联合国 A/CONF.213/9

第十二届联合国预防犯罪和刑事司法大会

2010 年 4 月 12 日至 19 日，巴西萨尔瓦多

Distr.: General
22 January 2010
Chinese
Original: English

临时议程*项目 8
在犯罪分子使用科学技术方面以及主管机关利用科学技术打击犯罪包括网络犯罪方面的最新发展情况

在犯罪分子使用科学技术方面以及主管机关利用科学技术打击犯罪包括网络犯罪方面的最新发展情况

秘书处编写的工作文件

一. 导言

1. 网络犯罪位列第十二届联合国预防犯罪和刑事司法大会议程中的重要位置，这说明网络犯罪的重要性从未降低，并且带来了严峻挑战，尽管对该问题的争论已经持续近半个世纪之久。

2. 过去 50 年间，人们已经讨论并制定了各种解决方案，以解决网络犯罪问题。在某种程度上，该问题依然具有挑战性，因为技术在不断发展，并且网络犯罪所采用的方法也在不断改变。

3. 从 1960 至 1980 年代，各国纷纷发现一些新的网络犯罪行为，例如计算机操纵和数据窃取行为，而这些是现有刑事立法通常尚未涉及到的。此时的讨论重点是从法律角度做出回应。[1]

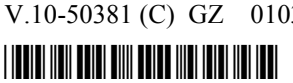
4. 1990 年代图形界面的引入，以及随后迅速增加的因特网用户人数带来了新的挑战。在一个国家合法登载的信息可在全球范围内获取，甚至在登载此类信

---

* A/CONF.213/1。

[1] 见：Susan H.Nycum，《计算机滥用的刑法特征：国家刑法在计算机滥用方面的适用性》（Menlo Park，加利福尼亚，斯坦福研究院，1976 年）和 Ulrich Sieber, *Computerkriminalität und Strafrecht*（Cologne、Karl Heymanns Verlag，1977 年）。

V.10-50381 (C) GZ 010310 010310



息属于违法的国家亦是如此。与在线服务有关的另一个问题是信息交换的速度，事实证明这在调查跨国犯罪过程中是特别具有挑战性的问题。[2]

5. 二十一世纪的前十年，复杂的犯罪新方法（例如“网络钓鱼”[3]和“僵尸网络攻击”[4]）以及技术（例如，网络电话通信和“云计算”）的使用大量出现，给执法人员的调查带来更多困难。

二. 网络犯罪带来的挑战

A. 范围的不确定性

6. 尽管技术不断进步，调查日益加强，但是将信息技术用于非法目的的范围保持稳定，甚至可能有所扩大。一些电子邮件提供商报告称，所有电子邮件中多达 75%至 90%是垃圾邮件。[5]与此类似，其他更加普遍的犯罪行为的公布数字也保持不变或有所增长。例如，因特网监视基金会在其《2008 年度慈善报告》中显示 2006 年至 2008 年间经确认的商业性儿童色情网站数量相当稳定。

7. 虽然统计信息有助于使人们注意到该问题在当前和未来将日趋重要，但是与网络犯罪有关的一个重大挑战是缺乏有关该问题范围以及逮捕、起诉和定罪情况的可靠信息。犯罪统计数字通常不单独列出各种犯罪，同时少数现有的关于网络犯罪影响的统计数字通常不够详细，难以向决策人提供犯罪规模或范围的可靠信息。[6]如果没有这些数据，则难以量化网络犯罪对社会的影响，难以制定解决该问题的策略。[7]

8. 统计信息缺失的一个原因是难以估计网络犯罪分子带来的经济损失规模和犯罪数量。一些消息来源估计网络犯罪每年给美国公司和机构造成的损失[8]价值

---

[2] 数据交换速度加快对网络犯罪调查的影响，见：国际电信联盟，《了解网络犯罪：针对发展中国家的指南》（2009 年，日内瓦）。来源：http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf。

[3] 如国际电信联盟在《了解网络犯罪：指南》（见脚注 2）中所述，“网络钓鱼”是一种使受害人泄露个人信息或秘密信息的行为。“网络钓鱼”一词原指利用电子邮件从大量因特网用户中“钓取”口令和财务数据。“ph”的使用与流行的黑客命名规则有关。

[4] “僵尸网络”是运转着外部控制软件的一组受到感染的计算机。 见 Clay Wilson，“僵尸网络、网络犯罪和网络恐怖主义：脆弱性和国会的政策问题”美国国会研究服务处（CRS）报告 RL 32114，2008 年 1 月 29 日更新，来源：www.fas.org/sgp/crs/terror/RL32114.pdf。

[5] 2009 年，反信息滥用工作组报告称所有电子邮件中 85%至 90%是垃圾邮件（http://www.maawg.org/sites/maawg/files/news/2009_MAAWG-Consumer_Survey-Part1.pdf）。

[6] 美利坚合众国国家审计总署，《网络犯罪：公共实体和私人实体在应对网络威胁方面面临的挑战》，美国审计总署报告 GAO-07-705（华盛顿特区，2007 年 6 月），第 22 页；以及 Ian Walden，《计算机犯罪和数字调查》（牛津大学，牛津大学出版社，2007 年）。

[7] Walden，《计算机犯罪和数字调查》。

[8] 美利坚合众国，联邦调查局，《2005 年美国联邦调查局计算机犯罪普查》，第 10 页。

多达 670 亿美元；然而，在抽样调查结果基础上进行的外推是否合情合理尚且无法确定。[9]对这种方法的批评不仅适用于损失，而且还适用于已确认的犯罪数量。[10]受害人报告网络犯罪的程度也是不确定的。虽然参与打击网络犯罪的当局鼓励受害人报告这些犯罪，但是令人担忧的是，特别是金融部门的受害人（例如银行）不报告发生了这种犯罪，因为他们担心负面宣传可能会损害自身的声誉。[11]如果一家公司宣布黑客已经进入了自己的服务器，那么用户可能会因此失去信心，并且全部成本和后果可能甚至比黑客攻击造成的损失还要严重。此外，受害人可能不相信执法机构能够查明罪犯。然而，如果不对罪犯进行报告和起诉，那么他们可能继续犯罪。

9. 与统计信息有关的另一个难点是反复引用的信息通常并不可靠，或者无法检验。其中一个实例涉及因特网儿童色情的商业特征的统计信息。在数项分析当中，人们通常引述全世界因特网儿童色情每年产生的利润达 25 亿美元。[12]然而，该数字的来源（www.toptenreviews.com）未提供开展该项研究的任何背景资料。鉴于该公司在其网站上表示公司“向您提供所需信息，帮助您明智完成交易，我们在每个种类中推荐最佳产品。通过利用并排对比图表、新闻、文章和影像，我们简化了消费者的购买过程”，但是该数据的可靠性实在令人担忧。在另一个实例中，2006 年，一名华尔街日报[13]新闻记者对儿童色情业每年价值 200 亿美元的观点进行了调查，发现包含年收入信息（30 亿至 200 亿）的两份主文件（美国全国失踪和被剥削儿童中心以及欧洲委员会的两份出版物）提及的机构并未对数字进行确认。

B. 跨国性

10. 网络犯罪在很大程度上具有跨国犯罪的性质。因特网发明之初是一种军用网络，以分散网络结构为基础。由于因特网的基本结构以及全球提供服务的特点，网络犯罪常常也具有国际性。载有非法内容的电子邮件被轻而易举地发至许多国家的接收人，甚至在一些情况下，原发送人和最终接收人处于同一国家，或者发送人或接收人使用的电子邮件服务由位于国外的提供商提供。一些很受欢迎的免费电子邮件服务提供商在全世界拥有数百万名用户，这更加突显了网络犯罪具有的跨国性质。

---

[9] 《了解网络犯罪：指南》（见脚注 2）。

[10] 同上。

[11] Neil Mitchison 和 Robin Urry，“犯罪和滥用电子商业”，IPTS 报告，第 57 卷，2001 年 9 月。

[12] Kim-Kwang Choo、Russel G. Smith 和 Rob McCusker，“技术犯罪的未来发展方向：2007-2009 年”，《研究与公共政策汇编》，第 78 号（2007 年，堪培拉，澳大利亚犯罪学研究所），第 62 页；国际终止儿童色情事业及贩卖协会，《网络空间中的儿童暴力》（2005 年，曼谷），第 54 页；欧洲委员会，《2005 年有组织犯罪情况报告：重点关注经济犯罪的威胁》（2005 年 12 月，斯特拉斯堡），第 41 页。

[13] Carl Bialik，“儿童色情贸易的衡量”，《华尔街日报》，2006 年 4 月 18 日。

11. 跨国因素给调查网络犯罪带来的挑战类似于调查其他跨国犯罪中遇到的困难。根据国家主权的基本原则，未经当地当局批准，无法在外国领土上开展调查，因此各国之间的密切合作在网络犯罪调查中至关重要。另一个重大挑战与调查网络犯罪可用的时间短暂有关。与非法贩毒不同，电子邮件可以在几秒钟内送达，在获得足够带宽的情况下可在几分钟内下载较大的文件，而非法贩毒则需依靠运输工具，并且要几周时间才能到达目的地。

12. 不同国家当局之间及时有效的合作也至关紧要，因为在网络犯罪中，证据常常被自动删除，并且时间十分短暂。旷日持久的正式流程会严重妨碍调查工作。

13. 许多现有的司法协助协议仍然以正式、复杂并且常常十分耗时的流程为基础。因此，建立事件快速反应流程和请求国际合作显得至关重要。

14. 《欧洲委员会网络犯罪公约》第三章载列了建立网络犯罪调查国际合作法律框架的一系列原则。[14]这一章指出了国际合作的日益增加的重要性（第 23-35 条），并提倡使用快速通信工具，包括传真和电子邮件（第 25 条第 3 款）。此外，还呼吁《公约》的缔约方指定一个联络点，一周七天一天 24 小时开放，以响应各国的援助请求（第 35 条）。此外，还可以在加强预防网络犯罪和恐怖主义国际公约草案以及国际电信联盟（国际电联）网络犯罪立法工具箱草案中找到其他方法。

C. 各国法律方法之间的差异

15. 因特网网络结构的一个实际影响是网络犯罪的罪犯无须处于犯罪现场。因此，预防罪犯避险天堂的出现已经成为预防网络犯罪工作的一个重要方面。[15]罪犯会利用避险天堂妨碍调查。一个被人熟知的实例是“爱虫”计算机蠕虫病毒于 2000 年[16]在菲律宾开发出来，据报道感染了全世界数以百万计的电脑。[17]在本地的调查受到妨碍，因为当时恶意开发和传播破坏性软件在菲律宾未加适当定罪。

---

[14] 欧洲委员会，《欧洲条约汇编》，第 185 号。亦见公约“解释报告”。

[15] 联合国大会在其第 55/63 号决议、八国集团在《打击高科技犯罪的原则和行动计划》（于 1997 年 12 月 10 日在华盛顿特区举行的八国集团司法与内政部长会议上通过）（网址 www.justice.gov/criminal/cybercrime/g82004/97Communique.pdf）中分别强调需要铲除将信息技术滥用于犯罪目的罪犯的避险天堂。

[16] 美国审计总署，《至关重要的基础设施的保护：“ILOVEYOU”计算机病毒突显提高警报和协调能力的必要性》，在美国参议院银行业、住房与城市事务委员会金融机构小组委员会所做证词，美国审计总署报告，GAO/T-AIMD-00-181（2000 年 5 月，华盛顿特区）。

[17] “爱虫病毒元凶擒拿在即”英国广播公司新闻，2000 年 5 月 6 日。来源：http://news.bbc.co.uk/2/hi/science/nature/738537.stm。

16. 立法趋同问题高度相关，因为许多国家司法协助制度的基础是双重犯罪原则。根据这一原则，某个违法行为必须在请求协助国家和协助国均视为犯罪。[18]在全球一级的调查通常限于那些在所有受影响国家均定为犯罪的行为。虽然许多犯罪行为在世界任何地方均遭到检举，但是地区性差异起着重要作用。例如，不同国家将不同种类的内容定为犯罪，[19]这意味着能够在一个国家的服务器上合法提供的材料在另一个国家可能被视为非法。[20]

17. 目前使用的计算机和网络技术在全世界基本上都是一样的。除了语言问题和电源适配器不同以外，在亚洲和欧洲出售的计算机系统和手机几乎毫无区别。所以出现的与因特网有关的情况也相似。由于采取标准化过程，在非洲国家使用的协议与在美国使用的一样。标准化使全世界的用户能够通过因特网获得一样的服务。[21]

18. 处理跨国网络犯罪的两种不同方法和不同的法律标准在以下各段予以讨论。

1. 立法的兼容性

19. 处理跨国网络犯罪的跨国性和改进国际合作的一种方法是制定相关法律并使之标准化。近年来，已经有几种区域性方法被采用。

20. 2002 年，英联邦制定了一项关于计算机和计算机犯罪的示范立法，旨在改进英联邦成员国的网络犯罪法律，并加强国际合作。如果不进行这种改进，英联邦国家之间需要不少于 1,272 项双边条约，才能在这方面开展跨境合作。[22]该示范法包含关于刑事实体法、程序法和国际合作的条款。由于示范法集中在某个地区，所以对协调工作的影响仅限于英联邦成员国。

---

[18] 关于网络犯罪调查中的双重犯罪原则问题，见联合国预防和管制计算机犯罪手册（《国际刑事政策评论》，第 43 期和第 44 期：联合国出版物，出售品编号：E.94.IV.5），第 269 页，以及 Stein Schjølberg 和 Amanda Hubbard 题为“统一各国打击网络犯罪的法律方法”的背景文件，第 5 页，该文件在 2005 年 6 月 28 日至 7 月 1 日于日内瓦举行的国际电信联盟网络安全主题会议上宣读。

[19] 对内容进行监管的法律方法不同，这是有关非法内容的某些方面未包括在《网络犯罪公约》中，而在附加议定书中予以处理的原因之一。亦见《了解网络犯罪：指南》，第 2.5 章（见脚注 2）。

[20] 各国针对儿童色情定罪的不同方法，例如，见 Ulrich Sieber, *Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet: eine strafrechtsvergleichende Untersuchung*（Forum Verlag Godesberg，1999 年，波恩）。

[21] 单一技术和单一法律标准的重要性，见：Marco Gercke，“打击网络犯罪的国家、区域和国际性方法”，《国际计算机法律评论》，2008 年，第 7 页。

[22] Richard Bourne，“2002 年英联邦法律部长会议：政策提要”，该文件为英联邦法律部长会议编写，该会议于 2002 年 11 月 18 日至 21 日在圣文森特和格林纳丁斯的金斯敦举行（英联邦研究学院，2002 年，伦敦），第 9 页。

21. 欧洲联盟也努力对 27 个成员国的网络犯罪法律加以协调，例如通过以下方式：欧洲议会和欧洲委员会关于内部市场信息社会服务特别是电子商务的某些法律问题的第 2000/31/EC 号指示；欧洲联盟理事会关于打击非现金支付手段方面的欺诈和伪造的第 2000/413/JHA 号框架决定；欧洲联盟理事会关于打击对儿童性剥削和儿童色情的第 2004/68/JHA 号框架决议；欧洲联盟理事会关于攻击信息系统行为的第 2005/222/JHA 号框架决定；[23]欧洲议会和欧洲联盟理事会关于在提供公共电子通信服务或公共通信网络过程中保留所生成或所处理的数据的第 2006/24/EC 号指示，以及第 2002/58/EC 号修正指示；欧洲联盟理事会修正关于打击恐怖主义的第 2002/475/JHA 号框架决定的第 2008/919/JHA 号框架决定。与大多数其他区域性方法不同，所有成员国必须执行欧洲联盟通过的文书。虽然这些文书行之有效，但是至少到 2010 年初前，欧洲联盟内实现协调一致的主要障碍仍然是刑法领域法律的权力有限。[24]造成方法多样的原因是欧洲联盟协调国家刑法的能力仅限于特殊领域。[25]修正《欧洲联盟条约》和《建立欧洲共同体条约》的《里斯本条约》已经改变这种状况，并且赋予欧洲联盟更大权力，以便将来统一有关计算机犯罪的法律——但是这仅限于 27 个成员国。

22. 欧洲委员会已经编制了三部主要文书以统一网络犯罪法律。最著名的是 1997 年至 2001 年制定的《网络犯罪公约》。该《公约》包含关于刑事实体法、程序法和国际合作方面的条款。截至 2009 年 12 月，已有 46 个国家签署该《公约》，26 个国家批准该《公约》。因为在《公约》的谈判期间，未能就种族主义和散布仇外材料的定罪达成一致，《网络犯罪公约关于宣告利用计算机系统犯下的种族主义或仇外行为为犯罪行为的附加议定书》于 2003 年引入。[26]到 2009 年 12 月，有 34 个国家[27]签署《附加议定书》，其中 15 个国家[28]批准该议定书。2007 年，《欧洲委员会保护儿童免遭性剥削和性虐待公约》[29]开放供签署。该公约中包含将交流儿童色情制品和在知情情况下通过信息和通信技术获取儿童色

[23] 更多信息，见：Marco Gercke，“欧盟关于信息系统攻击的框架决定”，*Computer und Recht*，2005 年，第 468 页及其后；以及《了解网络犯罪：指南》（见脚注 2），第 99 页。

[24] Helmut Satzger，*Internationales und Europäisches Strafrecht*（Baden-Baden, Nomos，2005 年），第 84 页；以及 P.J.G. Kapteyn 和 Pieter Verloren van Themaat，《欧洲共同体法律介绍：<欧洲单一法>生效以后》（Kluwer Law International，1989 年，波士顿）。

[25] 欧洲联盟国家网络犯罪法律：Lorenzo Valeri 等，《欧盟国家的计算机网络滥用法律程序手册》（兰德公司，2006 年，加利福尼亚圣莫尼卡）。

[26] 欧洲委员会，《欧洲条约汇编》，第 189 号。亦见附加议定书“解释报告”。

[27] 阿尔巴尼亚、亚美尼亚、奥地利、比利时、波斯尼亚和黑塞哥维那、加拿大、克罗地亚、塞浦路斯、丹麦、爱沙尼亚、芬兰、法国、德国、希腊、冰岛、拉脱维亚、列支敦士登、立陶宛、卢森堡、马尔他、黑山、荷兰、挪威、波兰、葡萄牙、摩尔多瓦共和国、罗马尼亚、塞尔维亚、斯洛文尼亚、南非、瑞典、瑞士、前南斯拉夫的马其顿共和国和乌克兰。

[28] 阿尔巴尼亚、亚美尼亚、波斯尼亚和黑塞哥维那、克罗地亚、塞浦路斯、丹麦、法国、拉脱维亚、立陶宛、挪威、罗马尼亚、塞尔维亚、斯洛文尼亚、前南斯拉夫的马其顿共和国和乌克兰。

[29] 欧洲委员会，《欧洲条约汇编》，第 201 号。

情制品定罪的具体条款（第 20 条第 1 款(f)项）。截至 2009 年 12 月，已有 38 个国家[30]签署了该《公约》，其中三个国家[31]批准了该《公约》。

23. 此外，加强预防网络犯罪和恐怖主义的国际公约草案是 1999 年美国斯坦福大学主办的一次会议的后续行动，国际电信联盟网络犯罪法律工具箱草案是由美国律师公会的代表及其他专家制定的。

2. 地域化

24. 理论上，技术标准化带来的发展远超过技术和服务的全球化，并且可能使得国内法实现统一。然而，如《网络犯罪公约》的批准情况和《公约附加议定书》的谈判过程所示，国内法原则变化的速度远不及技术发展的速度。这促成了第二次发展：即出现使因特网地域化的方法。

25. 虽然因特网可能不存在边境管制问题，但是仍然有一些方法可以限制某些信息的获取。[32]因此，因特网服务提供商有义务阻止用户进入包含儿童色情的网站，这已经引起各国政府和国际组织的注意。[33]从技术角度来讲，接入服务商通常能够检查用户希望进入的网站是否已被列入黑名单，并阻止用户访问。技术解决办法包括控制域名系统、使用代理服务器以及使用综合各种方法的混合解决办

[30] 阿尔巴尼亚、奥地利、阿塞拜疆、比利时、保加利亚、克罗地亚、塞浦路斯、丹麦、爱沙尼亚、芬兰、法国、格鲁吉亚、德国、希腊、冰岛、爱尔兰、意大利、列支敦士登、立陶宛、卢森堡、摩纳哥、黑山、荷兰、挪威、波兰、葡萄牙、摩尔多瓦共和国、罗马尼亚、圣马力诺、塞尔维亚、斯洛伐克、斯洛文尼亚、西班牙、瑞典、前南斯拉夫的马其顿共和国、土尔其、乌克兰和英国。

[31] 阿尔巴尼亚、丹麦和希腊。

[32] Jonathan Zittrain，“在线拦截的历史”，哈佛法律和技术杂志，第 19 卷，第 2(2006)期，第 253 页。

[33] 过滤义务和方法，见：Ilaria Lonardo，“意大利：服务提供商屏蔽内容的职责”，《国际计算机法律评论》，2007 年，第 89 页及其后；Ulrich Sieber 和 Malaika Nolde，*Sperrverfügungen im Internet: Nationale Rechtdurchsetzung im globalen Cyberspace?*（Berlin、Duncker 和 Humblot，2008 年）；W. Ph. Stol 等，*Filteren van kinderporno op internet: Een verkenning van technieken en reguleringen in binnen- en buitenland*（Boom Juridische Uitgevers，WODC，2008 年，海牙）；Tom Edwards 和 Gareth Griffith，“因特网审查和强制过滤”，*NSW 国会图书馆研究服务部*，E-Brief 5/08，2008 年 11 月；Jonathan Zittrain 和 Benjamin Edelman，“全世界因特网过滤文献汇编”，2003 年 10 月，项目载于：http://cyber.law.harvard.edu/filtering。

法。[34]开放网络促进会报告大约二十四个国家正在采用这种内容控制措施。[35]包括意大利、挪威、瑞典、瑞士和英国在内的几个欧洲国家以及中国、伊朗伊斯兰共和国和泰国等国家采用这种方法。欧盟也正在讨论履行这种义务。[36]伴随这种方法的担忧主要是目前所有技术解决办法均可能被人绕过，并且存在过度阻止用户获取因特网信息的危险。[37]欧洲委员会已经在其部长委员会关于采取措施促进使用因特网过滤器时尊重有关的言论和信息自由的建议中指出了保护基本权利的重要性。

D. 有组织犯罪

26. 虽然计算机犯罪的实施者通常是个人，但是有组织犯罪集团同样也很活跃。这一发展事关重大，因为这使得旨在应对有组织犯罪问题的文书例如《联合国打击跨国有组织犯罪公约》[38]可以适用。

27. 在讨论网络犯罪和有组织犯罪时，有必要区分有组织犯罪集团参与的两个主要种类：传统的有组织犯罪集团利用信息技术以及主要实施网络犯罪的有组织犯罪集团。[39]

28. 没有因特网犯罪活动背景的传统有组织犯罪集团正在利用信息技术，以协调活动并增加犯罪。[40]在这种情况下，信息技术被用于提高有组织犯罪集团在传

---

[34] 技术方面的综述，见：Sieber 和 Nolde, *Sperrverfügungen im Internet*，第 50 页及其后；Stol 等，*Filteren van kinderporno op internet*，第 10 页及其后；Andreas Pfitzmann、Stefan Köpsell 和 Thomas Kriegelstein, *Sperrverfügungen gegen Access-Provider: Technisches Gutachten*，德累斯顿工业大学，来源：www.eco.de/dokumente/20080428_technisches_Gutachten_Sperrvervuegungen.pdf；Richard Clayton、Steven J. Murdoch 和 Robert N. M. Watson，“忽视中国的防火墙长城”，该论文于第六次保护隐私技术讲习班上宣读，2006 年 6 月，剑桥；Lori Brown Ayre，《因特网过滤选项分析：中间报告》，该文件为 InfoPeople Project 编写，2001 年 5 月。

[35] Miklós Haraszti，《因特网管理：欧安组织区域内的自由和监管》的“序言”，C. Möller 和 A. Amouroux 编著（欧洲安全与合作组织，2007 年，维也纳），第 5-6 页。

[36] 欧洲共同体委员会，“关于拟订委员会打击儿童性虐待、性剥削以及儿童色情制品的框架决定，取消第 2004/68/JHA 号框架决定的建议”，文件 COM(2009)135，2009 年 3 月 25 日，布鲁塞尔。

[37] 了解《因特网屏蔽和保障基本自由》的更多信息，见 Cormac Callanan 等，《因特网屏蔽：在民主社会中平衡网络犯罪应对措施》（Aconite Internet Solutions，2009 年 10 月，都柏林），第六章和第七章。

[38] 联合国，《条约汇编》，第 2225 卷，第 39574 号。

[39] Kim-Kwang Raymond Choo，“网络空间的有组织犯罪集团：分类”，《有组织犯罪的趋势》，第 11 卷，第 3 号(2008 年 9 月)，第 270-295 页。在这篇文章中，Choo 表示有三种有组织犯罪集团正在利用信息技术破坏网络控制。

[40] 同上，第 273 页；Eoghan Casey，《数字证据和计算机犯罪：取证科学、计算机和因特网》，第二版（学术出版社，2004 年，伦敦），第 9 页。

统活动领域的效率。这包括开始使用电子通信，例如使有组织犯罪集团能够利用加密技术并且进行匿名通信。此外，因特网可用于打开新的市场，如联合王国的有组织犯罪工作队已经发现的那样，因特网为出售假冒和盗版货物者提供了新的规模更大的市场。[41]

29. 报告指出，传统的有组织犯罪集团有参与高科技犯罪领域的新型犯罪活动的趋势。[42]这包括软件盗版及其他形式的侵犯版权行为。[43]但是其他的网络犯罪领域，例如儿童色情[44]和与身份有关的犯罪也常常与有组织犯罪有关。在执行《有组织犯罪公约》时，以下特点和有组织网络犯罪集团需要纳入考虑之中：

(a) 网络犯罪集团的结构往往更加松散、灵活，这使得集团能够在有限时间内吸收成员；[45]

(b) 网络犯罪集团常常比传统的有组织犯罪集团规模小得多；[46]

(c) 集团成员常常只通过电子形式进行联络，从不见面。

三. 对网络犯罪的回应

30. 国际组织、区域组织、各国政府、执法机构和非政府组织正在通过各种方式打击网络犯罪，包括采取立法、执法和能力建设等手段。

---

[41] 联合王国，有组织犯罪工作组，《2007 年年度报告和威胁评估：北爱尔兰的有组织犯罪》（2007 年），第 34 页。来源：www.octf.gov.uk。

[42] 联合王国，打击严重有组织犯罪局，《联合王国有组织犯罪的威胁评估：2009/10》，第 10 页，来源：www.soca.gov.uk。

[43] 加拿大，加拿大安全情报局，“跨国犯罪活动：全球背景”，Perpectives，2000 年 8 月 17 日，来源：www.csis-scrs.gc.ca/pblctns/prspctvs/200007-eng.asp；Choo，“有组织犯罪集团”。第 273 页（见脚注 40）。

[44] Choo，“有组织犯罪集团”第 281 页；欧洲警察组织，“与贩卖人口有关的虐待儿童问题”，严重犯罪综述，2008 年 1 月，第 2 页；《2005 年有组织犯罪情况报告》，第 8 页；John Carr，《虐待儿童、儿童色情制品和因特网》（NCH，儿童慈善机构，2004 年，伦敦），第 17 页；加拿大，加拿大刑事情报局，《2007 年加拿大有组织犯罪年度报告》（2007 年，渥太华），第 4 页；“2004 年希腊有组织犯罪年度报告”，《有组织犯罪的趋势》，第 9 卷，第 2(2005)号，第 5 页；联合国人权委员会，买卖儿童、儿童卖淫和儿童色情制品问题特别报告员报告（E/CN.4/2005/78），第 8 页。

[45] Choo，“有组织犯罪集团”，第 273 页（见脚注 40）。

[46] Susan W. Brenner，“有组织网络犯罪？网络犯罪可能如何影响犯罪关系的结构”，北卡罗来纳法律和技术杂志，第 4(2002)号，第 27 页。

A. 立法

31. 目前，主要是在国家和区域一级制定网络犯罪法律。与用于数据传输过程的技术标准不同，迄今为止在全球范围内尚未就统一关于网络犯罪的法律作出努力，而数据传输过程的技术标准在全世界都是一致的。

1. 现有文书的覆盖面有限

32. 英联邦、西非国家经济共同体（西非经共体）、欧洲联盟和欧洲委员会已经采纳的区域性解决办法的全球性影响有限，因为这些方法仅适用于各组织的成员国。目前，覆盖面最广的文书是《网络犯罪公约》，该《公约》被公认对于打击网络犯罪至关重要，并且得到了不同国际组织的支持。此外，按照《公约》第37 条规定，非欧洲委员会成员的任何国家也可以加入该《公约》。四个非成员国（加拿大、日本、南非和美国）参加了《公约》的有关谈判，其中三个国家（加拿大、日本和美国）因拥有观察员地位而欧洲委员会联系紧密。截至 2009 年 12 月，有 46 个国家[47]（其中四个是参与了谈判的非成员国）签署了《公约》；迄今为止，26 个国家和一个非欧洲委员会成员国批准了该《公约》。[48]

33. 该《公约》对网络犯罪的影响无法仅仅通过已经签署或批准《公约》的国家数量来衡量。例如，阿根廷、博茨瓦纳、埃及、尼日利亚、巴基斯坦和菲律宾虽然未正式加入《公约》，但已按《公约》制定了本国的部分法律。但是，与全球标准相比，签署和批准国家的数量以及速度当然仍有问题。第一批 30 个国家于 2001 年 11 月 23 日签署了《公约》，随后的九年间仅仅有 16 个国家签署。自 2001 年，没有任何非欧洲委员会成员国加入《公约》，虽然五个国家（智利、哥斯达黎加、多米尼加共和国、墨西哥和菲律宾）被邀请加入。批准《公约》的速度同样缓慢，两个国家（阿尔巴尼亚和克罗地亚）于 2002 年、两个国家（爱沙尼亚和匈牙利）于 2003 年、四个国家（立陶宛、罗马尼亚、斯洛文尼亚和前南斯拉夫的马其顿共和国）于 2004 年、三个国家（保加利亚、塞浦路斯和丹麦）于 2005 年、七个国家（亚美尼亚、波斯尼亚和黑塞哥维那、法国、荷兰、挪威、乌克兰和美国）于 2006 年、三个国家（芬兰、冰岛和拉脱维亚）于 2007 年、两个国家（意大利和斯洛伐克）于 2008 年、三个国家（德国、摩尔多瓦共和国和塞尔维亚）于 2009 年批准《公约》。因为《公约》除得到批准外，

[47] 阿尔巴尼亚、亚美尼亚、奥地利、阿塞拜疆、比利时、波斯尼亚和黑塞哥维那、保加利亚、加拿大、克罗地亚、塞浦路斯、捷克共和国、丹麦、爱沙尼亚、芬兰、法国、格鲁吉亚、德国、希腊、匈牙利、冰岛、爱尔兰、意大利、日本、拉脱维亚、立陶宛、卢森堡、马尔他、黑山、荷兰、挪威、波兰、葡萄牙、摩尔多瓦共和国、罗马尼亚、塞尔维亚、斯洛伐克、斯洛文尼亚、南非、西班牙、瑞典、瑞士、前南斯拉夫的马其顿共和国、乌克兰、联合王国和美国。

[48] 阿尔巴尼亚、亚美尼亚、波斯尼亚和黑塞哥维那、保加利亚、克罗地亚、塞浦路斯、丹麦、爱沙尼亚、芬兰、法国、德国、匈牙利、冰岛、意大利、拉脱维亚、立陶宛、荷兰、挪威、摩尔多瓦共和国、罗马尼亚、塞尔维亚、斯洛伐克、斯洛文尼亚、前南斯拉夫的马其顿共和国、乌克兰和美国。

通常需要加以执行，因此文书的效率依赖于已经批准《公约》的国家是否充分修改国内法律。此外，国内法律是否得到充分修改需要加以证明。

2. 全球性争论

34. 区域框架发挥统一全球相关法律的文书的作用的另一个方面是能使非成员国参与其中。尽管网络犯罪具有跨国特点，但是对世界不同区域的影响有所不同。对于发展中国家来说尤其如此。[49]上文第 32 段中提及的区域性解决办法未能使非成员国广泛参与其中。目前，虽然《网络犯罪公约》的成员数量最多，但是该《公约》仍然对非成员国加入进行限制。《公约》第 37 条规定加入《公约》要求各国与《公约》各缔约国进行磋商，并获得各缔约国的一致同意。此外，关于在未来进行任何修订的争论也仅限于《公约》的缔约国参与（第 44 条）。

35. 经验表明，各国通常不愿批准或加入那些本国未参与制定和谈判过程的公约。不管公约的主题如何，都是如此。

36. 在第十二届联合国犯罪预防和刑事司法大会的所有四次区域筹备会议上，各方呼吁制定一项网络犯罪国际公约。

37. 在非洲、近东、中东和欧洲国家执法机构负责人会议上也发出了这样的呼吁，在这些会议上，对因特网、电子证据收集、立法等开展了讨论。在其他区域召开的会议上，与会者的结论是执法机构和司法机关准备不足，没有充足的能力应对网络犯罪的发展，无法在起诉、准备过程中利用网络技术收集并使用证据。人们普遍认为国内法律未能跟上步伐，需要修改这些法律以支持基于通过网络技术获取的证据对罪犯进行调查、起诉和定罪。各国之间急需建立共同规则并开展合作，从而使当局能够跨管辖范围采取有效行动，将罪犯绳之以法。学术界也呼吁制定国际文书。[50]

3. 对最近趋势做出的回应

38. 网络犯罪在不断变化中。在制定区域性解决办法例如英联邦计算机与计算机犯罪示范立法以及《网络犯罪公约》之时，大规模“僵尸网络攻击”、“网络钓鱼”以及将因特网用于恐怖主义目的或者不为人知，或者不如现在这样影响这么大。因此，具体条款未对这些犯罪加以规定。在第十二届大会区域筹备会议上，讨论了应对这些新情况的需求，特别是将因特网用于恐怖主义目的，从

---

[49] 见，例如，经济合作与发展组织报告，《发展中国家的垃圾邮件问题》（经合组织，2005 年，巴黎），第 4 页。来源：http://www.OECD.org/dataoecd/5/47/34935342.pdf；以及《了解网络犯罪：指南》，第 15 页（见脚注 2）。

[50] Joachim Vogel，“努力制订一项全球打击网络犯罪公约”，在第一次世界刑法会议上宣读的论文，2007 年 11 月 19-23 日，墨西哥，瓜达拉哈拉；Stein Schjølberg 和 Solange Ghernaouti-Hélie，《全球网络安全与网络犯罪协议：网络空间和平与安全倡议》（E-dit，2009 年，奥斯陆）。

通过因特网支付服务进行恐怖主义宣传、通信和融资，到收集与潜在目标有关的信息。反恐怖主义执行工作队已经在几个场合提到这种情况以及可能的法律对策。[51]

39. 虽然对于刑事实体法来说，这种现象常常由涉及系统干扰或与计算机伪造的条款加以管辖，但是适用现有区域文书中所包含的程序性文书则困难重重，特别是因为通过因特网（例如社交网络）提供的技术和服务已经发生了显著变化。窃听网络电话通信、刑事诉讼中可否接受数字证据、调查涉及使用加密技术或匿名通信手段案件的程序都是十分紧迫的问题，但是目前这些问题在区域一级并未得到处理，仅仅在有些情况下在国家一级得到处理。[52]

40. 处理这些问题十分重要，因为传统的调查工具常常无法开展网络犯罪调查。一个实例是通信窃听。最近几十年，各国开发了线路窃听等调查工具，这使他们能够对移动电话和非移动电话通信加以侦听。传统的电话通话通常通过电信提供商进行窃听。执法机构如果希望将相同原则用于网络电话通信，则需要与网络电话服务提供商打交道。然而，如果他们的服务是基于点对点技术，[53]那么服务提供商一般可能无法侦听通信，因为有关数据是在通信各方之间直接进行传递的。[54]因此，除有关的法律文书之外，可能还需要新技术。

41. 开展复杂调查的能力不仅与新的犯罪行为有关，而且还与更加传统形式的网络犯罪例如儿童色情有关。自从 1990 年代中期起，儿童色情的销售者和消费者已经可以使用网络服务，现在比以往使用更加频繁。[55]因特网已经成为交换儿童色情制品的主要媒介。从 1990 年代起人们已经认识到与发觉和调查儿童色情案情有关的问题，这些问题依然存在，在很大程度上是因为罪犯可以利用复杂技术以妨碍调查。例如，一项研究表明，因儿童色情问题的被捕者中有 6%使用加密技术，17%使用口令保护软件，3%使用证据消除软件，2%使用远程存储系统。[56]此外，技术的转变也引起了人们的注意：在因特网诞生之初，通过因特网

---

[51] 见，例如：反恐怖主义执行工作队，“打击将因特网用于恐怖主义目的工作组报告”，2009 年 2 月，来源：www.un.org/terrorism/pdfs/wg6-internet_rev1.pdf。

[52] 了解不同国家应对该问题的方法综述，见：《了解网络犯罪：指南》，第 6 章（见脚注 2）。

[53] 点对点技术使网络中各方能够直接连通，用户不必使用传统的以服务器为基础的集中式结构。

[54] 关于执法机构窃听网络电话通信，见 Steven Bellovin 等，“为执法行动提供通信协助以窃听网络电话对安全造成的影响”，2006 年 6 月 13 日，来源：www.cs.columbia.edu/~smb/papers/CALEAVOIPreport.pdf；Matthew Simon 和 Jill Slay，“网络电话：法鉴计算的影响”，在第四届澳大利亚数字法证会议上发表的论文，2006 年 12 月，澳大利亚佩思。

[55] 美国，众议院，“因特网上的儿童性剥削”（2007 年），第 109 届国会，第 9 页。

[56] Janis Wolak、David Finkelhor 和 Kimberly J. Mitchell，《在与因特网有关犯罪中逮捕的儿童色情制品持有人：全国青少年在线受害研究的结论》（全国失踪与受虐儿童服务中心，2005 年，弗吉尼亚亚历山大），第 9 页。

中继聊天等传统渠道进行的交流占据多数，最近儿童色情制品则通过其他技术例如点对点网络等进行交流。[57]

B. 执法

42. 除依靠法律文书之外，执法在很大程度上依靠是否具有取证软件（以收集证据，记录键盘细节以及解密或恢复已删除文件）和调查管理软件或数据库（例如载有来自已知儿童色情图像的哈希值）等调查工具。近年来，人们已经在几种工具，并将继续开发此类工具。[58]例如，都柏林大学正在开展名为“用于数字取证和入侵分析的自动事件重建”的研究项目（信息来自 http://cci.ucd.ie/?q=node/33），2009 年 12 月，美国引入了名为 PhotoDNA 的儿童色情追踪新技术。与开发此类工具有关的一个主要问题仍是开发商之间需要进行协调，从而避免重复。类似地，联络点网络（例如八国集团和刑警组织的联络点网络，以及与《网络犯罪公约》有关的网络）的工作也需要加以协调。

C. 能力建设

43. 网络犯罪不仅是发达国家，也是发展中国家面临的问题。发展门户基金会的数据显示，2005 年，发展中国家的因特网用户数量超过工业化国家。[59]西非经共体最近通过了一项关于网络犯罪的指示，东非共同体也提出了一个网络法律框架草案，这些都是积极的信号。进一步提供支持可以帮助执法机构为对付此类犯罪行为做好准备，因为这种犯罪可能会在发展中国家更多用户可以使用宽带接入时出现。联合国大会题为“加强联合国犯罪预防和刑事司法方案，特别是其技术合作能力”的第 64/179 号决议提请注意秘书长确定的新出现的政策问题（A/64/123），即海盗活动、网络犯罪、儿童性剥削和城市犯罪问题，并请联合国毒品和犯罪问题办公室在其任务范围内探讨处理这些问题的方式和方法。

---

[57] 美国，国家审计总署，《文件共享计划，儿童色情制品容易通过点对点网络获取》，在众议院政府改革委员会所做证词，美国审计总署报告 GAO-03-537T（2003 年 3 月，华盛顿特区）；Gretchen Ruethling，“国际在线儿童色情团伙中 27 人被起诉”，《纽约时报》，2006 年 3 月 16 日；Choo，“有组织犯罪集团”，第 282 页（见脚注 40）；联合王国，斯托克波特保护儿童委员会，《在斯托克波特保护儿童：政策和实践手册》（2008 年 5 月），第 299 页，来源：http://www.safeguardingchildreninstockport.org.uk/documents/Section%2000%20-%20Preface%20and%20contents.pdf。

[58] 见，例如，都柏林大学开展的称作“用于数字法证和入侵分析的自动事件重建”的研究项目（信息来源：htt://cci.ucd.ie/?q=node/33）。

[59] 信息来源：http://topics.developmentgateway.org/special/informationsociety。

D. 培训

44. 由于调查网络犯罪和起诉网络犯罪分子带来了独特的挑战，因此向执法人员、检察官和法官提供培训十分重要。如 2009 年 10 月 6 日和 7 日在维也纳举行的毒品和犯罪问题办公室网络犯罪专家组会议所强调，处理该问题的大多数国际和区域组织已经采取措施对参与网络犯罪调查的专家进行培训并编写培训教材。[60]

四. 结论和建议

45. 对于所有相关机构来说，调查网络犯罪和起诉网络犯罪分子十分具有挑战性。鉴于该问题十分复杂，并且技术不断发展，为所有相关部门提供持续不断、日益扩大的培训仍然是一个主要问题。2009 年毒品和犯罪问题办公室网络犯罪专家组会议的讨论表明，制度化的能力建设和长期可持续性是衡量未来举措成功与否的两个主要因素。

46. 为了消除避险天堂和改善国际合作，应当注意弥补现有法律的不足，促进法律的一致性、连贯性和兼容性。鉴于统一法律和利用第十二届联合国犯罪预防和刑事司法大会各次筹备会议的成果十分重要，制定一项打击网络犯罪的国际公约应当得到仔细和适当的考虑。

47. 同时，作为犯罪预防和刑事司法事务方面制定标准的机构，毒品和犯罪问题办公室将提供一个以发展中国家为重点的多边平台。它将通过综合打击犯罪活动方面经过证明的法律、执法和技术专门知识，以及已经参与打击网络犯罪的那些主要伙伴的完善的具体专门知识，继续采取以伙伴关系为基础的全面的多学科方法。毒品和犯罪问题办公室将致力于汇总这些工具并召集专家和与专家合作，包括私营部门的工具和专家（特别是因特网服务提供商），以便在某个国家或区域解决网络犯罪问题。首要任务是向需要的成员国提供技术援助，以便解决能力和专门知识不足的问题，并确保应对计算机犯罪工作的长期可持续性。

48. 特别是，毒品和犯罪问题办公室将致力于采取以下措施：帮助成员国通过相关法律，从而有效调查计算机犯罪和起诉罪犯；通过培训、修订/制定对计算机犯罪进行调查和起诉的培训教材等方式，提高法官、检察官和执法人员有关网络犯罪问题的业务和技术知识；对执法机关进行培训，从而有效利用国际合作机制打击网络犯罪；提高民间社会的认识，并激励决策者共同努力预防和解

[60] 例如，亚太经合组织组织过几次关于网络犯罪的培训活动，包括网络犯罪方面的法律；英联邦组织过法律和技术培训课程；欧洲委员会在世界各地帮助开展培训，并为法官编写了专门的培训教材；欧洲联盟提供支助为成员国执法机构制定网络犯罪培训课程，并编写教材，此外，还在欧洲和以外地区组织过几期培训课程；刑警组织为执法机构组织过几期培训课程，并编写了培训教材；国际电联以所有联合国语文编写了网络犯罪培训教材，并在几个区域活动期间提供一般培训，向法官提供专门培训。

决网络犯罪；确定和宣传预防和打击网络犯罪方面的良好做法，并促进该领域的公私伙伴关系。