的关键流量数据以确定通信的实际源头或目的地。每个人都有拼图的一部分，需要对每一部分进行检查，以确定源头或目的地。

168. 第 17 条确保在一个或多个服务供应商参与通信传输的情况下，可以在所有服务供应商之间实现流量数据的快速保存。该条没有具体说明实现这一目标的手段，而是让国内法来确定符合其法律和经济制度的手段。实现快速保全的一种方法是由主管机构迅速向每个服务供应商发出单独的保全令。然而，备齐一系列单独的命令可能会非常耗时。一种更可取的替代办法是出具一份单一的命令，其范围适用于随后被确定为参与特定通信传输的所有服务供应商。这份全面的命令可按顺序提供给每个查明的服务供应商。其他可能的替代方案可以涉及服务供应商的参与。例如，要求收到命令的服务供应商转告通信链中的下一个服务供应商关于保全令及其条件的事宜。根据国内法，这一通知可能具有允许另一服务供应商自愿保存相关流量数据(尽管有义务将其删除)或强制保存相关流量数据的效果。下一个服务供应商可以此类推通知通信链中的下一个服务供应商。

169. 由于在向服务供应商送达保全令时，流量数据不会被披露给执法机关(而是在采取其他法律措施后才获得或披露)，因此这些机关不知道服务供应商是否拥有所有重要的流量数据，或者是否有其他服务供应商参与了通信传输链。因此，本条要求收到保全令或类似措施的服务供应商迅速向主管机构或其他指定人员披露足够的流量数据，以便主管机构能够识别任何其他服务供应商以及通信传输的路径。主管机构应明确规定要求披露的流量数据的类型。收到这一信息将使主管机构能够决定是否对其他服务供应商采取保全措施。通过这种方式，调查部门可以回溯追踪到通信的源头，或向前追踪到其目的地，并查明正在调

查的具体罪行的肇事者。本条中的措施也受第 14 条和第 15 条中规定的限制、条件和保障的制约。

篇目 3--出示令

出示令(第 18 条)

170. 本条第 1 款要求各缔约国让其主管机构能够迫使其境内的人提供特定的存储计算机数据，或迫使在该缔约国境内提供服务的服务供应商提交用户信息。所指的数据是存储的或现有的数据，不包括尚未出现的数据，例如与未来通信相关的流量数据或内容数据。与其要求各国对第三方采取系统的强制性措施，如搜查和扣押数据，不如要求各国根据其国内法拥有另一种调查权，提供一种侵扰性较小的手段来获取与刑事调查有关的信息。

171. “出示令”提供了一种灵活的措施，执法部门可以在许多情况下适用，特别是代替更具侵扰性或更繁琐的措施。这种程序性机制的实施也将有利于第三方数据保管人，如互联网服务供应商，他们往往愿意在自愿的基础上通过提供其控制下的数据来协助执法部门，但他们更愿意基于适当的法律依据提供这种协助，从而免除其任何合同责任或非合同责任。

172. 出示令所指的是由个人或服务供应商拥有或控制的计算机数据或用户信息。该措施仅适用于个人或服务供应商所持有的此类数据或信息的范围。例如，一些服务供应商没有保存其服务用户的记录。

173. 根据第 1 款(a)项，缔约国应确保其主管执法机构有权命令其境内的人提交存储在该人拥有或控制的计算机系统或数据存储介质中的特定计算机数据。“所拥有或控制的”一词指的是在命令方领土上实际拥有的相关数据，在这种情况下，要产生的数据不属于此人的实际占有，但此人仍然可以在命令方领土上自由地控制数据的产生(例如，依适用的特权，接获需出示其通过远程在线存储服务存储在其账户中的信息的人，必须提供此类信息)。同时，仅仅是访问远程存储数据的技术能力(例如，用户通过网络链接访问不在其合法控制范围内的远程存储数据的能力)并不一定构成本条款意义上的“控制”。在一些国家，法律称之为“拥有”的概念涵盖有形和推定拥有，其范围足以满足这一“所拥有或控制的”要求。

根据第 1 款(b)项，缔约国还应规定有权命令在其境内提供服务的服务供应商“提交该服务供应商拥有或控制的用户信息”。如第 1 款(a)项所述，术语“所拥有或控制的”是指服务供应商实际拥有的用户信息，以及在服务供应商控制下远程存储的用户信息(例如在另一家公司提供的远程数据存储设施中)。术语“与此类服务有关的”是指有权获得与订购方领土上提供的服务相关的用户信息。

174. 根据各缔约国的国内法，本条第 2 款所指的条件和保障措施可以排除特权数据或信息。缔约国不妨就提交特定类别人员或服务供应商持有的特定类型计算机数据或用户信息规定不同的条款、不同的主管机构和不同的保障措施。例如，对于某些类型的数据，如可公开获得的用户信息，缔约国可能允许执法人员下达此类命令，而在其他情况下可能需要法院令。另一方面，在某些情况下，缔约国可能要求，或由人权保障措施授权，要求只有司法机构签发出示令才能获得某些类型的数据。缔约国不妨将出于执法目的披露此类数据的情况限制在司法机关已发出披露此类信息的出示令的情况。相称性原则还为措施的适用提供了一定的灵活性，例如在许多国家，排除在轻微的案件中适用。

175. 缔约国的另一个考虑是是否可能纳入保密措施。该条款没有具体提到保密事宜，以便与非电子领域保持平行，在非电子领域，出示令一般不需要保密。然而，在电子领域，特

别是在线领域，有时可以将出示令作为调查的初步措施，然后再采取进一步措施，如搜查和扣押或实时截取其他数据。保密有可能是调查成功的关键。

176. 关于出示方式，缔约国可订立义务，规定必须按照出示令中规定的方式提供指定的计算机数据或用户信息。这可以包括提及必须作出披露的时间段，或形式，如以“纯文本”、在线方式或纸质打印件或软盘的方式提供数据或信息。

177. “用户信息”的定义见第 3 款。原则上，它指的是服务供应商的管理部门持有的与其服务用户有关的任何信息。用户信息可以用计算机数据形式或任何其他形式(例如纸质记录形式)呈现。由于用户信息包括除计算机数据之外的其他形式的数据，因此本条中加入了一个特别条款来处理这类信息。“用户”旨在包括服务供应商的广泛客户，从持有付费订阅的人，到按使用量付费的人，以及接受免费服务的人。它还包括有权使用用户账户的人的信息。

178. 在刑事调查过程中，可能主要在两种特定情况下需要用户信息。首先，需要用户信息来识别用户已经使用或正在使用哪些服务和相关的技术措施，诸如所使用的电话服务的类型(例如，移动)、所使用的其他相关服务的类型(例如，呼叫转移、语音邮件等)、电话号码或其他技术地址(例如，电子邮件地址)。第二，当已知技术地址时，需要用户信息以帮助确定有关人员的身份。其他用户信息，例如有关用户的账单和支付记录的商业信息，也可能与刑事调查有关，特别是调查中的犯罪涉及计算机欺诈或其他经济犯罪的情况。

179. 因此，用户信息包括关于服务的使用和该服务的用户的各种类型的信息。就服务的使用而言，该术语是指除流量或内容数据之外的任何信息，通过该信息可以确定所使用的通信服务的类型、与其相关的技术规定以及该人订阅该服务的时间段。“技术规定”一词包括为使用户能够享受所提供的通信服务采取的所有措施。这些规定包括保留技术号码或地址(电话号码、网站地址或域名、电子邮件地址等)，以及提供和登记用户使用的通信设备，如电话设备、呼叫中心或局域网。

180. 用户信息不限于与使用通信服务直接相关的信息。它还指除流量数据或内容数据之外的任何信息，通过这些信息可以确定用户的身份、邮政或地理地址、电话和其他接入号码，以及基于用户与服务供应商之间的服务协议或安排可获得的账单和付款信息。它还指除流量数据或内容数据以外的任何其他信息，这些信息涉及安装通信设备的地点或位置，可根据服务协议或安排获得。后一种信息可能只在设备不可移动的情况下才有实际意义，但了解设备的可移动性或所谓的位置(根据服务协议或安排提供的信息)可能对调查有帮助。

181. 然而，本条不应被理解为规定服务供应商有义务保存其用户的记录，也不会要求服务供应商确保此类信息的正确性。因此，服务供应商没有义务登记所谓的移动电话服务预付卡用户的身份信息。它也没有义务核实用户的身份或抵制其服务的用户使用假名。

182. 由于本节中的权力和程序是为了特定的刑事调查或诉讼(第 14 条)，出示令将用于通常涉及特定用户的个别案件。例如，按照提供出示令中提到的特定姓名，可以要求提供特定的相关电话号码或电子邮件地址。根据特定的电话号码或电子邮件地址，可以要求提供有关用户的姓名和地址。该条款没有授权缔约国发布法律命令，例如为了数据挖掘的目的不加区分地披露服务供应商手中用户群的用户信息。

183. 对于“服务协议或安排”的提法应作广义的解释，包括客户使用供应商的服务所依据的任何一种关系。

篇目 4—搜查和扣押存储的计算机数据

搜查和扣押储存的计算机数据(第 19 条)

184. 本条旨在使有关为获取特定刑事调查或诉讼的证据而搜查和扣押所存储的计算机数据的国内法律现代化和协调一致。任何国内刑事诉讼法都包括搜查和扣押有形物品的权力。然而，在一些司法管辖区，存储的计算机数据本身不会被视为有形物体，因此不能像有形物体那样以平行的方式为刑事调查和诉讼提供保障，而只能通过保全其存储的数据介质。本公约第 19 条的目的是确立一种与存储数据有关的同等权力。

185. 在有关文件或记录的传统搜查环境中，搜查涉及收集过去以有形方式记录或登记的证据，如纸上的墨水。调查人员搜索或检查这种记录的数据，并扣押或实际带走有形记录。数据的收集是在搜查期间进行的，而且是针对当时存在的数据。获得进行搜查的法律授权的前提条件是，根据国内法和人权保障措施的规定，有理由相信这些数据存在某一特定地点并将提供特定刑事犯罪的证据。

186. 关于在新的技术环境中搜查证据，特别是计算机数据，传统搜查的许多特征仍然存在。例如，数据的收集是在搜查期间进行的，而且是针对当时存在的数据。获得法律授权进行搜查的前提条件仍然相同。无论数据是以有形方式还是以电子形式存在，获得法律授权进行搜查所需的确信度没有任何区别。同样，认定和搜查都是针对已经存在的数据，并且可以提供特定犯罪的证据。

187. 然而，在搜查计算机数据方面，有必要制定额外的程序性规定，以确保计算机数据的获取方式与搜查和扣押有形数据载体的方式同样有效。其中有几个原因：第一，数据是以无形的方式存在的，比如说以电磁形式存在。第二，虽然数据可以通过使用计算机设备来读取，但不能像纸质记录那样被扣押和带走。储存无形数据的有形媒介(如计算机硬盘或软盘)必须被扣押和带走，或者必须以有形方式(如计算机打印输出)或无形方式在有形媒介(如软盘)上制作数据的副本，然后才能扣押和带走含有该副本的有形媒介。在后两种情况下，如果制作了这样的数据副本，数据的副本就会留在计算机系统或存储设备中。国内法应规定制作这种副本的权力。第三，由于计算机系统的连接性，数据可能没有存储在被搜索的特定计算机中，但这些数据可能随时可以被该系统访问。它可能存储在直接与计算机相连的相关数据存储设备中，或通过通信系统(如互联网)间接与计算机相连。有可能需要也可能不需要制定新的法律，以允许将搜索范围扩大到数据实际存储地(或将数据从该地点检索到被搜索的计算机)，或在两个地点以更协调和迅速的方式使用传统的搜查权力。

188. 第 1 款要求缔约国授权执法机关访问和搜索计算机数据，这些数据要么包含在计算机系统或其一部分(如连接的数据存储设备)，要么包含在独立的数据存储介质(如(光盘或软盘)上。由于第 1 条中“计算机系统”的定义是指“任何设备或一组相互连接或相关的设备”，第 1 款涉及对计算机系统及其相关组成部分的搜索，这些组成部分可被视为共同构成一个不同的计算机系统(例如，一台个人电脑与一台打印机和相关存储设备一起，或一个局域网)。有时，通过与其他不同的计算机系统建立连接，可以合法地通过被搜索的计算机系统访问物理上存储在另一个系统或存储设备中的数据。这种情况涉及通过境内的同一电信网络(如广域网或互联网)与其他计算机系统的联系，在第 2 款中述及。

189. 虽然对“可储存计算机数据的计算机数据存储介质”(第 1 款(b)项)的搜查和扣押可以通过使用传统的搜查权来进行，但执行计算机搜查往往需要同时搜查计算机系统和紧邻计算机系统的任何相关计算机数据存储介质(如软盘)。由于这种关系，第 1 款提供了一个全面的法律授权，以涵盖这两种情况。

190. 第 19 条适用于存储的计算机数据。在这方面，出现的问题是，在收件人将电子邮件下载到他或她的计算机系统之前，在互联网服务供应商邮箱中等待的未打开的电子邮件是否必须被视为存储的计算机数据或传输中的数据。根据一些缔约国的法律，该电子邮件信息是通信的一部分，因此其内容只能通过适用截取权获得，而其他法律制度则将该信息视为

第 19 条所适用的存储数据。因此，缔约国应审查其关于这一问题的法律，以确定在其国内法律体系内哪一种合适。

191. 提到了“搜查或类似的访问”一词。使用传统的“搜查”一词传达了国家行使强制力的概念，并表明本条中提到的权力类似于传统的搜查。“搜索”指的是寻找、阅读、检查或审查数据。它包括搜索数据和搜检(检查)数据的概念。另一方面，“访问”一词的意思是中性的，但它更准确地反映了计算机术语。这两个术语的使用都是为了将传统概念与现代术语结合起来。

192. 提到“在其境内”是为了提醒人们，这一规定同本节中的所有条款一样，只涉及要求在国家一级采取的措施。

193. 第 2 款允许调查部门在有理由相信所需数据储存在另一个计算机系统或其一部分的情况下，将其搜查或类似的访问扩大到该计算机系统。然而，另一个计算机系统或其中的一部分也必须“在其境内”。

194. 本公约并没有规定如何允许或进行扩大搜查。这将留给国内法处理。一些可能的条件的例子是：授权司法或其他机关批准对特定计算机系统进行计算机搜查，如果有理由相信(已达到国家法律和人权保障要求的程度)所连接的计算机系统可能包含正在寻找的特定数据，则授权其扩大搜查范围或以类似方式访问连接的系统；授权调查部门在有类似理由相信所寻找的特定数据存储在另一计算机系统中的情况下，将对特定计算机系统的授权搜查或类似的访问扩展到所连接的计算机系统；或者以协调和迅速的方式在两个地点执行搜查或类似的访问权限。在所有情况下，要搜索的数据必须可以从最初的计算机系统合法访问或获得。

195. 本条不涉及“跨境搜查和扣押”，即各国可以在其他国家领土上搜查和扣押数据，而不必通过通常的司法协助渠道。这个问题将在下面关于国际合作一章中讨论。

196. 第 3 款涉及授权主管机构扣押或以类似方式保护根据第 1 款或第 2 款被搜查或以类似方式访问的计算机数据的问题。这包括扣押计算机硬件和计算机数据存储介质的权力。在某些情况下，例如，当数据存储在唯一的操作系统中而无法复制时，不可避免地必须将数据载体作为一个整体予以扣押。当需要对数据载体进行检查，以便从其中检索出被覆盖但仍在数据载体上留下痕迹的旧数据时，这也可能是必要的。

197. 在本公约中，“扣押”是指带走记录数据或信息的物理媒介，或制作和保留此类数据或信息的副本。“扣押”包括使用或扣押旨在访问被扣押数据所需的程序。除了使用传统“扣押”一词外，还包括“以类似方式保护”一词，以反映在计算机环境中删除无形数据、使之无法访问或以其他方式接管其控制权的其他手段。由于这些措施涉及存储的无形数据，主管机构需要采取额外措施来确保数据的安全；即“保持数据的完整性”，或保持数据的“监管链”，这意味着被复制或删除的数据应保留在扣押时发现的国家，并在刑事诉讼期间保持不变。该术语指的是对数据的控制或取走。

198. 造成无法访问的数据可以包括加密数据或以其他方式在技术上拒绝任何人访问该数据。这一措施可以有效地适用于涉及危险或危害社会的情况，如病毒程序或关于如何制造病毒或炸弹的说明，或非法的数据或数据内容，如儿童色情制品。“删除”一词意在表明：虽然数据被删除或变得无法访问，但它并没有被销毁，而是继续存在。嫌疑人暂时被剥夺了数据，但在刑事调查或诉讼的结果出来后，可以将其归还。

199. 因此，扣押或以类似方式保护数据有两个功能：1)收集证据，如复制数据，或 2)没收数据，如复制数据并随后使数据的原始版本无法访问或予以删除。扣押并不意味着最终删除扣押的数据。

200.第 4 款引入了一项强制性措施，以方便对计算机数据的搜查和扣押。该款解决了一个实际问题，即鉴于可处理和存储的数据量、安全措施的部署以及计算机操作的性质，可能难以访问和识别作为证据的数据。该款认识到，可能需要就如何最好地进行搜查的技术方式咨询对计算机系统有特殊了解的系统管理员。因此，该款允许执法部门迫使系统管理员在合理的情况下协助进行搜查和扣押。

201.这项权力不只是对调查部门有利。如果缺乏此种合作，调查部门可能会在进行搜查时，在被搜查的场所长时间停留，并阻止对计算机系统的访问。这可能会给在此期间被拒绝访问数据的合法企业或客户和用户带来经济负担。命令知情者合作的方法将有助于使搜查工作更有效率和更具成本效益，对执法人员和受影响的无辜个人都是如此。从法律上强制系统管理员提供协助也可以免除管理员不得披露数据的任何合同义务或其他义务。

202.可命令要求提供的材料是那些能够进行搜查和扣押，或类似可以访问或保全的必要信息。然而，这些信息的提供仅限于“合理的”范围。在某些情况下，合理的规定可能包括向调查部门披露密码或其他安全措施。然而，在其他情况下，这可能是不合理的；例如，密码或其他安全措施的泄露会不合理地威胁到其他用户的隐私或未经授权可搜索的其他数据。在这种情况下，提供“必要的信息”意味着以能理解和可读的形式披露主管机构正在寻找的实际数据。

203.根据本条第 5 款，这些措施须符合根据本公约第 15 条制定的国内法规定的条件和保障。这些条件可包括与聘请证人和专家及其经济补偿有关的规定。

204.起草者在第 5 款的框架内进一步讨论了是否应通知有关各方启用了搜查程序。在网上世界，数据被搜查和扣押(复制)可能不如在网下世界进行的扣押明显，因为被扣押的物品会实际消失。一些缔约国的法律没有规定在传统的搜索情况下的通知义务。如果本公约要求对计算机搜索进行通知，将在这些缔约国的法律中造成不一致。另一方面，一些缔约国可能认为通知是该措施的一个基本特征，以便保持计算机搜索存储数据(一般不打算成为一种秘密措施)与截取流动数据(这是一种秘密措施，见第 20 条和第 21 条)之间的区别。因此，通知问题由国内法决定。如果缔约国考虑强制通知有关人员的制度，应铭记这种通知可能会妨碍调查。如果存在这种风险，应考虑推迟通知的时间。

篇目 5--实时收集计算机数据

205.第 20 条和第 21 条对实时收集流量数据和实时截取与计算机系统传输的特定通信相关的内容数据做出了规定。这些条款涉及主管机构对此类数据的实时收集和实时截取，以及服务供应商对此类数据的收集或截取。还涉及到保密义务。

206.电信截取通常指的是传统的电信网络。这些网络可以包括电线或光缆的电缆基础设施，以及与无线网络的相互连接，包括移动电话系统和微波传输系统。如今，特殊的卫星网络系统也促进了移动通信。计算机网络也可以由独立的固定电缆基础设施组成，但更经常地通过电信基础设施的连接作为虚拟网络运行，从而允许创建计算机网络或全球性质的网络链接。随着电信和信息技术的融合，电信和计算机通信之间的区别及其基础设施之间的区别正在变得模糊。因此，第 1 条中“计算机系统”的定义并不限制设备或设备组相互连接的方式。因此，第 20 条和第 21 条适用于通过计算机系统传输的特定通信，这可能包括在另一个计算机系统接收之前通过电信网络传输的通信。

207.第 20 条和第 21 条没有区分公共或私人拥有的电信或计算机系统，也没有区分向公众或封闭的用户群体或私人提供的系统和通信服务的使用。第 1 条中的“服务供应商”的定义是指向其服务的使用者提供通过计算机系统进行通信的能力的公共和私人实体。

208. 本篇规范了当前产生的通信中所包含的证据的收集，这些证据是在通信发生时(即“实时”)收集的。数据在形式上是无形的(例如，以语音或电子脉冲传输的形式)。数据的流动不会因收集而受到严重干扰，而且通信会到达预期的接收者。不对数据进行物理扣押，而是对通信的数据进行录制(即拷贝)。这种证据的收集是在一定的时间段内进行的。对未来事件(即数据的未来传输)寻求允许收集的法律授权。

209. 可以收集的数据类型有两种：流量数据和内容数据。第 1 条(d)项中定义的“流量数据”是指与通过计算机系统进行的通信有关的任何计算机数据，这些数据由计算机系统生成，构成通信链的一部分，表明通信的始发地、目的地、路径、时间、日期、大小和持续时间或服务类型。本公约对“内容数据”没有给出定义，所指的是通信中的通信内容；即通信的内含或主旨，或者通信所传达的讯息或信息(流量数据除外)。

210. 在许多国家，就授权采取这种调查措施所需的法律先决条件和可对之采取这种措施的犯罪而言，实时截取内容数据和实时收集流量数据是有区别的。许多国家虽然认识到这两类数据可能都有相关的隐私利益，但认为由于通信内容或信息的性质，内容数据的隐私利益更大。相对于流量数据而言，对内容数据的实时收集可能施加更大的限制。为了有助于这些国家认识到这种区别，本公约虽然在操作上承认数据是在两种情况下收集或记录的，但在条款篇目中以规范方式将流量数据的收集称为“实时收集”，将内容数据的收集称为“实时截取”。

211. 一些国家，现行立法没有对收集流量数据和截取内容数据加以区分，要么是因为法律中没有对隐私利益的差异加以区分，要么是因为这两种措施的技术收集手段非常相似。因此，授权采取措施所需的法律先决条件和可对其采取措施的罪行是相同的。本公约第 20 条和第 21 条的实际文本中普遍使用“收集或记录”一词，也承认了这种情况。

212. 关于实时截取内容数据，法律往往规定，该措施仅适用于调查严重犯罪行为或严重犯罪类别。这些罪行在国内法中被确定为严重罪行，往往是通过在适用的罪行清单中列出，或通过提及适用于该罪行的某一最高监禁刑罚而被列入这一类别。因此，关于内容数据的截取，第 21 条明确规定，缔约国只需“针对国内法确定的一系列严重罪行”制定该措施。

213. 另一方面，关于收集流量数据的第 20 条则不受限制，原则上适用于本公约所涵盖的任何刑事犯罪。然而，第 14 条第 3 款规定，缔约国可保留仅对保留中指明的犯罪或犯罪类别适用该措施的权利，但犯罪或犯罪类别的范围不得比其适用截取内容数据措施的罪行范围更有限。然而，如果作出这种保留，该缔约国应考虑对这种保留加以限制，以便能够最广泛地适用收集流量数据的措施。

214. 对一些国家来说，本公约中规定的罪行通常不会被认为严重到允许截取内容数据，或者在某些情况下甚至允许收集流量数据。然而，这种技术对于调查本公约确立的一些罪行，如涉及非法访问计算机系统、传播病毒和儿童色情制品的罪行，往往至关重要。例如，在某些情况下，如果不能实时收集流量数据，就无法确定入侵或传播的来源。在某些情况下，如果不能实时截取内容数据，就无法发现通信的性质。这些犯罪由于其性质或传播手段，涉及到计算机技术的使用。因此，应该允许使用技术手段来调查这些犯罪行为。然而，由于围绕截取内容数据问题的敏感性，本公约将这一措施的范围留给国内法律来决定。由于一些国家在法律上将流量数据的收集与内容数据的截取相提并论，因此允许有保留的可能性，以限制前一项措施的适用性，但其程度不能超过缔约国对内容数据实时截取措施的限制。尽管如此，缔约国应考虑将这两项措施适用于本公约第二章第 1 节所确立的犯罪，以便为调查这些计算机犯罪和计算机相关犯罪提供有效手段。

215. 有关实时截取内容数据和实时收集流量数据的权力和程序的条件和保障措施受第 14 条和第 15 条的制约。由于截取内容数据是一种对私人生活极具侵扰性的措施，因此需要严格的保障措施，以确保在司法利益与个人基本权利之间取得适当的平衡。在截取方面，本公

约本身没有规定具体的保障措施，只是将截取内容数据的授权限制在对国内法律规定的严重刑事犯罪的调查上。然而，在这一领域适用于国内法律的重要条件和保障措施有：司法或其他独立监督；要截取的通信或人员的具体情况；必要性、辅助性和相称性(如证明采取该措施合理的法律前提；其他侵扰性较小的措施效果不佳)；对截取时间的限制；获得补救的权利，其中许多保障措施反映了《欧洲人权公约》及其随后的判例法(见 Klass 案[1]、Kruslin 案[2]、Huvig 案[3]、Malone 案[4]、Halford 案[5]、Lambert[6]案的判决)。其中一些保障措施也适用于流量数据的实时收集。

实时收集流量数据(第 20 条)

216. 通常，以往的流量数据可能不再有用，或者可能不相关，因为侵入者已经更改了通信路径。因此，实时收集流量数据是一个重要的调查手段。第 20 条涉及为特定刑事调查或诉讼目的实时收集和记录流量数据的问题。

217. 传统上，收集与电信有关的流量数据(例如，电话通话)一直是一种有用的调查工具，用于确定各种类型的非法通信(如犯罪威胁和骚扰、犯罪阴谋、欺诈性虚假陈述)以及提供过去或未来犯罪证据的通信(如贩毒、谋杀、经济犯罪等)源头或目的地(例如，电话号码)和相关数据(如时间、日期和持续时间)。

218. 计算机通信可以构成或提供相同类型犯罪的证据。然而，鉴于计算机技术能够传输大量数据，包括文字、视觉图像和声音，它也有更大的潜力实施涉及传播非法内容(例如儿童色情制品)的犯罪活动。同样，由于计算机可以存储大量数据，通常是私人性质的数据，如果这些数据的完整性受到干扰，无论是对经济、社会还是个人都可能构成潜在的巨大危害。此外，由于计算机技术科学是建立在数据处理的基础上的，无论是作为最终产品还是作为其操作功能的一部分(例如，计算机程序的执行)，对该数据的任何干扰都会对计算机系统的正常运行产生灾难性的影响。当非法传播儿童色情制品，非法访问计算机系统或干扰计算机系统正常运行或数据完整性的行为发生时，特别是通过互联网等远距离传播时，追踪从受害者到犯罪者的通信路线是必要和关键的。因此，收集计算机通信数据的能力与收集纯粹的传统电信数据一样重要，甚至更重要。这种调查技术可以将嫌疑人通信的时间、日期、来源和目的地与侵入受害者系统的时间联系起来，识别其他受害者或显示与同伙的联系。

219. 根据该条，相关的流量数据必须与缔约国境内的特定通信有关联。指定的“通信”是复数，因为要想确定来源者或目的地，可能需要收集涉及若干通信的流量数据(例如，在一个家庭中，几个不同的人使用同一台电信设备，可能需要将若干通信与个人使用计算机系统的机会联系起来)。然而，必须具体说明可以收集或记录流量数据的通信。因此，本公约并不要求或授权对大批流量数据进行不加区分的普遍监视和收集。本公约不允许出现“远海捕捞”情况，即企望发现其他犯罪活动，而不是调查特定的犯罪事件。授权收集的司法令或其他令必须指明收集流量数据所涉及的通信。

[1] 欧洲人权法院对 Klass 等人诉德国案的判决，(A)28,1978 年 06 月 09 日。

[2] 欧洲人权法院对 Kruslin 诉法国案的判决，176-(A)，1990 年 4 月 24 日。

[3] 欧洲人权法院对 Huvig 诉法国案的判决，176-(B)，1990 年 4 月 24 日。

[4] 欧洲人权法院对 Malone 诉联合王国案的判决，(A)82,1984 年 2 月 8 日。

[5] 欧洲人权法院对 Halford 诉联合王国案的判决，《1997-报告第三卷》，1997 年 6 月 25 日。

[6] 欧洲人权法院对 Lambert 诉法国案的判决，《1998 年报告》第五卷，1997 年 6 月 25 日。

220. 在不违反第 2 款的情况下，缔约国有义务根据第 1 款(a)确保其主管机构有能力通过技术手段收集或记录流量数据。该条没有从技术上规定如何进行收集，也没有界定技术方面的义务。

221. 此外，根据第 1 款(b)项，缔约国有义务确保其主管机构有权迫使服务供应商收集或记录流量数据，或在收集或记录此类数据方面与主管机构合作并给予协助。关于服务供应商的这种义务仅适用于在服务供应商现有的技术能力范围内的收集或记录、合作和协助。该条并未规定服务供应商有义务确保其具备从事收集、录制、合作或协助的技术能力。该条并未要求服务供应商购买或开发新的设备、聘请专家支持或参与昂贵的系统重新配置。然而，如果其系统和人员有现有的技术能力来提供这种收集、记录、合作或协助，该条则要求它们采取必要的措施来利用这种能力。例如，系统可能以这种方式配置，或者服务供应商可能已经拥有计算机程序，允许采取这种措施，但在服务供应商的正常运作过程中通常不执行或使用。该条要求服务供应商依照法律要求使用或开启这些功能。

222. 由于这是一项在国家一级实施的措施，这些措施适用于在缔约国境内收集或记录特定的来文。因此，实际上，只要服务供应商在该领土上有一些能够采取这些措施的实际基础设施或设备，这些义务就普遍适用，尽管这不一定是其主要业务或总部所在地。就本公约而言，如果通信方之一(人或计算机)位于某一缔约国境内，或者通信所经过的计算机或电信设备位于该缔约国境内，则可理解为通信位于该缔约国境内。

223. 一般来说，第 1 款(a)项和(b)项中收集流量数据的两种可能性并不是替代办法。除第 2 款规定外，缔约国必须确保这两项措施都能执行。这是必要的，因为如果一个服务供应商没有技术能力承担收集或记录流量数据(第 1 款(b)项)，那么一个缔约国必须有可能让其执法部门自己承担这项任务(第 1 款(a)项)。同样，如果主管机构没有能力本身收集或记录流量数据，那么第 1 款(b)项(2)目规定的合作和协助主管机构收集或记录流量数据的义务就毫无意义。此外，在一些可能不涉及服务供应商的局域网的情况下，收集或记录的唯一方法是由调查部门自己进行。第 1 款(a)和(b)项中的两项措施不一定每次都要使用，但该条要求两种方法都能使用。

224. 然而，这种双重义务给某些国家带来了困难，因为在这些国家，执法部门只能通过服务供应商的协助来截取电信系统中的数据，或者至少在服务提供商不知情的情况下偷偷摸摸地截取数据。为此，第 2 款顾及到了这种情况。如果一缔约国由于“其国内法律制度的既定原则”不能采取第 1 款(a)项所述的措施，它可以采取不同的办法，例如只强迫服务供应商提供必要的技术设施，以确保执法部门实时收集流量数据。在这种情况下，关于领土、通信的特殊性和技术手段的使用的所有其他限制仍然适用。

225. 与实时截取内容数据一样，实时收集流量数据只有在被调查者不知情的情况下才有效。截取是秘密的，必须以通信方不会察觉到的方式进行。因此，对截取行动知情的服务供应商及其雇员，必须承担保密义务，以便有效地实施该程序。

226. 第 3 款规定，缔约国有义务采取必要的立法或其他措施，责成服务供应商对本条规定的有关实时收集流量数据的任何措施之事及执行情况予以保密。这项规定不仅确保了调查的保密性，而且还免除了服务供应商通知用户正在收集他们的数据的任何合同义务或其他法律义务。第 3 款可以通过在法律中设定明确的义务来实现。另一方面，一缔约国有可能根据其他国内法律规定确保该措施的保密性，例如有权以妨碍司法为由起诉那些通过将该措施告诉罪犯而帮助他们的人。虽然具体的保密要求(在违反情况下进行有效制裁)是一种可取的程序，但使用妨碍司法罪可以作为防止不当披露的替代手段，因此也足以执行本款。如果规定了明确的保密义务，这些义务应当受第 14 条和第 15 条规定的条件和保障措施的约束。鉴于调查措施的秘密性质，这些保障措施或条件应对义务的持续时间规定合理的期限。

227. 如上所述，一般认为收集流量数据的隐私利益比截取内容数据的隐私利益要小。关于通信时间、持续长短和规模的流量数据几乎没有揭示某人(无论男女)想法的个人信息。然而，关于通信来源或目的地的数据(如访问的网站)可能存在更大的隐私问题。在某些情况下，收集这种数据可以汇总出一个人的兴趣、伙伴和社会背景的概况。因此，缔约国在根据第 14 条和第 15 条确立采取此类措施的适当保障和法律先决条件时，应谨记这些考虑。

截取内容数据(第 21 条)

228. 传统上，收集电信(如电话交谈)方面的内容数据是一种有用的调查工具，可以确定通信具有非法性质(如通信构成犯罪威胁或骚扰、犯罪阴谋或欺诈性虚假介绍)，并收集过去或未来犯罪的证据(如贩毒、谋杀、经济犯罪等)。计算机通信可以构成或提供相同类型犯罪的证据。然而，鉴于计算机技术能够传输大量数据，包括书面文本、视觉图像和声音，它更有可能犯下涉及传播非法内容(例如儿童色情制品)的犯罪。许多计算机犯罪涉及数据传输或通信，作为其犯罪的一部分；例如，为实现对计算机系统的非法访问或计算机病毒的传播而发送的通信。如果不截取信息的内容，就不可能实时确定这些通信的有害和非法性质。如果没有能力确定和防止正在进行的犯罪行为的发生，执法部门将只能调查过去已经发生的损害和犯罪。因此，对计算机通信内容数据的实时截取与对电信的实时截取同样重要，甚至更重要。

229. “内容数据”是指通信的内容；即通信的内含或目的，或者通信所传达的讯息或信息。它是作为通信的一部分传输的所有内容，而非流量数据。

230. 该条的大部分内容与第 20 条的内容相同。因此，上述有关收集或记录流量数据、合作和协助义务以及保密义务的提法同样适用于内容数据的截取。由于与内容数据相关的隐私利益较高，调查措施仅限于“国内法确定的一系列严重犯罪行为”。

231. 此外，如上文关于第 20 条的评论所述，适用于实时截取内容数据的条件和保障措施可能比适用于实时收集流量数据的条件和保障措施更严格，或适用于搜查和扣押或类似的获取或保护存储数据的条件和保障措施。

第 3 节　管辖权

管辖权(第 22 条)

232. 本条规定了一系列标准，根据这些标准，缔约国有义务对本公约第 2 至第 11 条所列举的刑事犯罪确立管辖权。

233. 第 1 款(a)项基于属地原则。要求各缔约国制裁在其领土上犯下的由本公约所确立的罪行。例如，如果攻击计算机系统的人和受害者系统都在其境内，而且被攻击的计算机系统在其境内，即使攻击者不在其境内，一个缔约国也会主张领土管辖权。

234. 曾考虑列入一项规定，要求各缔约国对涉及以其名义登记的卫星的犯罪行为确立管辖权。起草者决定，这样的规定是不必要的，因为涉及卫星的非法通信总是从地球上发出和(或)在地球上接收。因此，如果传输源自或终止于第 1 款(a)至(c)项规定的地点之一，则可使用该款规定的缔约国管辖权的依据之一。此外，如果涉及卫星通信的犯罪是由缔约国国民在任何国家的领土管辖范围以外实施的，则将有根据第 1 款(d)项的管辖权依据。最后，起草人对登记是否是主张刑事管辖权的妥当依据提出质疑，因为在许多情况下，所犯罪行与登记国之间没有任何有意义的联系，因为卫星仅仅是一个传输渠道。

235. 第 1 款(b)项和(c)项是基于属地原则的一个变体。这些条款要求各缔约国对悬挂其国旗的船舶或根据其法律注册的飞机上发生的罪行确立刑事管辖权。这项义务已在许多国家

的法律中作为一般事项予以履行，因为此类船舶和飞机经常被视为国家领土的延伸。在犯罪发生时船舶或飞机不在其境内的情况下，这种类型的管辖权最为有用，因此，第 1 款(a)项将不能作为主张管辖权的依据。如果犯罪发生在船旗国领土以外的船只或航空器上，除这一要求外，可能没有其他国家能够行使管辖权。此外，如果犯罪发生在仅仅通过另一国水域或领空的船只或飞机上，则后者行使管辖权可能面临重大的实际障碍，因此登记国也拥有管辖权是有益的。

236. 第 1 款(d)项基于国籍原则。在沿用大陆法系传统的国家中最长应用国籍理论。它规定，一国国民即使在其领土之外也有义务遵守国内法。根据(d)项，如果一个国民在国外犯罪，如果该行为根据发生地国的法律也是一种犯罪，或者该行为发生在任何国家的领土管辖范围之外，则该缔约国须能对其进行起诉。

237. 第 2 款允许缔约国对第 1 款(b)、(c)和(d)项规定的管辖权理由提出保留。但是，不允许对(a)项规定的确立属地管辖权，或对第 3 款规定的属于 "不引渡即起诉"(引渡或起诉)原则下确立管辖权的义务提出保留，即该缔约国以国籍为由拒绝引渡被指控的犯罪人，而该犯罪人在其境内的情况。如果根据本公约第 24 条第 6 款“引渡”的要求请求引渡的缔约国提出请求，则有必要根据第 3 款确立管辖权，以确保拒绝引渡国民的缔约国具有在国内进行调查和起诉的法律能力。

238. 第 1 款规定的管辖权依据不是排他性的。本条第 4 款允许当事各方根据其国内法确立其他类型的刑事管辖权。

239. 在利用计算机系统实施犯罪的情况下，有时会出现不止一个缔约国对犯罪的某些或所有参与者拥有管辖权的情况。例如，许多通过使用互联网实施的病毒攻击、欺诈和侵犯版权行为的目标是位于许多国家的受害者。为了避免工作重复、给证人造成不必要的不便或有关国家执法官员之间出现竞争，或者为了促进诉讼的效率或公平性，受影响的各方必须进行协商，以确定适当的起诉地点。在某些情况下，由有关国家选择单一的起诉地最为有效；在其他情况下，最好是由一个国家起诉某些参与者，而由一个或多个其他国家起诉其他参与者。根据本款规定，这两种结果都是允许的。最后，协商的义务不是绝对的，而是在"适当的时候"进行。因此，例如，如果缔约国知道没有必要进行协商(例如，一方已收到确认，另一方不打算采取行动)，或者如果一缔约国认为协商可能损害其调查或诉讼，它可以推迟或拒绝协商。

第三章　国际合作

240. 第三章载有关于引渡和缔约国之间司法协助的某些规定。

第 1 节　一般原则

篇目 1--关于国际合作的一般原则

关于国际合作的一般原则(第 23 条)

241. 第 23 条规定了关于第三章下国际合作的三项一般原则。

242. 首先，该条明确规定，缔约国之间应“尽可能广泛地”开展国际合作。这项原则要求各方提供广泛的合作，尽量减少信息和证据在国际上快速畅通流动的障碍。

243. 其次，第 23 条规定了合作义务的一般范围：合作范围应扩大到与计算机系统和数据有关的所有刑事犯罪(即第 14 条第 2 款(a)项和(b)项所涵盖的犯罪)，以及收集刑事犯罪的电子形式的证据。这意味着，无论是通过使用计算机系统实施的犯罪，还是没有通过使用计算机系统实施的普通犯罪(如谋杀)凡涉及电子证据，都适用第三章的规定。然而，应当指出，第 24 条(引渡)、第 33 条(关于实时收集流量数据的互助)和第 34 条(关于截取内容数据的互助)允许缔约国对这些措施的不同适用范围作出规定。

244. 最后，合作既要“根据本章的规定”进行，也要“通过适用有关刑事事项国际合作的国际文书、在统一或对等立法基础上商定的安排和国内法”进行。后一条款确立了一项一般原则，即第三章的规定不会取代关于法律互助和引渡的国际协定的规定、缔约国之间的互惠安排(下文对第 27 条的讨论有更详细的描述)或与国际合作有关的国内法规定。第 24 条(引渡)、第 25 条(有关互助的一般原则)、第 26 条(自发提供信息)、第 27 条(在无适用的国际协议的情况下提出互助请求的程序)、第 28 条(保密和使用限制)、第 31 条(关于访问存储的计算机数据的互助)、第 33 条(实时收集流量数据方面的互助)和第 34 条(截取内容数据方面的互助)均明确加强了这一基本原则。

篇目 2--有关引渡的原则

引渡(第 24 条)

245. 第 1 款规定，引渡义务仅适用于根据本公约第 2 至第 11 条确定的、根据有关双方的法律可处以剥夺自由最长至少一年或更严厉处罚的罪行。起草者决定插入一个最低限度的制裁，因为根据本公约，缔约国可以用相对较短的最长监禁期来制裁某些罪行(例如，第 2 条“非法访问”和第 4 条“数据干扰”)。有鉴于此，起草者认为要求将第 2 至第 11 条中确定的每一项罪行本身视为可引渡罪行是不合适的。因此，就一项一般要求达成了一致意见，即如果像《欧洲引渡公约》(《欧洲条约集》第 24 号)第 2 条那样，对寻求引渡的罪行可施加最高惩罚至少是一年监禁，则该罪行应被视为可以引渡。确定一项罪行是否可以引渡，并不取决于手头特定案件的实际刑罚，而是取决于对违法且要求引渡的犯罪行为可依法判处的最长期限。

246. 同时，根据第三章规定的国际合作应按照缔约国之间生效的文书进行的一般原则，第 1 款还规定，如果在两个或两个以上缔约国之间生效的引渡条约或基于统一或对等立法的安排(见下文第 27 条讨论中对该术语的描述)规定了不同的引渡门槛，则应适用此种条约或安排规定的门槛。例如，欧洲国家和非欧洲国家之间的许多引渡条约规定，只有最高处罚超过一年监禁或更严厉的处罚时，罪犯才可以引渡。在这种情况下，国际引渡工作人员将继续适用其条约惯例下的正常门槛，以确定某项罪行是否可引渡。即使根据《欧洲引渡公约》(《欧洲条约集》第 24 号)，保留也可以为引渡规定不同的最低处罚。在该公约的缔约国中，当向作出这种保留的缔约国寻求引渡时，对确定该罪行是否可以引渡，应适用保留中规定的处罚。

247. 第 2 款规定，第 1 款所述罪行应被视为包括在缔约国之间的任何引渡条约中的可引渡罪行，并应被纳入彼此之间今后可能谈判的条约中。这并不意味着每次提出请求时都必须准许引渡，而是必须有可能批准对此类罪行的人进行引渡。根据第 5 款，缔约国可以规定引渡的其他要求。

248. 根据第 3 款，缔约国如因与请求方没有引渡条约或因为现行条约并不涵盖就根据本公约确立的罪行提出的请求因而不准许引渡时，该缔约国尽管没有义务这样做，仍可以利用公约本身作为依据，移交被请求移交的人。

249. 如果缔约国不依赖引渡条约，而是利用一般法定计划进行引渡，则第 4 款要求其将第 1 款所述的罪行列入可予引渡的罪行。

250. 第 5 款规定，如果被请求方对满足适用条约或法律规定的所有条款和条件的情况并不满意，则不必引渡。因此，这是缔约国之间应根据有效的适用国际文书、对等安排或国内法条款开展合作的原则的又一个例子。例如，《欧洲引渡公约》(《欧洲条约集》第 24 号)及其附加议定书(《欧洲条约集》第 86 号和第 98 号)规定的条件和限制将适用于这些协议的缔约国，并可以此为由拒绝引渡(例如，《欧洲引渡公约》第 3 条规定，如果犯罪被认为具有政治性质，或者如果认为引渡请求是基于种族、宗教、国籍或政治见解等原因起诉或制裁某人而提出的，则应拒绝引渡)。

251. 第 6 款适用“不引渡即审判”(“引渡或起诉”)原则。由于许多国家拒绝引渡其国民，因此，除非地方当局有义务采取行动，否则在其国民所在的缔约国发现的罪犯可能会逃避对在另一缔约国所犯罪行的责任。根据第 6 款，如果另一缔约国要求引渡罪犯，而引渡被拒绝，理由是罪犯是被请求方的国民，则被请求方必须根据请求方的要求，将案件提交给主管机构起诉。如果引渡请求被拒绝的一方没有要求将案件提交当地调查和起诉，被请求方没有义务采取行动。此外，如果没有提出引渡请求，或以国籍以外的理由拒绝引渡，本款规定被请求方没有义务将案件提交国内起诉。此外，第 6 款要求地方调查和起诉应尽职尽责；必须像对待提交案件的缔约国“任何类似性质的犯罪”的相同方式认真对待此案。该缔约国应向提出请求的缔约国报告其调查和起诉的结果。

252. 为使各缔约国知道其临时逮捕或引渡请求应当向谁提出，第 7 款要求各缔约国向欧洲委员会秘书长通报其负责在没有条约的情况下提出或接受引渡或临时逮捕请求的主管机构的名称和地址。这一规定仅限于有关缔约国之间无生效的引渡条约的情况，倘若缔约国之间有双边或多边引渡条约(如《欧洲条约集》第 24 号)，缔约国应知道向谁提出引渡和临时逮捕请求，而无需登记要求。必须在签署时或在交存缔约国的批准书、接受书、核准书或加入书时向秘书长通报此事宜。应该指出的是，指定一个机构并不排除使用外交渠道的可能性。

篇目 3--有关互助的一般原则

有关互助的一般原则(第 25 条)

253. 第 1 款规定了提供互助义务的一般原则，应“尽可能广泛地”提供合作。因此，与第 23 条(″关于国际合作的一般原则″)一样，相互援助原则上应是广泛的，其障碍应受严格限制。其次，第 23 条规定了合作义务的一般范围：合作范围应扩大到与计算机系统和数据有关的所有刑事犯罪(即第 14 条第 2 款(a)和(b)项所涵盖的犯罪)，以及收集刑事犯罪的电子形式的证据。各方同意对这一大类犯罪规定合作的义务，原因在于这两类犯罪同样需要简化的国际合作机制。然而，第 34 条和第 35 条允许缔约国对这些措施规定不同的适用范围。

254. 本章的其他规定将澄清提供互助的义务一般应根据适用的司法互助条约、法律和安排的条款来履行。根据第 2 款，倘若各缔约国的条约、法律和安排尚未包含此类规定，则需要有法律依据来开展本章其余部分所述的具体合作形式。提供这种机制，特别是第 29 条至第 35 条(具体规定--第 1、2、3 编)中的机制，对于在与计算机有关的刑事调查方面开展有效合作至关重要。

255. 对于适用第 2 款所述的规定，一些缔约国不需要任何执行法案，它们认为应自动执行建立详细互助制度的国际条约的规定。预计缔约国要么能够将这些条款视为自动执行，要

么在现有的互助立法下已具备足够的灵活性来执行本章规定的互助措施，要么能够迅速颁布所需的任何这种立法。

256.计算机数据非常不稳定。通过几个按键或自动程序的操作，数据就可能会被删除，从而使人们无法追踪到犯罪行为人或者关键罪证已破坏。某些形式的计算机数据在被删除之前只存储很短的时间。在其他情况下，如果不迅速收集证据，可能会给人身或财产造成重大损害。在这种紧急情况下，不仅应迅速提出请求，也应迅速做出答复。因此，第 3 款的目标是促进加快获得互助进程，以便关键信息或证据不会因为在准备、传递和答复援助请求之前被删除而丢失。第 3 款通过以下方式实现：(1)授权缔约国通过快速通信手段提出紧急合作请求，而不是通过传统慢得多的外交邮袋或邮件递送系统传送书面密封文件；要求被请求方在这种情况下使用快速手段答复请求。如果各缔约国的互助条约、法律或安排尚未作出规定，则必须有能力采用这一措施。所列出的传真和电子邮件性质上是示意性的；在现有特殊情况下，可酌情使用任何其他快速通信手段。随着技术的进步，将进一步开发更快捷的可用于互助请求通信手段。关于本款所载的真实性和安全要求，缔约国可自行决定如何确保通信的真实性，以及是否需要在特别敏感的情况下可能需要的特别安全保护(包括加密)。最后，该款还允许被请求方要求请求方如果选择快速传送后通过传统渠道发送正式确认。

257.第 4 款规定了互助要遵守适用的司法互助条约(ML(A)Ts)和国内法律条款的原则。这些制度为在被请求方境内可能成为互助请求对象的人提供了权利保障。例如，除非被请求方适用于国内案件的侵扰性措施的基本要求得到满足，否则不得以请求方的名义执行这种措施，如搜查和扣押。缔约国还可确保通过司法协助保护与扣押和提供的物品有关的人的权利。

258.然而，如果"本章另有具体规定"，则第 4 款不适用。这一条款旨在表明，本公约包含一般原则的几个重要例外。第一种例外情况见于该条第 2 款，该款规定各缔约国有义务确定本章其余条款所规定的合作形式(如保全、实时收集数据、搜查和扣押以及维持全天候网络)，无论其司法互助条约、同等安排或互助法律目前是否对这些措施作出了规定。另一个例外见于第 27 条，在请求方与被请求方之间没有司法互助条约或同等安排的情况下，该条始终适用于执行请求，以代替被请求方关于国际合作的国内法律。第 27 条规定了拒绝的一整套条件和理由。本条特别规定的另一个例外是，至少就本公约第 2 至第 11 条规定的犯罪而言，不得以被请求方认为请求涉及"财务"犯罪为由拒绝合作。最后，第 29 条是一个例外，它规定不得以双重犯罪为由拒绝保全，尽管在这方面规定了保留的可能性。

259.第 5 款基本上是本章为互助目的对双重犯罪行为所下的定义。如果允许被请求方要求双重犯罪作为提供协助的条件(例如，被请求方根据第 29 条“迅速保全储存的计算机数据”第 4 款，保留要求在保全数据方面符合双重犯罪的权利)，如果被请求协助所涉及的行为也是被请求方法律规定的刑事犯罪，即便被请求方的法律将该罪行归入不同的犯罪类别或使用不同的术语命名该罪行，则应视为存在双重犯罪。为确保被请求方在适用双重犯罪时不会采用过于僵硬的检验标准，这一规定被认为是必要的。鉴于各国法律制度的不同，犯罪行为的术语和分类必然会出现差异。如果这种行为在两种制度下都构成犯罪，这种技术差异不应妨碍援助。相反，在适用双重犯罪标准的事这一规定被认为是必要的，以 j 项上，应以灵活的方式适用这一标准，以方便给予协助。

自发提供的信息(第 26 条)

260.本条源自欧洲委员会早期文书的规定，如《关于犯罪收益的洗白、搜查、扣押和没收问题的公约》(《欧洲条约集》第 141 号)第 10 条和《腐败问题刑法公约》(《欧洲条约集》第 173 号)第 28 条。越来越多的情况是，一缔约国掌握其认为可能有助于另一缔约国进行刑事调查或诉讼的宝贵信息，而进行调查或诉讼的一方并不知道存在这些信息。在这种情况下，不会出现互助请求。第 1 款授权拥有该信息的国家在没有事先收到请求的情况

下将信息转交给另一国家。该款被认为是有用的，因为根据一些国家的法律，为了在没有请求的情况下提供协助，需要这种积极的法律授权。一缔约国没有义务自发地将信息转发给另一缔约国；前者可根据当前案件的情况行使其自由裁量权。此外，自发披露信息并不排除披露方(如果它有管辖权)就所披露的事实开展调查或提起诉讼。

261.第 2 款涉及的事实是，在某些情况下，只有能够对敏感信息加以保密或对信息的使用施以其他条件限制的情况下，缔约国才会自发提供信息。特别是，如果信息被公开，可能会危及提供国的重要利益，例如，需要保护收集信息手段的身份或正在调查一个犯罪集团事实，那么保密性将是一个重要考虑因素。如果预先查询显示，接收方不能遵守提供方要求的条件(例如，由于信息需要作为公开审判的证据而不能遵守保密条件)，接收方应告知提供方，尔后提供方可以选择不提供信息。然而，如果接受方同意这一条件，则必须遵守该条件。可以预见的是，本条规定的条件应与提供方应接受方的互助请求所施加的条件相一致。

篇目 4--在无适用的国际协议情况下提出互助请求的程序

在无适用的国际协定情况下提出互助请求的程序(第 27 条)

262.第 27 条规定，在请求方与被请求方之间没有基于统一或对等立法的互助条约或安排的情况下，缔约国有义务适用某些互助程序和条件。因此，该条强化了应通过适用相关条约和类似的互助安排开展互助的一般原则。起草者拒绝按照本公约设立一个单独的一般互助制度，以取代其他适用的文书或安排，而是同意作为一个一般事项，依赖现有的司法互助条约制度更为实际，从而允许互助工作人员使用其最熟悉的文书和安排，避免因设立相互竞争的制度可能造成混乱。如前所述，只有对于在与计算机有关的刑事事项中快速有效合作特别必要的机制，如第 29 至 35 条(具体规定——见篇目 1、2、3)中的机制，如果目前的互助条约、安排或法律尚未奠定法律基础，则要求各缔约国奠定此种法律基础，以便能够开展这种形式的合作。

263.因此，本章规定的大多数互助的形式将继续按照《欧洲刑事事项互助公约》(《欧洲条约集》第 30 号)及其议定书(《欧洲条约集》第 99 号)在这些文书的缔约国之间实行。或者，如果本公约缔约国之间有双边司法互助条约或其他关于刑事案件互助的多边协定(例如欧洲联盟成员国之间)，除非它们同意适用本条的全部或任何规定，否则应继续适用其条款，并辅之以第三章其余部分所述的专门针对计算机或与计算机有关犯罪的机制。互助也可以基于在统一或对等立法基础上商定的安排，例如北欧国家之间建立的合作制度，该制度也得到《欧洲刑事事项互助公约》(第 25 条第 4 款)以及英联邦成员国之间的承认。最后，提及以统一或对等立法为基础的互助条约或安排，不仅限于本公约生效时有效的文书，还包括未来可能通过的文书。

264.第 27 条(关于在无适用的国际协议的情况下提出互助请求的程序)第 2 至第 10 款规定了一些规则，用于在没有司法互助条约或基于统一或对等立法的安排的情况下提供互助的一些规则，包括设立中央机关、规定在推迟或拒绝情况下的条件、理由和程序、对请求保密以及直接联络。对于此类明确涵盖的问题，在没有统一或对等立法基础上的互助协议或安排的情况下，本条的规定将取代其他适用的国内互助法律。同时，第 27 条并没有为通常由涉及国际互助的国内立法处理的其他问题确定规则。例如，没有规定涉及请求的形式和内容、在被请求方或请求方获取证人证词、提供官方或商业记录、移交被羁押的证人或在没收事宜中提供援助。关于这类问题，第 25 条第 4 款规定，如果本章没有具体规定，提供这类援助的具体方式应受被请求方的法律管辖。

265. 第 2 款要求设立一个或多个中央机关，负责发送和答复援助请求。中央机关是处理刑事事宜互助的现代文书的一个共同特点，它特别有助于确保打击计算机或与计算机有关的犯罪活动所需的快速反应。最初，这种机构之间的直接传送比通过外交渠道传递更快、更有效。此外，设立一个积极的中央机关可以发挥重要作用，确保认真处理收到和发出的请求，就如何更好地满足被请求方的法律要求向外国执法伙伴提供咨询意见，并确保特别紧急或敏感的请求得到妥善处理。

266. 为提高效率，鼓励缔约国为互助目的指定一个中央机关；一般来说，在适用本条时，由缔约国根据司法互助条约或国内法为此目的指定的机构兼任中央机关是最有效率的。然而，缔约国在互助制度下，可以在适当的情况下灵活指定一个以上的中央机关。如果设立了不只一个中央机关，已经设立的缔约国应确保每个机关都以同样的方式解释本公约的规定，并确保迅速有效地处理收到的和发出的请求。各缔约国均应向欧洲委员会秘书长通报被指定接收和答复本条规定的互助请求的一个或多个机关的名称和地址(包括电子邮件和传真号码)，缔约国有义务确保其指定机关没有过时。

267. 请求互助的国家的一个主要目标是确保遵守国内关于证据可采用性的法律，因而能够在法院使用该证据。为确保这种证据要求能够得到满足，第 3 款规定被请求方有义务按照请求方规定的程序执行请求，除非这样做与其法律相抵触。需要强调的是，本款仅涉及遵守技术程序要求的义务，与基本程序保护无关。因此，例如，请求方不能要求被请求方实施不符合其针对该措施的基本法律要求的搜查和扣押。鉴于该义务的有限性质，各方一致认为，仅凭被请求方的法律系统不了解此种程序这一事实就不足以构成拒绝适用请求方所要求的程序的理由；相反，该程序必须与被请求方的法律原则不符才能成立。例如，根据请求方的法律，证人对陈述进行宣誓可能是一项程序上的要求。即使被请求方在国内没有宣誓作证的要求，也应尊重请求方的请求。

268. 第 4 款规定了拒绝本条所述的互助请求的可能性。可以根据第 25 条第 4 款确定的理由(即被请求方法律规定的理由)拒绝协助，包括损害国家主权、安全、公共秩序或其他基本利益，以及被请求方认为是政治犯罪或与政治犯罪有关的罪行。为了促进应提供最广泛合作这一首要原则(见第 23 和 25 条)，被请求方应缩小所制订的拒绝理由的范围并有节制地使用。这些理由不能过于宽泛，以免造成对类别广泛的证据或信息断然拒绝提供协助或施加苛刻条件的可能。

269. 根据这一方法，可以理解，除了第 28 条规定的那些理由外，只有在特殊情况下才能以数据保护为由拒绝提供协助。如果在权衡特定案件所涉及的重要利益(一方面是公共利益，包括健全的司法行政，另一方面是隐私利益)后，提供请求方要求的具体数据会引起重大困难，以致被请求方认为属于出于基本利益的拒绝理由，就可能出现这种情况。因此，禁止广泛、明确或系统地利来用数据保护原则来拒绝合作。因此，有关各方保护数据隐私的制度不同(例如，请求方没有专门的数据保护机构)或保护个人数据的手段不同(例如，请求方使用删除程序以外的手段保护执法机构收到的个人数据的隐私性或准确性)，这并不构成拒绝的理由。在援引“基本利益”作为拒绝合作的依据之前，被请求方应尝试提出允许传输数据的条件，(见第 27 条第 6 款和本报告第 271 段)。

270. 第 5 款允许被请求方在立即对请求采取行动会有损于被请求方的调查或诉讼程序的情况下推迟而不是拒绝提供协助。举例来说，如请求方为调查或审讯的目的谋求取得证据或证人证词，但被请求方在即将进行的审讯中需要同样的证据或证人，则被请求方有理由推迟提供协助。

271. 第 6 款规定，如果所寻求的援助本来会被拒绝或推迟，被请求方可以在有条件的情况下提供协助。如果请求方不同意这些条件，被请求方可修改这些条件，或行使拒绝或推迟援助的权利。由于被请求方有义务提供尽可能广泛的协助，双方同意在提出拒绝的理由和条件时应有所节制。

272.第 7 款规定，被请求方有义务随时向请求方通报请求的结果，并要求在拒绝或推迟援助的情况下说明理由。提供理由除其他外可协助请求方了解被请求方如何解释本条的要求，为协商提供基础，以提高日后的互助效率，以及向请求方提供以前不为人知的有关证人或证据的可用性或状况的事实材料。

273.有时，缔约国在特别敏感的案件中提出请求，或者如果过早公开请求背后的事实，可能会产生灾难性的后果。因此，第 8 款允许请求方要求对请求之事和其内容保密。但是，如果保密会损害被请求方获得所需证据或信息的能力，则不得要求保密，例如，为了获得实施援助所需的法院命令而需要披露信息，或者为了成功执行请求而需要让拥有证据的私人知道该请求。如果被请求方不能满足保密请求，则应通知请求方，请求方可选择撤回或修改该请求。

274.根据第 2 款指定的中央机关应相互直接联系。但是，在紧急情况下，请求方的法官和检察官可以直接向被请求方的法官和检察官发出司法协助请求。采用这一程序的法官或检察官还必须提交一份向其本国中央机关提出的请求副本，以便由它转交被请求方的中央机关。根据(b)项规定，请求可通过国际刑警组织转达。被请求方中央机关在收到不属于其职权范围的请求时，根据(c)项规定，有两方面的义务。首先，必须将请求转交给被请求方的主管机构。第二，必须将所作的转交通知请求方中央机关。根据(d)项，即使没有紧急情况，也可以在没有中央干预的情况下直接提出请求，只要被请求方中央机关能够遵守请求而不使用胁迫行动。最后，(e)项使缔约国能够通过欧洲委员会秘书长通知其他缔约国，出于效率原因，应与其中央机关直接沟通。

保密性和使用限制(第 28 条)

275.这项规定特别对信息或材料的使用作出限制，以便被请求方对于特别敏感的信息或材料，确保其使用仅限于给予协助的范围，或确保其不会流入请求方执法人员以外者手中。这些限制提供了可用于数据保护等目的的保障措施。

276.与第 27 条的情况一样，第 28 条只适用于请求方和被请求方之间没有互助条约或基于统一或对等立法安排的情况。如果这种条约或安排已生效，其关于保密性和使用限制的规定应代替本条的规定，除非缔约国另有约定。这避免了与现有的双边和多边司法互助条约及类似安排重叠，从而使执业人员能够继续在所熟悉的正常制度下运作，而不是寻求适用两种相互竞争、可能相互矛盾的文书。

277.第 2 款允许被请求方在回应互助请求时提出两类条件。首先，如果在缺乏这种条件的情况下(例如涉及机密信息提供者的身份)不能遵守要求，它可以要求对所提供的信息或材料予以保密。在被请求方有责任提供所要求的协助的个案中，要求绝对保密是不适当的，因为在很多情况下，这会妨碍请求方成功调查或检控罪行的能力，例如在公开审讯中使用证据(包括强制性披露)。

278.其次，被请求方可规定提供信息或材料的条件是，这类信息或材料不得用于请求所述以外的调查或诉讼。为使这一条件适用，被请求方必须明确提及这一条件，否则，请求方的使用不受这一限制。在已提及的情况下，这一条件将确保信息和材料只能用于请求中指明的目的，从而排除了未经被请求方同意将材料用于其他目的的可能性。谈判者认识到限制使用能力的两种例外情况，它们隐含在该款的规定中。首先，根据许多国家的基本法律原则，如果所提供的材料是证明被告无罪的证据，则必须向辩方或司法机构披露。此外，根据互助制度提供的大部分材料均旨在审判中使用，通常是公开程序(包括强制性披露)。一旦做出这种披露，该材料基本上就进入了公共领域。在这类情况下，不可能确保对寻求互助的调查或程序保密。

279. 第 3 款规定，如果接受信息的缔约国不能遵守规定的条件，它应通知提供信息的缔约国，而后一缔约国可以选择不提供信息。然而，如果接受方同意该条件，则必须予以遵守。

280. 第 4 款规定，可以要求请求方对其在第 2 款所述条件下收到的信息或材料的使用情况作出解释，以便被请求方可以确定这种条件是否得到遵守。经商定，不得要求被请求方提供过于繁琐的说明，例如每次访问所提供的材料或信息的时间。

第 2 节　具体规定

281. 本节的目的是规定具体机制，以便在涉及计算机相关犯罪和电子形式证据的案件中采取有效和协调一致的国际行动。

篇目 1--关于临时措施方面的互助

迅速保全存储的计算机数据(第 29 条)

282. 本条规定了一个国际一级的机制，相当于第 16 条规定的供国内使用的机制。本条第 1 款授权缔约国提出请求，要求各缔约国有法律能力迅速保全在被请求方境内通过计算机系统存储的数据，以便在准备、传递和执行获取数据互助请求所需的时间内不更改、移除或删除数据。保全是一种有限的临时性措施，旨在比实施传统的互助要快得多。如前所述，计算机数据是高度不稳定的。只需按几下键盘或通过自动程序操作就可能删除、更改或移除数据，从而无法追踪到犯罪者，或销毁关键的犯罪证据。某些形式的计算机数据在被删除之前只存储很短的时间。因此，各方一致认为，需要建立一种机制，以确保在执行正式互助请求这一更长、更复杂的过程(可能需要数周或数月的时间)之前提供这类数据。

283. 虽然这项措施比一般的互助做法快得多，但侵扰性较低。被请求方互助负责官员无须向数据保管者取得对数据的拥有。被请求方的首选程序是确保保管者(通常是服务供应商或其他第三方)保留(而不是删除)数据，以等待启动程序，并要求在稍后阶段将数据移交给执法人员。这项程序的优点是既快捷又能保障有关人员的私隐，因为在符合一般互助制度所规定的全面披露准则之前，任何政府官员都不会披露或审查有关材料。同时，被请求方获准使用其他程序确保迅速保存数据，包括加快签发和执行数据出示令或搜查令。关键要求是要有一个极为快速的流程，以防数据不可挽回地丢失。

284. 第 2 款规定了根据本条提出的保全请求的内容。考虑到这是一项临时措施，而且需要迅速准备和传送请求，所提供的信息需简明扼要，只包括能够保存数据的最低限度的信息。除了具体说明寻求保全的机构和寻求措施的犯罪行为外，请求必须提供事实摘要、足以确定要保全的数据及其位置的信息，并表明该数据与调查或起诉所涉罪行有关，以及保全实属必要。最后，请求方必须承诺随后将提交互助请求，以便其获得数据的出示。

285. 第 3 款阐述了不要求双重犯罪作为提供保全条件的原则。一般来说，在保全方面，适用双重犯罪原则会适得其反。首先，在现代互助实践中，除最具侵扰性的程序措施，如搜查、扣押或截取外，其他所有措施均有取消双重犯罪规定的趋势。然而，按照起草者的设想，保全并不特别具有侵扰性，因为保管者只是保持对其合法拥有的数据的持有，而且在执行寻求披露数据的正式互助请求之前，这些数据不会向被请求方官员披露或受到审查。其次，作为一个实际问题，提供必要的澄清以最终确定双重犯罪的存在往往需要很长时间，以至于数据会在这一期间被删除、移除或更改。例如，在调查的早期阶段，请求方可能意识到其境内的计算机受到了入侵，但可能直到后来才对损害的性质和程度有充分的了解。如果被请求方在确定双重犯罪之前推迟保全可追踪入侵来源的流量数据，关键数据通常只

在传输后几小时或几天内即被服务供应商删除。其后即使请求方能够确立双重犯罪，但关键的流量数据已无法恢复，犯罪者也将永远无法被识别。

286. 因此，一般规则是，缔约国为了保全的目的，必须免除任何双重犯罪要求。但是，根据第 4 款，可以作出有限的保留。如果一缔约国要求将双重犯罪作为回应提供数据互助请求的条件，而且有理由相信在披露时不会满足双重犯罪要求，它可以保留要求双重犯罪作为保全的前提条件的权利。关于根据第 2 条至第 11 条确立的犯罪，假定缔约国之间自动满足双重犯罪的条件，但在本公约允许的情况下，它们可能对这些犯罪提出任何保留。因此，缔约国只能对本公约所界定的罪行以外的罪行施加这一要求。

287. 否则，根据第 5 款，被请求方只能在执行保全请求将损害其主权、安全、公共秩序或其他基本利益的情况下，或在其认为该罪行是政治罪或与政治罪有关的罪行的情况下拒绝保全请求。由于这一措施对于有效调查和起诉计算机犯罪或与计算机有关的犯罪具有核心意义，各方同意排除以任何其他理由拒绝保全请求的情况。

288. 被请求方有时会意识到数据保管者可能会采取威胁请求方调查的保密性或以其他方式损害请求方调查的行动(例如，须保全的数据由犯罪集团控制下的服务供应商持有，或由调查对象本身持有)。在这种情况下，根据第 6 款，必须迅速通知请求方，以便它可以评估是承担继续实施保全请求带来的风险，还是寻求更具侵扰性但更安全的互助形式，如出示或搜查和扣押。

289. 最后，第 7 款要求各缔约国确保根据本条保全的数据在收到寻求披露数据的正式互助请求之前至少保存 60 天，并在收到请求后继续保全。

加快披露保存的流量数据(第 30 条)

290. 该条规定了与第 17 条规定的国内使用权力相当的国际权力。通常，应犯罪发生地缔约国的请求，被请求方会保全通过其计算机传输的流量数据，以便追踪传输的源头，确定犯罪人，或找到关键证据。在这样做时，被请求方可能会发现，在其领土上发现的流量数据表明，传输是从第三国的服务供应商或请求方本身的供应商那里发送的。在这种情况下，被请求方须迅速向请求方提供足够数量的流量数据，以便能够识别对方国家的服务供应商及其通信路径。如果传输来自第三国，此信息将使请求方能够向该国提出保全和加快互助请求，以便追查传输的最终源头。如果传输绕圈返回请求方，它将能够通过国内程序获得更多流量数据的保全和披露。

291. 根据第 2 款，只有在披露流量数据可能损害被请求方主权、安全、公共秩序或其他基本利益，或被请求方认为有关罪行属于政治罪或与政治罪有关的罪行时，被请求才可以拒绝披露流量数据。正如第 29 条(迅速保全储存的计算机数据)所述，由于这类信息对于确认在本本公约范围内犯下罪行的人或寻找关键证据非常关键，拒绝的理由应受到严格限制，并一致认为，拒绝援助的任何其他理由均不成立。

篇目 2--关于调查权的互助

关于访问存储的计算机数据的互助(第 31 条)

292. 各缔约国必须有能力为协助另一缔约国搜查或以类似方式访问、扣押或以类似方式保护通过其境内的计算机系统存储的数据——正如第 19 条(搜查和扣押存储的计算机数据)所规定的那样，它必须有能力为国内目的这样做。第 1 款授权缔约国请求这类互助，第 2 款要求被请求方能够提供这种互助。第 2 款还遵循以下原则，即提供这种合作的条款和条件

应是适用的条约、安排和国内法律中关于刑事事项法律互助的条款和条件。根据第 3 款，如果(1)有理由相信相关数据特别容易丢失或被修改，或(2)此类条约、安排或法律有如此规定，必须迅速答复此类请求。

经同意或在可公开获得的情况下跨境访问存储的计算机数据(第 32 条)

293.本公约起草者详细讨论了如下问题，即何时允许一个缔约国在不寻求互助的情况下单方面访问另一个缔约国存储的计算机数据。详细审议了哪些情况下国家可以接受单方面行动，哪些情况下不可以。起草者最终决定，目前还不可能制定一个全面、具有法律约束力的制度来规范这一领域。这在一定程度上是因为迄今为止缺乏处理此类情况的具体经验；而且，这在一定程度上是因为人们认识到，适当的解决办法往往取决于个别案件的具体情况，因此难以制定一般规则。最终，起草者决定只在本公约第 32 条中规定所有人都同意允许单方面行动的情况。他们同意，在进一步收集经验，并可能根据这一情况作出进一步讨论之前，不规范其他情况。在这方面，第 39 条第 3 款规定，既不准许也不排除其他情况。

294.第 32 条(经同意或在可公开获得的情况下跨境访问存储的计算机数据)涉及两种情况：第一，被访问的数据是可公开获得的；第二，该缔约国通过其领土上的计算机系统访问或接收了位于其领土以外的数据，并获得了拥有通过该系统向该缔约国披露该数据的合法权力者的合法自愿同意。谁是“合法授权”披露数据的人，可能会因情况、有关人员的性质和适用法律的不同而异。例如，一个人的电子邮件可能被服务供应商存储在另一个国家，或者一个人可能故意将数据存储在另一个国家。这些人可以检索数据，如果他们拥有合法权限，既可以按照该条的规定，自愿向执法人员披露数据或允许这类人员查阅数据。

实时收集流量数据方面的互助(第 33 条)

295.在许多情况下，调查人员无法确保他们能够通过跟踪先前传输的记录来追踪通信的来源，因为传输链中的关键流量数据可能在保全之前已被服务供应商自动删除。因此，至关重要的是各缔约国的调查人员都有能力实时获取有关通过其他缔约国的计算机系统进行的通信的流量数据。因此，根据第 33 条(实时收集流量数据方面的互助)，各缔约国都有义务为另一缔约国实时收集流量数据。虽然这一条要求缔约国在这些问题上进行合作，但这里和其他地方一样，需尊重现有的互助方式。因此，提供这种合作的条款和条件通常是有关刑事事项法律互助的适用条约、安排和法律中规定的条款和条件。

296.许多国家对流量数据的实时收集提供了广泛互助，因为这种收集被视为比截取或搜查和扣押内容数据的侵扰性要小。然而，一些国家采取了较为狭窄的做法。因此，正如缔约国可以根据第 14 条(程序规定的范围)第 3 款对同等国内措施的范围提出保留一样，第 2 款允许缔约国将该措施的适用范围限制在比第 23 条(有关国际合作的一般原则)规定的范围更窄的犯罪行为。其中规定了一个注意事项：在任何情况下，犯罪范围都不得比在同等国内情况下可采取这种措施的犯罪范围更窄。事实上，由于实时收集流量据有时是确定犯罪人身份的唯一途径，而且由于该措施的侵扰性较小，因此在第 2 款中使用“至少”一词的目的是鼓励各缔约国允许尽可能广泛的协助，即便在没有双重犯罪的情况下也是如此。

截取内容数据方面的互助(第 34 条)

297.由于截取的侵扰程度较高，为截取内容数据提供互助的义务受到限制。应在缔约国适用的条约和法律允许的范围内提供援助。由于为截取内容提供合作是一个新出现的互助实践领域，因此决定遵从现行互助制度和国内法律有关协助义务的范围和限制。在这方面，请参考对第 14、15 和 21 条的评论，以及关于《欧洲刑事事项互助公约》在截取电信的调查委托书的实际应用的第 R(85)10 号建议。

篇目 3-全天候网络

全天候网络(第 35 条)

298.如前所述，有效打击利用计算机系统实施的犯罪和有效收集电子形式的证据需要作出非常迅速的反应。此外，只需敲击几下键盘，在世界某地采取的行动就会立即在数千公里之外和许多时区产生影响。因此，现有的警务合作和互助模式需要有补充渠道，才能有效地应对计算机时代的挑战。本条所建立的渠道是基于在八国集团主持下建立的一个已经运作的网络所取得的经验。根据本条规定，各缔约国有义务指定一个每周 7 天、每天 24 小时运转的联络点，以确保为本章范围内的调查和诉讼提供即时援助，特别是第35条第1款(a)至(c)项规定的援助。各方一致认为，建立这一网络是本公约提供的最重要手段之一，以确保缔约国能够有效应对计算机或与计算机有关的犯罪构成的执法挑战。

299.各缔约国的全天候联络点主要是协助或直接提供技术咨询、保全数据、收集证据、提供法律信息和确定嫌疑人的位置。第 1 款中的“法律信息”一词是指向寻求合作的另一缔约国就提供正式或非正式合作所需的任何法律先决条件的建议。

300.各缔约国均可自由决定在其执法机构内将联络点设在何处。有些缔约国可能希望将全天候联络点设在其中央互助机构内，有些缔约国可能认为最佳地点是专门打击计算机犯罪或与计算机有关的犯罪的警察单位，但鉴于某一缔约国的政府结构和法律制度，其他选择可能对其更合适。由于全天候联络点既要为阻止或追踪攻击提供技术建议，又要履行查找嫌疑人等国际合作职责，因此没有唯一的正确答案，而且预计网络结构将随着时间的变化而变化。在指定国家联络点时，应适当考虑与使用其他语言的联络点沟通的需要。

301.第 2 款规定，全天候联络点要执行的关键任务之一是有能力促进快速执行其本身不直接执行的职能。例如，如果一个缔约国的全天候联络点是警察单位的一部分，它必须有能力迅速与其政府内部的其他相关部门协调，例如负责国际引渡或互助的中央机关，以便可以在白天或夜晚的任何时候采取适当的行动。此外，第 2 款要求每个缔约国的全天候联络点有能力迅速与网络的其他成员进行联络。

302.第 3 款要求网络中的每个联络点都有恰当的设备。最新的电话、传真和计算机设备对网络的顺利运行至关重要，随着技术的进步，其他形式的通信和分析设备也将成为系统的一部分。第 3 款还要求作为缔约国网络团队成员的人员接受有关计算机或与计算机有关的犯罪以及如何有效应对的适当培训。

第五章　最后条款

303.除某些例外情况，本章所载的大部分规定是基于 1980 年 2 月部长委员会在第 315 次代表会议上批准的《欧洲委员会内缔结的公约和协定的示范性最后条款》。由于第 36 至 48 条中的大多数规定要么使用示范条款的标准用语，要么以欧洲委员会条约制定的长期实践为基础，因此不需要具体评论。然而，对标准示范条款或一些新条款的某些修改需要作一些解释。在这方面，应当指出，示范条款是作为一套不具约束力的条款获得通过的。正如示范条款的导言所指出的那样，“这些示范性最后条款只是为了方便专家委员会的工作，避免出现没有任何实际理由的文本差异。该模式并无约束力，不同的条款可能会为了因应个别情况而作出调整。“

签署和生效(第 36 条)

304. 第 36 条第 1 款的起草遵循了在欧洲委员会框架内制定的其他公约中确立的若干先例，例如《被判刑人移交公约》(《欧洲条约集》第 112 号)和《关于犯罪收益的洗白、搜查、扣押和没收问题的公约》(《欧洲条约集》第 141 号)，这两项公约不仅允许欧洲委员会成员国签署，而且允许参与拟订上述公约的非成员国签署。这一规定的目的是使尽可能多的感兴趣的国家，而不仅仅是欧洲委员会成员，尽快成为缔约国。在此，该条款拟适用于积极参与本公约制定工作的四个非成员国——加拿大、日本、南非和美国。本公约一旦生效，根据第 3 款，可邀请本条款未涵盖的其他非成员国根据第 37 条第 1 款加入本公约。

305. 第 36 条第 3 款规定本公约生效所需的批准书、接受书或核准书的数量为 5 个。这一数字高于欧洲委员会条约中通常的门槛(3 个)，反映了这样一种信念，即需要一个稍微大一点的国家集团才能成功地开始应对国际计算机或与计算机有关的犯罪的挑战。然而，这一数字并不高，以免不必要地拖延本公约的生效。在最初的五个国家中，至少有三个必须是欧洲委员会成员，但另外两个国家可以来自参与本公约制定的四个非成员国。当然，这一规定还允许本公约在欧洲委员会五个成员国表示同意受其约束的基础上生效。

加入公约(第 37 条)

306. 第 37 条也是根据欧洲委员会其他公约中确立的先例起草的，但增加了一个明确的内容。根据长期惯例，部长委员会在与所有缔约国(无论是否是成员国)协商后，主动或应请求决定邀请一个未参与公约制定的非成员国加入公约。这意味着如果任何缔约国反对非成员国加入，部长委员会通常不会邀请该国加入公约。然而，根据通常的行文，部长委员会理论上可以邀请这样一个非成员国加入公约，即使一个非成员国反对其加入。这意味着，从理论上说，在将欧洲委员会条约扩大到其他非成员国的过程中，通常不会给予非成员国否决权。然而，加入了一项明确要求，即部长委员会在邀请一个非成员国加入本公约之前，必须与所有缔约国(而不仅仅是欧洲委员会成员国)协商，并取得一致同意。如上所述，这一要求符合实践，并认识到本公约的所有缔约国都应能够确定将与哪些非成员国建立条约关系。然而，依照惯例，邀请非成员国加入的正式决定将由有权担任部长委员会成员的缔约国代表作出。这一决定需要《欧洲委员会规约》第 20 条(d)项规定的三分之二多数票和有权参加部长委员会的缔约国代表的一致表决。

307. 寻求加入本公约但打算根据第 41 条作出声明的联邦国，必须事先提交第 41 条第 3 款所指的声明草案，以便缔约国能够评估联邦条款的适用将如何影响未来缔约国对本公约的执行(见第 320 段)。

公约的效力(第 39 条)

308. 第 39 条第 1 款和第 2 款涉及本公约与其他国际协定或安排的关系。上文提到的示范性条款不涉及欧洲委员会各项公约之间或与欧洲委员会以外缔结的其他双边或多边条约之间的联系问题。欧洲委员会刑法领域的公约(例如《关于海上非法贩运的协定》(《欧洲条约集》第 156 号)通常采用的做法是规定：(1)新公约不影响现有关于特殊事项的国际多边公约所产生的权利和承诺；(2)新公约缔约国可就公约所处理的事项相互缔结双边或多边协定，以补充或加强公约的规定，或促进公约所体现的原则的适用；(3)如新公约的两个或两个以上缔约国已就公约所处理的某一主题缔结协定或条约，或以其他方式就该主题建立关系，则它们有权适用该协定或条约或相应地调整这些关系，以代替新公约(只要这有利于国际合作)。

309. 由于本公约总的意图是补充而非取代缔约国之间的多边和双边协定和安排，起草者认为可能对“特殊事项”进行限制的提法并不特别有指导意义，他们担心这可能会导致不必要的混乱。相反，第 39 条第 1 款仅指出，本公约补充了缔约国之间的其他适用条约或安排，并作为几个例子特别提到三项欧洲委员会条约：1957 年《欧洲引渡公约》(《欧洲条约集》第 24 号)、1959 年《欧洲刑事事项互助公约》(《欧洲条约集》第 30 号)及其 1978 年《附

加议定书》(《欧洲条约集》第 99 号)。因此，就一般事项而言，此类协议或安排原则上应由《网络犯罪公约》缔约国适用。关于仅由本公约处理的具体事项，“特别法优于一般法”的解释规则规定，缔约国应优先考虑本公约所载的规则。第 30 条就是一个例子，该条规定，在必要时应加快披露保存的流量数据，以查明特定通信的路径。在这一具体领域，本公约作为特别法，应确定一项优先于一般互助协定条款的规则。

310.同样，起草者认为，将现有或未来协定的适用取决于它们是否“加强”或“促进”合作的措辞可能存在问题，因为根据“国际合作一章”确定的办法，推定缔约国将适用相关的国际协定和安排。

311.如果有现行的互助条约或安排作为合作的基础，则本公约只在有需要时补充现有的规则。例如，如果原条约或安排不存在如下可能，本公约将规定通过快速通信方式(见第 25 条第 3 款)传送互助请求。

312.根据本公约的补充性质，特别是其对国际合作的处理方式，第 2 款规定，缔约国还可以自由适用已经生效或将来可能生效的协定。这种表述的先例见于《被判刑者转移公约》(《欧洲条约集》第 112 号)。当然，在国际合作方面，预期其他国际协议(其中许多协议提供了行之有效的长期国际援助方案)实际上会促进合作。根据本公约的规定，缔约国也可以同意适用其国际合作条款来代替其他此类协议(见第 27 条第 1 款)。在这种情况下，第 27 条规定的有关合作规定将取代此类其他协定中的有关规则。由于本公约一般规定最低限度的义务，第 39 条第 2 款承认，除了本公约已经规定的义务之外，缔约国在就本公约所涉事项建立关系时，可以自由承担更具体的义务。然而，这不是一项绝对权利：缔约国在这样做时必须遵守本公约的目标和原则，因此不能接受违背其宗旨的义务。

313.此外，在确定本公约与其他国际协定的关系时，起草者还同意，缔约国可从《维也纳条约法公约》的相关条款中寻求更多的指导。

314.虽然本公约提供了一个亟需的协调程度，但它并不打算解决所有悬而未决涉及计算机或与计算机有关的犯罪的问题。因此，插入第 3 段是为了明确指出，本公约只影响其涉及的内容。不受影响的是可能存在，但本公约未涉及的其他权利、限制、义务和责任。这种“保留条款”的先例可以在其他国际协定中找到(例如，联合国《制止向恐怖主义提供资助的国际公约》)。

声明(第 40 条)

315.第 40 条提及某些条款，主要涉及本公约在实体法部分确立的犯罪，其中允许缔约国纳入某些特定的补充内容，以修改条款的范围。这些补充内容旨在适应某些概念或法律上的差异，在一项拥有全球目标的条约中，这些差异比在纯粹的欧洲委员会背景下可能更有理由。通常认为声明是对本公约条款的可接受的解释，应与保留区分开来，后者允许一个缔约国排除或修改本公约中规定的某些义务的法律效力。由于本公约缔约国必须了解其他缔约国附加了哪些内容(如果有的话)，因此有义务在签署时或在交存批准书、接受书、核准书或加入书时，向欧洲委员会秘书长申明。这种通知对于罪行的定义特别重要，因为缔约国在适用某些程序性权力时，必须符合双重犯罪的条件。关于声明，认为没有必要设置数量限制。

联邦条款(第 41 条)

316.依照吸纳尽可能多的国家成为缔约国的目标，第 41 条允许提出保留，目的是照顾到联邦国家由于中央和地方当局之间权力分配的特点可能面临的困难。在刑法领域以外，存在

着对其他国际协定作出联邦声明或保留的先例[1](1)。在此，第 41 条承认，作为联邦制国家的缔约国，由于既定的国内法律和实践，可能会出现覆盖范围的细微变化。这种变化必须基于宪法或其他关于中央政府与联邦国家的组成州或领土实体之间在刑事司法事项上有关权力划分的基本原则。本公约起草者一致认为，联邦条款的实施只会导致公约适用上的微小变化。

317. 例如，在美国，根据宪法和联邦制的基本原则，联邦刑事立法通常根据其对跨州或外国商业的影响来规范行为，而最低限度或纯粹地方性的事项，传统上由组成州来规范。这种联邦制方法仍然规定了美国联邦刑法对本公约所包括的非法行为的广泛覆盖，但承认各组成州将继续监管影响很小或纯属地方性质的行为。在某些情况下，在国家法律而非联邦法律监管的这一狭窄类别的行为中，一个组成州可能不会规定本来属于本公约范围的措施。例如，只有根据发生攻击的国家的法律规定，对独立的个人计算机或连接在一栋建筑物内的计算机网络攻击才有可能是犯罪；然而，如果通过互联网进入计算机，该攻击将属于联邦犯罪，因为互联网的使用对跨州或外国商业提供了援引联邦法律所需的影响。通过美国联邦法律或在类似情况下通过另一个联邦制国家的法律执行本公约，将符合第 41 条的要求。

318. 联邦条款的适用范围仅限于第二章(实体刑法、程序法和管辖权)的规定。对于利用该条款的联邦国家来说，即使逃犯或证据所在的组成州或其他类似的领土实体没有将该行为定为犯罪或没有本公约规定的程序，它仍有义务根据第三章与其他缔约国合作。

319. 此外，第 41 条第 2 款规定，联邦国家在根据本条第 1 款提出保留时，不得以适用这种保留的条款来排除或大幅减少其对第二章所规定的措施的义务。总的来说，它应提供针对这些措施的广泛而有效的执法能力。对于属于组成州或其他类似领土实体立法管辖范围的条款，联邦政府应将这些条款提交给这些实体的主管机构，并表示赞同，鼓励它们采取适当行动使其生效。

保留(第 42 条)

320. 第 42 条规定了一些保留的可能性。这种做法源于以下事实，即本公约涵盖的刑法和刑事诉讼法领域对许多国家来说都是相对较新的。此外，本公约的全球性质——它将向欧洲委员会成员国和非成员国开放——使得其有必要拥有这种保留的可能性。这些保留的可能性旨在使尽可能多的国家能够成为本公约的缔约国，同时允许这些国家保持符合其国内法的某些做法和概念。与此同时，起草者努力限制提出保留的可能性，以便最大限度地确保缔约国统一适用本公约。因此，除了列举的保留外，不得提出其他保留。此外，只有在一缔约国签署时或交存批准书、接受书、核准书或加入书时，方可提出保留。

321. 认识到对于某些缔约国来说，某些保留对于避免与其宪法或基本法律原则相抵触是必不可少的，第 43 条没有对撤回保留规定具体时限。相反，一旦情况允许，就应立即撤回。

322. 为了对缔约国保持一定的压力，使其至少考虑撤回保留，本公约授权欧洲委员会秘书长定期询问撤回保留的前景。询问这种可能性是欧洲委员会若干文书规定的现行做法。因此，缔约国有机会表明其是否仍然需要维持对某些条款的保留，并随后撤回那些不再需要的保留。希望随着时间的推移，缔约国能够尽可能多地撤回保留，以促进本公约的统一实施。

修正(第 44 条)

[1] 例如，1951 年 7 月 28 日《关于难民地位的公约》第 34 条；1954 年 9 月 28 日《关于无国籍人地位的公约》第 37 条；1958 年 6 月 10 日《承认及执行外国仲裁裁决公约》第 11 条；1972 年 11 月 16 日《保护世界文化和自然遗产公约》第 34 条。

323. 第 44 条借鉴了《关于犯罪收益的洗白、搜查、扣押和没收问题的公约》(《欧洲条约集》第 141 号)的先例，引入该条是在欧洲委员会框架内制定的刑法公约方面的一项创新。修正程序大多被认为是针对程序性和技术性相对较小的修改。起草者认为，可以附加议定书的形式对本公约作出重大修订。

324. 缔约国本身可以根据第 46 条规定的协商程序，审查是否有必要进行修正或制定议定书。在这方面，将定期向犯罪问题委员会通报情况，并要求其采取必要措施，协助缔约国努力修正或补充本公约。

325. 根据第 5 款，所通过的任何修正案只有在所有缔约国通知秘书长已接受的情况下才能生效。这一要求旨在确保公约以统一的方式演进。

争端的解决(第 45 条)

326. 第 45 条第 1 款规定，应随时向犯罪问题委员会通报本公约条款的解释和适用情况。第 2 款规定缔约国有义务寻求和平解决与本公约的解释或适用有关的任何争端。任何解决争端的程序都应经过各当事方同意。该条建议了三种解决争端的可能机制：犯罪问题委员会本身、仲裁庭或国际法院。

缔约国协商(第 46 条)

327. 第 46 条为缔约国提供了一个框架，以便就本公约的执行情况、与计算机或计算机相关犯罪主题有关的重大法律、政策或技术发展的影响、以电子形式收集证据以及补充或修正本公约的可能性进行协商。协商应特别审查在使用和执行本公约过程中出现的问题，包括根据第 40 条和第 42 条作出的声明和保留的影响。

328. 程序是灵活的，如果缔约国愿意，可以决定如何以及何时召开会议。公约起草者认为，这一程序是必要的，以确保本公约的所有缔约国，包括欧洲委员会的非成员国，能够平等参与任何后续机制，同时保留犯罪问题委员会的职权。后者不仅应定期了解缔约国之间正在进行的协商情况，还应为这些协商提供便利，并采取必要的措施协助缔约国努力补充或修正本公约。鉴于有效预防和起诉网络犯罪及其相关隐私问题的需要、对商业活动的潜在影响以及其他相关因素，包括执法部门、非政府组织和私营部门组织在内的有关各方的意见可能会有助于这类协商（另见第 14 款)。

329. 第 3 款规定在本公约生效 3 年后将对其实施情况作出审查，届时可提出适当的修正建议。犯罪问题委员会应当在缔约国的协助下开展审查。

330. 第 4 款指出，除非由欧洲委员会承担费用，否则根据第 46 条第 1 款进行的任何协商将由缔约国自行出资。然而，除了犯罪问题委员会之外，欧洲委员会秘书处也应协助各缔约国根据本公约开展工作。