联合国 E/CN.15/2011/19

经济及社会理事会

Distr.: General
2 March 2011
Chinese
Original: English

预防犯罪和刑事司法委员会
第二十届会议
2011 年 4 月 11 日至 15 日，维也纳
临时议程*项目 6
世界犯罪趋势和预防犯罪和刑事司法领域
新出现的问题及应对措施

不限成员名额政府间专家组关于网上犯罪问题以及会员国、国际社会和私营部门就此采取的对策的综合研究报告

秘书处的说明

1. 根据大会第 65/230 号决议第 9 段，委员会按照《关于应对全球挑战的综合战略：预防犯罪和刑事司法系统及其在不断变化的世界中的发展的萨尔瓦多宣言》（大会第 65/230 号决议，附件）第 42 段设立的不限成员名额政府间专家组自 2011 年 1 月 17 日至 21 日在维也纳举行了会议。专家组依照其任务授权审议了下述问题：

> 综合研究网上犯罪问题以及会员国、国际社会和私营部门就此采取的对策，包括就国家立法、最佳做法、技术援助和国际合作开展信息交流，以期审查各种备选方案，加强现有的并提出新的国家和国际应对网上犯罪的法律和其他对策。

2. 大会第 65/230 号决议第 11 段请不限成员名额政府间专家组向委员会报告工作进展情况。因此，专家组审查并通过了随附的题为“收集专题，供在关于网上犯罪的影响和对策的综合研究中审议”（附件一）和“研究方法”（附件二）的结果文件，将其转交委员会第二十届会议审议。

* E/CN.15/2010/1。

V.11-80325 (C) GX 250211 250211

3. 在通过“收集专题供在关于网上犯罪的影响和对策的综合研究中审议”（附件一）后，哥伦比亚代表做出下述发言，并请将发言列入不限成员名额政府间专家组的报告中：

1. 在不限成员名额政府间专家组会议期间，许多代表团对为恐怖主义目的频繁滥用新信息和通信技术问题表示了关切。在这方面，秘书处一名代表介绍了毒品和犯罪问题办公室围绕此问题，特别是滥用互联网问题开展的工作。考虑到关于网上犯罪问题的研究必须充分而全面，需对表示的所有关切加以解决。由此，研究应当涵盖恐怖主义和网上犯罪之间关系的方方面面，这变得至关紧要。恐怖主义组织通过一系列不同方式利用这些技术，例如：

(a) 为宣传目的；

(b) 用来收集信息；

(c) 作为一个培训工具；

(d) 用来组织非法活动；

(e) 为招募和煽动目的而传播信息；

(f) 为安全存储和传送信息目的；

(g) 用来亲自攻击计算机网络。

2. 为了达成共识，哥伦比亚同意阿根廷代表团关于此主题事项的建议，但请不限成员名额政府间专家组第一次会议报告注意下列各项：

(a) 关于收集专题供在关于网上犯罪的影响和对策的综合研究中审议（附件一）第 12 段，哥伦比亚认为，所提及的已刑事定罪的罪行盘点包括恐怖主义这个主题事项；

(b) 关于该文件第 18 段前的标题，哥伦比亚认为，网上犯罪的挑战也包括恐怖主义这个主题事项；

(c) 哥伦比亚还表示希望此项研究将考虑到该文件第 25 段所提问题，即恐怖分子可能滥用能用于实施网上犯罪的工具。

附件一

收集专题，供在关于网上犯罪的影响和对策的综合研究中审议

一. 导言

1. 在 2010 年举行的第十二届联合国预防犯罪和刑事司法大会期间，成员国对网上犯罪问题作了略有深度的讨论，并决定请预防犯罪和刑事司法委员会召集不限成员名额的政府间专家组，对网上犯罪问题及对策进行综合研究。预防犯罪和刑事司法委员会采纳了这一建议，随后经济及社会理事会第 2010/18 号决议和大会第 65/230 号决议也采纳了该建议。

2. 按照《关于应对全球挑战的综合战略：预防犯罪和刑事司法系统及其在不断变化的世界中的发展的萨尔瓦多宣言》第 42 段，该项综合研究将审查：

> 网上犯罪问题以及会员国、国际社会和私营部门就此采取的对策，包括就国家立法、最佳做法、技术援助和国际合作开展信息交流，以期审查各种备选方案，加强现有的并提出新的国家和国际应对网上犯罪的法律和其他对策。

3. 因此，《萨尔瓦多宣言》第 42 段不仅指出了这项研究应当调查的各实质方面（网上犯罪问题、国家立法、最佳做法、技术援助和国际合作），还有出发角度（会员国、国际社会和私营部门的对策）和侧重点（审查各种备选方案，加强现有对策并提出新的国家和国际打击网上犯罪的法律和其他对策）。

4. 为了拟订该项研究的结构，已将这三个方面（实质方面、角度和侧重点）转化为符合《宣言》要求的 12 个专题。这 12 个专题组成以下类别。

网上犯罪问题（专题 1-3）

5. 《萨尔瓦多宣言》强调，该项研究应当对网上犯罪问题进行调查。为了全面应对网上犯罪所造成的问题，确定了三个关键领域供进行详细分析：

(a) 网上犯罪现象（专题 1）；

(b) 统计信息（专题 2）；

(c) 网上犯罪的挑战（专题 3）。

应对网上犯罪的法律对策（专题 4-9）

6. 《萨尔瓦多宣言》呼吁研究关于应对网上犯罪的法律对策，包括就国家立法、良好做法和国际合作交流信息。除立法统一工作的一般方面外，还确定了法律对策的具体领域：

(a) 共同的立法办法（专题 4）；

(b) 刑事定罪（专题 5）；

(c) 程序权力（专题 6）；

(d) 国际合作（专题 7）；

(e) 保障和条件，包括保护基本人权和个人资料；

(f) 尊重各国主权平等和不干涉他国事务原则；

(g) 电子证据（专题 8）；

(h) 服务提供方和私营部门的作用和责任（专题 9）。

预防犯罪和刑事司法能力及应对网上犯罪的其他对策（专题 10）

7. 《萨尔瓦多宣言》不仅提及了研究关于应对网上犯罪的法律对策，还提及了范围更广的应对网上犯罪的其他类型对策。

国际组织（专题 11）

8. 《萨尔瓦多宣言》呼吁对会员国、国际社会和私营部门采取的对策进行分析。尽管与国际社会采取的法律对策有关的事项包含在法律对策标题下，但就国际社会的对策单列一个标题将便利分析更一般的方面，如区域办法和国际办法之间的关系。

技术援助（专题 12）

9. 鉴于网上犯罪对发展中国家的影响以及有必要采取统一而协调的办法打击网上犯罪，将在综合研究中作为一个具体领域述及技术援助。

二. 各专题详细概览

专题 1. 网上犯罪现象

背景

10. 计算机犯罪和较为确切的网上犯罪这两个术语用于描述一种具体类别的犯罪行为。与这类犯罪行为有关的挑战包括所涵盖的罪行范围广泛和犯罪手法不断翻新。

计算机犯罪和网上犯罪的发展

11. 在 1960 年代，采用了使用晶体管的计算机系统，计算机变得更为普及，[1]对犯罪行为的刑事定罪侧重于对计算机系统及所存数据的物理破坏。[2]1970 年代，针对计算机系统实施的传统的财产犯罪[3]逐渐为新型犯罪所取代，[4]其中包括非法使用计算机系统[5]和篡改[6]电子数据。[7]随着人工交易转变为由计算机操作的交易，产生了另一种新型犯罪：与计算机有关的欺诈。[8]1980 年代，个人计算机日益普遍，各种关键基础设施首次依赖于计算机技术。[9]计算机系统普及的副作用之一是人们对软件的兴趣增加，开始出现了初步形式的软件盗版和与专利有关的犯罪。[10]此外，由于计算机系统开始相互联接，犯罪分子不必亲临犯罪现场便能进入计算机系统。[11]1990 年代开始采用图形界面（万维网）之后，互联网

---

[1] 关于相关挑战，见 R. T. Slivka and J. W. Darrow, “Methods and problems in computer security”, *Rutgers Journal of Computers and the Law*, vol. 5, No. 2 (1976), pp. 217-269。

[2] McLaughlin, “Computer crime: the Ribicoff Amendment to United States Code, Title 18”, *Criminal Justice Journal*, vol. 2, 1978, pp. 217 ff。

[3] Gemignani, “Computer crime: the law in ‘80”, *Indiana Law Review*, vol. 13, 1980, p. 681。

[4] McLaughlin, “Computer crime: the Ribicoff Amendment”。

[5] Freed, Materials and Cases on Computer and Law (n.p., 1971), p. 65。

[6] Bequai, “The electronic criminals: how and why computer crime pays”, *Barrister*, vol. 4, 1977, pp. 8 ff。

[7] Criminological Aspects of Economic Crime: Proceedings of the 12th European Conference of Directors of Criminological Research Institutes (November 1976), vol. XV, Collected Studies in Criminological Research (Strasbourg, Council of Europe, 1977), pp. 225 ff.; United States of America, Staff Study of Computer Security in Federal Programs: Committee on Government Operations — United States Senate (Washington, D.C., United States Government Printing Office, 1977)。

[8] McLaughlin, “Computer crime: the Ribicoff Amendment” （见上文脚注 2）; Bequai, “Computer crime: a growing and serious problem”, *Police Law Quarterly*, vol. 6, 1977, p. 22。

[9] E. A. Glynn, “Computer abuse: the emerging crime and the need for legislation”, *Fordham Urban Law Journal*, vol. 12, No. 1 (1983-1984), p. 73。

[10] BloomBecker, “The trial of computer crime”, *Jurimetrics Journal*, vol. 21, 1981, p. 428; W. Schmidt, “Legal proprietary interests in computer programs: the American experience”, *Jurimetrics Journal*, vol. 21, 1981, pp. 345 ff.; M. Dunning, “Some aspects of theft of computer software”, *Auckland University Law Review*, vol. 4, No. 3 (1982), pp. 273 ff.; Weiss, “Pirates and prizes: the difficulties of protecting computer software”, *Western State University Law Review*, vol. 11, 1983, pp. 1 ff.; R. P. Bigelow, “The challenge of computer law”, *Western England Law Review*, vol. 7, No. 3 (1985), p. 401; G. Thackeray, “Computer-related crimes: an outline”, *Jurimetrics Journal*, vol. 25, No. 3 (1985), pp. 300 ff。

[11] Yee, “Juvenile computer crime: hacking — criminal and civil liability”, *Comm/Ent Law Journal*, vol. 7, 1984, pp. 336 ff.; “Who is calling your computer next? Hacker!”, *Criminal Justice Journal*, vol. 8, 1985, pp. 89 ff.; A. M. Wagner, “The challenge of computer-crime legislation: how should New York respond?”, *Buffalo Law Review*, vol. 33, No. 3 (1984), pp. 777 ff。

用户人数迅速增加，随之出现了新的犯罪方法。例如，虐童材料的传播从书籍和录像带的实物交换转为通过网站和互联网服务在线传播。[12]计算机犯罪一般是在某一地实施的犯罪，而互联网使电子犯罪转变为跨国犯罪。在二十一世纪的第一个十年中，最突出的是各种极其复杂的犯罪新手法，如“网络钓鱼”、[13]“僵尸”[14]攻击，以及新出现的“互联网协议语音（网络电话）通信”[15]和“云计算”[16]等技术的使用，这给执法造成了很多难题。

研究范围

12. 对此专题的研究将侧重于网上犯罪现象本身，并不涵盖对网上犯罪采取的对策：

(a) 网上犯罪现象分析，同时考虑到现行法律框架所涵盖的行为；

(b) 已刑事定罪的罪行盘点；

(c) 尚未刑事定罪的行为盘点；

(d) 组合犯罪（如“网络钓鱼”）和未来趋势概览；

(e) 相关案例盘点；

(f) 网上犯罪定义的重要性探讨。

---

[12] “Child pornography”, 为 2001 年 12 月 12 日至 20 日在日本横滨举行的第二届禁止对儿童商业色情剥削世界大会编拟的主题文件, p. 17; “Sexual exploitation of children over the Internet”, report prepared for the use of the Committee on Energy and Commerce, United States, House of Representatives, 109th Congress, January 2007, p. 9。

[13] “网络钓鱼”一词系指为使受害者透露个人/秘密信息而进行的行动。该词原指使用电子邮件从大海一样的互联网用户中“钓取”密码和金融数据。英文词“phishing”中使用“ph”与黑客中流行的命名传统有关。更多信息见国际电信联盟, *Understanding Cybercrime: A Guide for Developing Countries* (Geneva, 2009), chap. 2.8.4。

[14] “僵尸”是简称，系指一组在外部控制下运行软件、安全受到危害的计算机。更多详细信息见 Clay Wilson, “Botnets, cybercrime, and cyberterrorism: vulnerabilities and policy issues for congress”, Congressional Research Service Report RL32114, 2007, p. 4。

[15] M. Simon and J. Slay, “Voice over IP: forensic computing implications”, 为 2006 年 12 月 4 日在珀思举行的第四次澳大利亚数字法医学会议编拟的文件。

[16] Cristos Velasco San Martin, “Jurisdictional aspects of cloud computing”, 提交 2009 年 3 月 10 日至 11 日在斯特拉斯堡举行的欧洲委员会“章鱼接口会议：合作打击网上犯罪”的文件；M. Gercke, “Die Auswirkungen von Cloud Storage auf die Tätigkeit der Strafverfolgungsbehörden”, in *Inside the Cloud: Neue Herausforderungen für das Informationsrecht*, J. Taeger and A. Wiebe, eds., Oldenburger Tagungsbände (Edewecht, Germany, Oldenburger Verlag für Wirtschaft, Informatik und Recht, 2009), pp. 499 ff。

专题 2. 统计信息

背景

13. 犯罪统计数据为政策制定者和学者的讨论和决策提供依据。[17]此外，执法机关若对网上犯罪的实际程度掌握准确的信息，便能够改进打击网上犯罪的策略，遏制潜在的攻击并确保颁布更适当有效的法律。

网上犯罪统计数据的现状

14. 关于犯罪程度的信息通常取自犯罪统计数据和调查。[18]若使用这两类来源制定政策建议，便会出现一些难题。首先，犯罪统计数据一般是在国家一级编制的，不会反映这一事项在国际上的程度如何。虽然理论上可以将不同国家提供的数据合并起来，但这种办法不会产生可靠的信息，因为各国的立法和记录做法各不相同。[19]要合并和比较各国的犯罪统计数据，需要有一定程度的可比性，[20]而在网上犯罪方面却缺乏这种可比性。网上犯罪行为即使已经记录在案，也不一定会单独列出。[21]

15. 其次，统计数据所能反映的只有已经侦破和报案的犯罪。[22]特别是在网上犯罪方面，恐怕有大量案件并未报案。[23]企业可能担心负面消息公开后会破坏其声

---

17 P. A. Collier and B. J. Spaul, “Problems in policing computer crime”, *Policing and Society*, vol. 2, No. 4 (1992), p. 308。

18 关于犯罪统计数据日益突出的重要性，见 D. A. Osborne and S. C. Wernicke, *Introduction to Crime Analysis: Basic Resources for Criminal Justice Practice* (Binghamton, New York, Haworth Press, 2003), pp. 1 ff。

19 在这方面见 *Overcoming Barriers to Trust in Crimes Statistics: England and Wales*, Monitoring Report No. 5, interim report (London, United Kingdom Statistics Authority, December 2009), p. 9。可查阅：www.statisticsauthority.gov.uk。

20 A. Alvazzi del Frate, “Crime and criminal justice statistics challenges”, in *International Statistics on Crime and Justice*, S. Harrendorf、M. Heiskanen and S. Malby, eds., HEUNI Publication Series, No. 64 (Helsinki, European Institute for Crime Prevention and Control, affiliated with the United Nations, 2010), p. 168。可查阅：www.unodc.org/documents/data-and-analysis/Crime-statistics/International_Statistics_on_Crime_and_Justice.pdf。

21 “Computer crime”, Parliamentary Office of Science and Technology, *Postnote*, No. 271, October 2006, p. 3。

22 关于相关挑战，见 M. E. Kabay, “Understanding studies and surveys of computer crime”, June 2009。可查阅：www.mekabay.com/methodology/crime_stats_methods.pdf。

23 美国联邦调查局已请各公司不要对网络钓鱼攻击和公司信息技术系统受到的攻击保持缄默，而要向当局通报，使当局更多了解互联网上的犯罪活动。“我们的问题是，一些公司对不良声誉的担忧显然大于对黑客攻击成功后所造成的后果的担忧，”联邦调查局纽约办事处代理主任 Mark Mershon 解释说。见 “FBI wants to know more about hacker attacks”, *Heise News*, 27 October 2006。可查阅：www.h-online.com/security/news/item/FBI-wants-to-know-more-about-hacker-attacks-731717.html。另见“Comments on computer crime: Senate Bill S. 240”, *Memphis State University Law Review*, 1980, p. 660。

誉。[24]如果一家公司宣称有黑客侵入了自己的服务器，可能会失去客户的信任，这样付出的代价可能比黑客攻击造成的损失更大。但是，如果对犯罪行为不报案不起诉，犯罪分子可能还会继续犯罪。受害者可能不相信执法机关有能力查明犯罪分子，[25]也可能认为报案没有意义。[26]由于网上犯罪攻击的自动化，网上犯罪分子得以制订一种战略，以小额金钱为目标进行多次攻击，从中获取巨额利润（预付款诈骗案的情形即是如此），[27]因此对未举报的犯罪可能有很大影响。受害人如果只有小额损失，可能宁可不走向执法机关报案这种费时的程序。在实际中，所报案件牵涉的费用通常极高。[28]

研究范围

16. 对此专题的研究将包括以下内容：

(a) 收集关于网上犯罪普遍程度和严重程度的最新统计数据、调查和分析；

(b) 评价统计数据对于政策建议的价值；

(c) 确定在收集准确统计数据方面可能存在的障碍；

(d) 确定有哪些国家专门收集关于网上犯罪行为的统计数据；

(e) 评价收集网上犯罪统计信息的必要性和益处；

(f) 审查可用于收集这类信息的可能技术；

(g) 讨论统计信息中央托管机构的可能模式。

---

[24] 见 N. Mitchison and R. Urry, “Crime and abuse in e-business”, in *IPTS Report*, No. 57, 2001, pp. 18-22; Collier and Spaul, “Problems in policing computer crime” (见上文脚注 17), p. 310。

[25] 见 Collier and Spaul, “Problems in policing computer crime” (见上文脚注 17), p. 310; R. G. Smith, “Investigating cybercrime: barriers and solutions”, paper prepared for the Association of Certified Fraud Examiners, Pacific Rim Fraud Conference, Sydney, 11 September 2003, p.2。可查阅：www.aic.gov.au/about_aic/research_programs/staff/smith_russell.aspx。

[26] 实际上，报纸和电视台对成功的互联网调查的报道仅限于轰动的案件，如通过恢复恋童癖嫌疑人经过篡改的照片查明其身份的案件。关于该案件和报道情况的更多信息，见 “Interpol in appeal to find paedophile suspect”, *New York Times*, 9 October 2007。可查阅：www.nytimes.com/2007/10/09/world/europe/09briefs-pedophile.html?_r=1&oref=slogin；以及国际刑事警察组织（刑警组织）网站上提供的信息，可查阅：www.interpol.int/Public/THB/vico/Default.asp。

[27] 见 United Kingdom, Serious Organised Crime Agency, “International crackdown on mass marketing fraud revealed”, 2007。

[28] 在国家白领犯罪中心发表的 2006 NW3C Internet Crime Report 中，所报案件的美元损失总额中只有 1.7%与尼日利亚信件诈骗有关，但所报案件的平均损失为 5,100 美元。所报犯罪行为的数量很少，但造成的平均损失很高。

专题 3. 网上犯罪的挑战

背景

17. 目前十分注重制定战略应对网上犯罪的各种具体挑战。这一发展情况的原因有二：首先，调查网上犯罪需要一些新工具，因此需要进行大量研究，其次，涉及网络技术的犯罪的调查工作有一些独特的挑战，是传统的调查工作不会遇到的。

打击网上犯罪和相关威胁面临的挑战

18. 网上犯罪在技术和法律上的独特挑战很多。犯罪分子可以通过利用不要求深入的技术知识的工具实施网上犯罪，如为找寻敞开的端口或破解密码保护而设计的软件工具，[29]这只是其中的一个例子。[30]还有一个挑战是，很难追踪犯罪分子。尽管用户在使用互联网服务时会留下很多痕迹，但犯罪分子可以通过隐蔽身份而阻碍调查工作。例如，如果犯罪分子使用公共互联网终端或开放式无线网络实施犯罪，他们的身份便很难查到。网上犯罪调查工作中一个较为普遍的挑战是因为，实际上，从技术角度看，互联网提供的可为执法工作所用的控制工具极少。互联网最初是作为军事网络设计的，[31]其基础是一种分散自立的网络架构，即使是在网络的组成部分受到攻击时也力求保持其主要功能完好。这种分散自立方式的原始设计并不方便犯罪调查或防止从网络内部发起的攻击，调查措施需要使用控制手段，因而在这一环境下构成了独特的挑战。[32]

研究范围

19. 对此专题的研究将包括以下内容：

(a) 与打击网上犯罪有关的各种挑战全面盘点；

(b) 应对这些挑战的最佳技术和法律做法归纳。

---

[29] “Websense”, *Security Trends Report 2004*, p. 11; United States of America, General Accounting Office, *Information Security: Computer Controls over Key Treasury Internet Payment System*, GAO-03-837 (Washington, D.C., 2003), p. 3; U. Sieber, “The threat of cybercrime”, in *Organised Crime in Europe: The Threat of Cybercrime — Situation Report 2004* (Strasbourg, Council of Europe Publishing, 2005), p. 143。

[30] K. Ealy, “A new evolution in hack attacks: a general overview of types, methods, tools, and prevention”, SANS Institute, 2003, p. 9。

[31] 关于互联网简史，包括其军事起源，见 B. Leiner 等, “A brief history of the Internet”, 可查阅：www.isoc.org/internet/history/brief.shtml。

[32] H. F. Lipson, *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues* (Pittsburgh, Carnegie Mellon University, Software Engineering Institute, 2002)。

专题 4. 共同的立法办法

背景

20. 在过去 20 年间，各国和区域组织为应对网上犯罪问题制定了立法和法律框架。尽管已经形成了某些共同趋势，但各国立法之间仍然存在很大差异。

国家和区域差异

21. 各国和区域在立法框架方面存在差异的一个原因是，正如打击垃圾电子邮件的工作所表明的那样，网上犯罪的影响并不是普遍相同的。[33]在发展中国家，由于资源稀有昂贵，垃圾电子邮件问题比西方国家严重。[34]在非法内容方面，一些国家和区域可能会将散布某种材料的行为定为刑事犯罪，而这类材料在另一些国家可能会被视为受言论自由原则[35]保护的。[36]

22. 由于网上犯罪是一种真正的跨国犯罪，[37]调查和起诉要取得成功，国际合作是必不可少的。[38]有效的国际合作需要达成一定程度的共识和采取共同的立法办法，以防止产生安全庇护所。[39]

---

[33] Understanding Cybercrime: A Guide for Developing Countries (见上文脚注 13), chap. 2.6.7。

[34] 见经济合作与发展组织, “Spam issues in developing countries”, document DSTI/CP/ICCP/SPAM(2005)6/FINAL, 26 May 2005, p. 4。可查阅：www.oecd.org/dataoecd/5/47/34935342.pdf。

[35] 关于言论自由原则，见 T. L. Tedford and D. A. Herbeck, *Freedom of Speech in the United States*, 5th ed. (State College, Pennsylvania, Strata, 2005); E. Barendt, *Freedom of Speech* (Oxford, Oxford University Press, 2007); C. E. Baker; *Human Liberty and Freedom of Speech* (New York, Oxford University Press, 1989); J. W. Emord, *Freedom, Technology and the First Amendment* (San Francisco, Pacific Research Institute for Public Policy, 1991); 关于这一原则对于电子监视的重要性，见 C. Woo and M. So, “The case for Magic Lantern: September 11 Highlights — the need for increasing surveillance”, *Harvard Journal of Law and Technology*, vol. 15, No. 2 (2002), pp. 530 ff.; M. Chesterman, *Freedom of Speech in Australian Law: A Delicate Plant* (Aldershot, Hampshire, Ashgate, 2000); E. Volokh, “Freedom of speech, religious harassment law, and religious accommodation law”, *Loyola University Chicago Law Journal*, vol. 33, 2001, pp. 57 ff.,可查阅：www.law.ucla.edu/volokh/harass/religion.pdf; H. Cohen, “Freedom of speech and press: exceptions to the First Amendment”, Congressional Research Service Report 95-815, 2009, 可查阅：www.fas.org/sgp/crs/misc/95-815.pdf。

[36] 人们对于表达意见自由的关切（如对美国《宪法》的第一次增订）解释了为什么某些种族主义行为在《网上犯罪公约》（欧洲委员会，《欧洲条约汇编》，第 185 号）中没有定为非法，而关于将利用计算机系统犯下的种族主义和仇外行为定为刑事犯罪的《网上犯罪公约第一附加议定书》（欧洲委员会，《欧洲条约汇编》，第 189 号）将其定为刑事犯罪。另见《附加议定书》说明性报告，可查阅：http://conventions.coe.int/Treaty/en/Reports/Html/185.htm。

[37] 关于跨国攻击在破坏性最大的网上攻击中所占部分的大小，见 A. D. Sofaer and S. E. Goodman, “Cyber crime and security: the transnational dimension”, in *The Transnational*

23. 对此专题的研究将包括以下内容：

(a) 对采取共同办法制定网上犯罪法律的工作进行分析；

(b) 与采取共同办法制定网上犯罪法律的工作有关的其他要素，包括已认识到的行为严重程度和人权规范的影响；

(c) 汇编各国执行区域组织法律标准的所有办法，并分析确定哪些技术可有助于确保这些办法保持协调一致；

(d) 分析网上犯罪立法上的差异对国际合作有多大程度的影响。

专题 5. 刑事定罪

背景

24. 要有效调查和起诉网上犯罪，如果某些行为尚未列入现行法律，便需要确立新罪名。适当法律的存在不仅与国内调查工作有关，而且如上所述，还影响到国际合作。

实体刑法

25. 为应对网上犯罪问题而制定的综合性区域框架大多载有一整套实体刑法规定，其目的是缩小国家立法方面的差距。这些框架中的标准规定包括将非法侵入、非法截取、非法干扰数据、非法干扰系统、与计算机有关的诈骗和与计算机有关的伪造等行为定为刑事犯罪。而一些国家框架则更进一步，将制造和传播可用于实施网上犯罪或用于恐怖主义的工具（如软件或硬件）、与虐童材料有关的行为、为色情目的诱骗儿童行为或煽仇言论等罪行定为刑事犯罪。

Dimension of Cyber Crime and Terrorism, A. D. Sofaer and S. E. Goodman, eds., Hoover National Security Forum Series (Stanford, California, Hoover Institution Press, 2001), p. 7。可查阅：http://media.hoover.org/documents/0817999825_1.pdf。

[38] 关于在打击网上犯罪方面进行国际合作的必要性，见 T. L. Putnam and D. D. Elliott, “International responses to cyber crime”, in *Transnational Dimension of Cyber Crime and Terrorism*, A. D. Sofaer and S. E. Goodman, eds., Hoover National Security Forum Series (Stanford, California, Hoover Institution Press, 2001), pp. 35 ff., 可查阅：http://media.hoover.org/documents/0817999825_35.pdf; 以及 Sofaer and Goodman, “Cyber crime and security: the transnational dimension”。

[39] 关于国际调查工作中的两国共认罪行原则，见 1994 年第 43 和 44 号《国际刑事政策评论》（联合国出版物，出售品编号：E.94.IV.5）中的《联合国预防和控制与计算机有关的犯罪手册》第 269 段，可查阅：www.uncjin.org/Documents/EighthCongress.html; Judge Stein Schjolberg and Amanda M. Hubbard, “Harmonizing national legal approaches on cybercrime”, paper prepared for the International Telecommunication Union, WSIS Thematic Meeting on Cybersecurity, Geneva, 28 June-1 July 2005, p. 5。

研究范围

26. 对此专题的研究将以关于网上犯罪现象的专题 1 的研究结果为基础：

(a) 对网上犯罪，包括与参与和企图进行网上犯罪有关的行为进行刑事定罪的国家和区域办法盘点；

(b) 刑事定罪方面最佳做法评价；

(c) 不同法律制度和传统对网上犯罪进行刑事定罪的办法差异分析。

专题 6. 程序权力

背景

27. 为了开展有效调查，执法机关需要进入调查程序才能采取必要措施查明犯罪分子的身份并收集刑事诉讼所需的证据。[40]这些措施可能与不涉及网上犯罪的传统调查使用的措施相同。但是，鉴于犯罪分子不一定需要亲临犯罪现场，甚至不需要在犯罪现场附近，网上犯罪调查工作很可能需要以不同于传统调查的方式进行。[41]

调查措施

28. 除与实质性的网上犯罪行为有关的规定外，为应对网上犯罪问题所制定的综合性区域框架大多还载有为便利对网上犯罪的调查工作而专门制定的一整套规定。标准规定包括具体的搜查和扣押程序、迅速保存计算机数据、披露所储存的数据、截获内容数据以及收集通信量数据。

29. 目前，执法机关遇到新开发的技术，这些技术对传统的调查方法产生负面影响。尚未应对其中的许多挑战。

研究范围

30. 对此专题的研究将包括以下内容：

---

[40] 关于在打击网上犯罪中采取的以用户为工作对象的办法，见 S. Görling, “The myth of user education”, paper prepared for the Virus Bulletin Conference, Montreal, 11-13 October 2006,可查阅：www.virusbtn.com/conference/vb2006/abstracts/Gorling.xml。另见法国内政部长 Jean-Pierre Chevènement 在 2000 年于巴黎举行的八国集团关于网络空间安全和信任问题的会议上所作的评论：“更广泛地说，我们必须对用户进行教育。所有用户都必须明白自己在互联网上什么能做什么不能做，还必须警告他们可能存在的危险。随着互联网使用的增多，我们自然要在这方面加大工作力度。”

[41] 由于互联网通信中使用的协议以及在世界各地均可接入互联网，几乎不需要亲临实际提供服务的地点。由于行动地点和犯罪现场的独立性，许多与互联网有关的刑事犯罪都是跨国犯罪。关于行动地点的独立性和犯罪后果，见 *Understanding Cybercrime: A Guide for Developing Countries*（见上文脚注 13）, chap. 3.2.7。

(a) 一些突出表明需要采取具体的网上犯罪调查措施的调查案例盘点；

(b) 区域和国家法律框架所载不同调查规定盘点；

(c) 纵览执法机关对网上犯罪具体调查规定的现有需求，以应对新技术造成的各种挑战；

(d) 不同法律制度和传统制定网上犯罪调查规定的办法差异分析。

专题 7. 国际合作

背景

31. 越来越多的网上犯罪具有国际性的一面，[42]特别是因为犯罪分子通过跨国界的互联网进行操作，通常不需要亲临受害人所在地。由于受害人和犯罪分子所在地点不同以及犯罪分子的机动性，执法和司法机关有必要进行国际合作，并对具有管辖权的国家进行协助。[43]有效的国际合作在打击日益全球化的犯罪（包括传统形式的犯罪和网上犯罪）方面成为主要挑战之一。各国在立法和做法上的差异可能会给国际合作造成困难，而可供各国利用的关于国际合作的条约和协定数量较为有限这一点也可能造成国际合作困难。[44]此外，还应当讨论什么应被视为网上犯罪案件中的国际事项这一问题并就此达成一致。

国际合作文书

32. 正式的国际合作，如引渡、刑事事项司法协助、为没收目的而进行的合作等形式，所必需的法律依据有不同来源。关于国际合作的规定可能构成《联合国打击跨国有组织犯罪公约》[45]等国际和区域协定的一部分。

---

[42] 关于网上犯罪跨国性的一面，见 Mike Keyser, “The Council of Europe Convention on Cybercrime”, *Journal of Transnational Law and Policy*, vol. 12, No. 2 (2003), p. 289, 可查阅： www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf. Sofaer and Goodman, “Cyber crime and security: the transnational dimension” (见上文脚注 37), pp. 1 ff。

[43] 在这方面见《联合国打击跨国有组织犯罪公约及其各项议定书实施立法指南》(联合国出版物，出售品编号：E.05.V.2), p. 217。可查阅：www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf。

[44] Carlos A. Gabuardi, “Institutional framework for international judicial cooperation: opportunities and challenges for North America”, *Mexican Law Review*, vol. 1, No. 2 (2009), p. 156, 可查阅：http://info8.juridicas.unam.mx/pdf/mlawrns/cont/2/cmm/cmm7.pdf。

[45] 联合国，《条约汇编》，第 2225 卷，第 39574 号；关于本《公约》，见 Jennifer M. Smith, “An international hit job: prosecuting organized crime acts as crimes against humanity”, *Georgetown Law Journal*, vol. 97, 2009, p. 1,118, 可查阅：www.georgetownlawjournal.org/issues/pdf/97-4/Smith.PDF。

研究范围

33. 对此专题的研究将包括以下内容：

(a) 对互联网刑事执法国际事项进行定义的国内法律办法盘点；

(b) 审查普遍国际依据等与有效的法律依据有关的备选项及其他打击网上犯罪的对策；

(c) 在网上犯罪案件中开展有效的国际合作，特别是引渡和司法协助方面的挑战，包括适用双重犯罪和调查措施上的差异；

(d) 涉及网上犯罪调查和起诉相关国际合作的国家和国际规定盘点；

(e) 双边和多边条约和安排中最佳做法实例（除其他外，从联络点 24/7 网络运转中吸取的教训）盘点；

(f) 涉及国际合作的网上犯罪案件盘点；

(g) 情报共享等非正式国际合作手段的作用和挑战；

(h) 有关机关在国际合作方面的现有需求概览；

(i) 查明正在开展的培训方案、经验交流、能力建设和技术援助活动并确定这些方面今后的想法，以加强刑事司法能力和使各国能够进行国际合作。

专题 8. 电子证据

背景

34. 由于越来越多的信息以数字形式储存，电子证据与网上犯罪调查和传统调查工作均相关。计算机和网络技术已经成为发达国家日常生活的一部分，正在逐渐走进发展中国家的日常生活。硬盘[46]的储存能力不断增大，数字化文件储存与有形文件的储存相比成本低廉，[47]因此数字化文件日渐增多。[48]今天，大量数

---

[46] 见 D. Abramovitch, “A brief history of hard drive control”, *IEEE Control Systems Magazine*, vol. 22, No. 3 (2002), pp. 28 ff.; T. Coughlin, D. Waid and J. Porter, “The disk drive: 50 years of progress and technology innovation — the road to two billion drives”, *Computer Technology Review*, April 2005, 可查阅：www.tomcoughlin.com/Techpapers/DISK%20DRIVE%20HISTORY,%20TC%20Edits,%20050504.pdf。

[47] S. M. Giordano, “Electronic evidence and the law”, *Information Systems Frontiers*, vol. 6, No. 2 (2006), p. 161; S. D. Willinger and R. M. Wilson, “Negotiating the minefields of electronic discovery”, *Richmond Journal of Law and Technology*, vol. 10, No. 5 (2004)。

[48] Lange/Minster, Electronic Evidence and Discovery, p. 6。

据仅以数字化形式储存。[49]由于这种增长，文本文件、数字视频和数字图片等电子文件[50]正在网上犯罪调查和相关的法院诉讼中发挥着作用。[51]

电子证据规则

35. 电子证据构成了许多挑战，有的是在证据收集阶段，有的是在证据采信阶段。[52]在证据收集过程中，调查人员必须满足某些程序和要求，如为保护数据完整性而必须进行的特别处理。执法机关需要采取具体措施以便成功进行调查。是否具备这类措施，在没有传统形式的证据如指纹或证人指认的情况下，尤其相关。在这些情形下，能否成功认定并起诉犯罪分子，依据的是正确收集和评价数字化证据。[53]

36. 数字化还影响执法机关和法院处理证据的方式。[54]传统文件在法庭上出示即可，而数字化证据所需的专门程序可能不适合将其转换为传统证据，如文件的打印本。[55]

---

[49] Chet Hosmer, “Proving the integrity of digital evidence with time”, *International Journal of Digital Evidence*, vol. 1, No. 1 (2002), p. 1, 可查阅：www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf。

[50] 关于数字图像的可采信性和可靠性，见 Jill Witkowski, “Can juries really believe what they see? New foundational requirements for the authentication of digital images”, *Washington University Journal of Law and Policy*, vol. 10, 2002, pp. 267 ff。

[51] Michael Harrington, “A methodology for digital forensics”, Thomas M. Cooley Journal of Practical and Clinical Law, vol. 7, 2004, pp. 71 ff.; Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 2nd ed. (London, Academic Press, 2004), p. 14. 关于不同国家的法律框架，见 C. A. Rohrmann and J.S.A. Neto, “Digital evidence in Brazil”, Digital Evidence and Electronic Signature Law Review, No. 5, 2008; M. Wang, “Electronic evidence in China”, Digital Evidence and Electronic Signature Law Review, No. 5, 2008; P. Bazin, “An outline of the French Law on digital evidence”, Digital Evidence and Electronic Signature Law Review, No. 5, 2008; A. B. Makulilo, “Admissibility of computer evidence in Tanzania”, Digital Evidence and Electronic Signature Law Review, No. 4, 2007; R. Winick, “Search and seizures of computers and computer data”, Harvard Journal of Law and Technology, vol. 8, No. 1 (1994), p. 76; F. Insa, “Situation report on the admissibility of electronic evidence in Europe”, in Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, p. 213。

[52] Casey, Digital Evidence and Computer Crime （见脚注 51）, p. 9.。

[53] 关于确定计算机法医学形式的必要性，见 R. Leigland 和 A. W. Krings, “A formalization of digital forensics”, *International Journal of Digital Evidence*, vol. 3, No. 2 (2004)。

[54] 关于根据传统程序和原则处理数字证据方面的困难，见 R. Moore, “To view or not to view: examining the plain view doctrine and digital evidence”, *American Journal of Criminal Justice*, vol. 29, No. 1 (2004), pp. 57 ff。

[55] 见 John R. Vacca, *Computer Forensics: Computer Crime Scene Investigation*, 2nd ed. (Hingham, Massachusetts, Charles River Media, 2005), p. 3. 关于早期对打印件使用问题进行的讨论，见 Robinson, “The admissibility of computer printouts under the business records exception in Texas”, *South Texas Law Journal*, vol. 12, 1970, pp. 291 ff。

研究范围

37. 对此专题的研究将包括以下内容：

(a) 涉及电子证据收集、保存、储存、分析和采信的规定、保障和标准盘点；

(b) 不同法律制度和传统的电子证据处理办法差异分析及共同原则鉴别；

(c) 收集关于专门培训、能力建设和技术交流的最佳做法；

(d) 跨境数字化证据交流机制分析。

专题 9. 服务提供方和私营部门的作用和责任

背景

38. 预防和调查网上犯罪取决于许多不同因素。即使犯罪分子是单独行动的，网上犯罪的实施也会自动涉及一连串的个人和企业。由于互联网结构的原因，传输简单的电子邮件信息需要若干服务提供方的服务：电子邮件服务提供方、接入服务提供方和向收件人转发电子邮件信息的路由网段服务提供方。下载含有虐待儿童内容的材料的情形与之类似。下载过程涉及（例如在网站上）上传图片的内容提供方、为网站提供储存器的寄存托管方、向用户转发文件的路由网段服务提供方，最后是用户得以进入互联网的接入服务提供方。

39. 尽管经常强调要确保有适当的立法，但私营行业仍在预防和协助调查网上犯罪方面发挥着重要作用。然而私营行业参与网上犯罪调查工作也伴有许多挑战。

法律问题

40. 实际上，网上犯罪若无提供方的参与便无法实施，而且提供方往往并无能力预防网上犯罪，因而产生的问题是，是否应当对服务提供方的责任加以限制。这一问题的答案对于信息和通信技术基础设施的经济发展至关重要。

41. 执法机关的努力往往有赖于互联网提供方的合作。这不禁令人关切，因为限制服务提供方为用户行为而承担的责任可能会影响到服务提供方对网上犯罪调查工作给予的合作和支持，也会影响到对网上犯罪的实际预防。

行业作用

42. 行业在应对网上犯罪问题方面的作用是错综复杂的；其范围可能包括制定并实施解决办法保护自己的服务不遭非法滥用，以及保护用户和支持调查工作。行业采取的自我保护措施通常是综合性业务战略中的合理内容，一般不要求有具体的法律依据，只要这些措施不涉及非法的主动防范。代表用户采取的

保护措施只要是征得用户同意后采取的，也不成问题。但行业参与犯罪调查工作在许多国家造成了难题，对此也采取了不同办法。一些国家让行业完全自愿地参与犯罪调查，并为便利行业和执法机关合作而制定了准则。还有的国家采用了另一种办法，规定行业在法律上有义务与执法机关合作进行犯罪调查。

研究范围

43. 对此专题的研究将包括以下内容：

(a) 服务提供方责任相关办法和做法，包括区分不同类型的服务提供方；

(b) 描述服务提供方等私营部门的作用、性质和职能；

(c) 私营部门预防和调查网上犯罪的做法；

(d) 私营部门和执法机关开展预防和调查网上犯罪合作的相关做法；

(e) 国内和跨国服务提供方协助执法机关预防和调查网上犯罪的能力；

(f) 打击网上犯罪的费用分配；

(g) 评价现有办法的优缺点。

专题 10. 预防犯罪和刑事司法能力及应对网上犯罪的其他对策

背景

44. 关于应对网上犯罪的讨论往往侧重于法律对策，但打击网上犯罪的战略通常遵循的是一种更为综合的办法。

其他对策

45. 除应对网上犯罪的法律对策外，其他对策包括采取预防犯罪措施、为调查和起诉犯罪而发展必要的基础设施（例如设备和人员）、对参与打击网上犯罪的专家进行培训、制定最佳做法、对互联网用户进行教育以及预防或调查网上犯罪的技术解决办法。

研究范围

46. 对此专题的研究将包括以下内容：

(a) 用于应对网上犯罪的其他办法概览；

(b) 网上犯罪预防措施；

(c) 确定这些办法成功与否的衡量手段；

(d) 不同对策之间的关系分析及其结合并用的可能性分析；

(e) 学术界可能发挥的作用，特别是通过制定适当的课程和开展对网上犯罪现象的研究。

专题 11. 国际组织

背景

47. 在 1970 和 1980 年代，对网上犯罪采取的法律办法主要是在国家一级制定的。在 1990 年代，区域组织和国际组织开始应对网上犯罪问题，包括通过大会（多年来大会已经通过了关于网上犯罪的若干决议）、[56]英联邦（《网上犯罪示范法》及可能对《哈拉雷计划》进行扩充以将电子数据涵盖在内）、欧洲委员会（《网上犯罪公约》）、欧洲联盟（关于攻击信息系统问题的《框架决定》和理事会根据《欧洲联盟条约》第 34 条制定的欧洲联盟成员国间刑事事项互助公约）、独立国家联合体（独联体）（2001 年独联体国家打击计算机信息领域犯罪的合作协定）、美洲国家组织和上海合作组织等。包括国际电信联盟（国际电联在全球网络安全议程框架内开展了活动）在内的国际组织以及联合国毒品和犯罪问题办公室收集了数据，筹备了各项研究。

统一各种标准

48. 实践证明，在技术协议方面单一的统一标准是成功的，这也提出了一个问题，即如何避免不同国际办法之间的冲突。[57]欧洲委员会《网上犯罪公约》和英联邦《网上犯罪示范法》都采用了最全面的办法，其中涵盖了实体刑法、程序法和国际合作。可在此专题下对现有框架进行审查，以确定其范围、优缺点和可能存在的任何差距。

研究范围

49. 对此专题的研究将包括以下内容：

(a) 区域组织和国际组织包括联合国的最佳做法盘点；

(b) 现有办法的优缺点；

(c) 现有国际法律办法的差距分析。

---

[56] 例如，大会第 45/121、55/63、56/121 和 60/177 号决议。

[57] 详细情况见 M. Gercke, “National, regional and international legislative approaches in the fight against cybercrime”, *Computer Law Review International*, 2008, pp. 7 ff。

专题 12. 技术援助

背景

50. 人们有时会认为，网上犯罪问题主要影响的是发达国家，其实不然。2005 年，发展中国家互联网用户的数量首次超过了工业国家的用户数量。[58]由于打击网上犯罪战略的基本目标之一便是防止用户沦为网上犯罪受害者，因此在发展中国家打击网上犯罪的重要性不容低估。还必须考虑到的一个事实是，网上犯罪对发展中国家和发达国家的影响可能有所不同。2005 年，经济合作与发展组织发表了一份报告，其中分析了垃圾电子邮件对发展中国家的影响，[59]发现发展中国家经常报告其互联网用户与发达国家用户相比受垃圾电子邮件和互联网滥用的影响更加严重。

技术援助

51. 网上犯罪由于其跨国性的一面，需要所有国家有效而协调地行动。发达国家和发展中国家在提供技术援助方面存在共同利益。防止为网上犯罪分子建立安全庇护所是打击网上犯罪的关键挑战之一。[60]因此，在发展中国家进行能力建设使之能够打击网上犯罪成为国际社会的一个主要任务。

52. 2010 年举行的第十二届联合国预防犯罪和刑事司法大会通过的《萨尔瓦多宣言》体现了技术援助的重要性，其中建议联合国毒品和犯罪问题办公室应根据请求向各国提供技术援助以应对网上犯罪问题。《萨尔瓦多宣言》还建议考虑与所有相关合作伙伴共同制定国际性的能力建设行动计划。技术援助应当与时俱进并持续提供。

研究范围

53. 对此专题的研究将包括以下内容：

(a) 确定应对网上犯罪方面的技术援助的基本要素和原则；

(b) 国家、区域和国际现有网上犯罪问题培训课程盘点；

(c) 确定在应对网上犯罪方面提供技术援助的最佳做法。

---

[58] 见 Development Gateway's Special Report, *Information Society — The Next Steps* (2005)。

[59] "Spam issues in developing countries"（见上文脚注 34）。

[60] 有若干国际组织论述了这一问题。大会第 55/63 号决议指出："各国应确保其法律和做法能够消除向非法滥用信息技术的人提供的安全庇护所"。决议全文可查阅：www.unodc.org/pdf/crime/a_res_55/res5563e.pdf。1997 年 12 月 10 日在华盛顿特区举行的八国集团司法和内政部长会议核可的打击高科技犯罪的原则和行动计划强调："决不为滥用信息技术者提供安全庇护所"。

附件二

研究方法

1. 为了完成专家组有关此研究的任务授权，对下述结构进行了详细阐述，以便利研究的进行。研究将在专家组的主持下开展。

2. 各国均有权提出本国的看法，并应在研究中得以反映。

3. 将责成联合国毒品和犯罪问题办公室（毒品和犯罪问题办公室）制定研究，包括编制一份调查表、收集和分析数据以及编拟研究案文草稿。为完成这一任务，毒品和犯罪问题办公室将利用从其各专题部门（条约事务司、政策和研究处）获得的内部专门知识和能力。为此，应提供充分的预算外资源，使毒品和犯罪问题办公室得以有效履行这些职能。为帮助秘书处确保充分体现主要的技术专门知识、系统和需求，各区域组将向秘书处提供政府专家（不超过六名）的姓名、联系信息和专长领域。秘书处将酌情临时与作为技术顾问的各位专家交换意见。

4. 秘书处将就流程情况定期向专家组主席团作简要介绍和咨询，并向会员国散发咨询会议记录。拟定专家名单的目的并非是为了设立任何封闭型的专家组或者专家组的其他平行或附属机构。

5. 为了采集信息，毒品和犯罪问题办公室将编制一份调查表，更广泛地分发给会员国、政府间组织和私营部门实体（见下文的指示性时间表）。调查表将包括一个单一的调查工具。该调查工具将参照第一次专家组会议的概念/工作文件所载的经修正的纲要和第一次专家组会议报告体现的建议。

6. 其次，秘书处铭记需要均衡不同区域的代表情况，将根据需要与私营部门代表，包括互联网服务提供方、服务使用者和其他相关行为者的代表、发达国家和发展中国家的学术界代表以及相关政府间组织代表交换意见。

指示性时间表

2011 年 1 月：第一次专家组会议提供政策指示和准则。核可研究专题、方法和时间表。

2011 年 2 月至 4 月：确定协助毒品和犯罪问题办公室开展研究的专家（见上文）。向专家组主席团提交姓名。通过各区域组沟通政府专家姓名。

2011 年 4 月：预防犯罪和刑事司法委员会第二十届会议。分发毒品和犯罪问题办公室的调查表草案进行信息采集。征求会员国的反馈/意见。开展在线磋商，接收专家组成员的意见。委员会认可第一次专家组会议的成果及第一次会议上建议的今后的工作。

2011 年 6 月中旬：接收关于调查表的意见的最后期限。

2011 年 7 月中旬：最后确定调查表并分发给会员国。调查表还会以单独信函的形式发送给政府间组织及私营部门和学术机构代表，请他们提供信息和对与之

切合的问题作出答复。特别会向私营部门作出保证，将对收到的任何数据保守秘密，若公开，则匿名。

2011 年 7 月中旬至 12 月末：数据收集和分类（5 个半月，秘书处将在 2011 年 10 月初发出中期提示）。

2011 年 12 月初：在举行委员会第二十届会议续会的同时举行第二次专家组会议。简报所取得的进展情况。中期进展情况报告，供委员会第二十一届会议（2012 年 4 月）获悉情况。

2012 年 4 月：向委员会第二十一届会议提交中期进展情况报告。

2012 年 1 月中旬至 2012 年 7 月：分析数据和起草研究报告。研究案文草稿定稿。

2012 年 8 月：向专家组成员分发研究案文草稿，确保按时编拟成文，提交第三次专家组会议。

2012 年 10 月：第三次专家组会议，审查、修订和通过研究报告草稿。

2013 年 4 月：向委员会第二十二届会议提交研究报告，供其审议。