20 December 2010
Chinese
Original: English

网上犯罪问题专家组
2011 年 1 月 17 日至 21 日，维也纳

在关于网上犯罪的影响和对策的综合研究中审议的专题草稿

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也在其第 2010/18 号决议中采纳了该建议。

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，该项综合研究将研究：

> 网上犯罪问题以及各会员国、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打击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个实质方面（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 13 个专题。这 13 个专题组成以下几个小类。

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。为了全面处理网上犯罪所造成的问题，将对三个关键领域进行详细分析：

V.10-58676 (C) GX 130111 130111

(a) 各种网上犯罪行为（专题 1）；

(b) 统计数据（专题 2）；

(c) 网上犯罪的挑战（专题 3）。

处理网上犯罪的法律对策（专题 4-9）

6. 《萨尔瓦多宣言》要求研究关于处理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。除了统一法律工作的一般方面，还提出了法律对策的五个具体领域：

(a) 统一法律（专题 4）；

(b) 实质刑法（专题 5）；

(c) 侦查工具（专题 6）；

(d) 国际合作（专题 7）；

(e) 电子证据（专题 8）；

(f) 赔偿责任（专题 9）。

处理网上犯罪的法律外对策（专题 10）

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

国际社会采取的对策（专题 11）

8. 《萨尔瓦多宣言》要求对会员国、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，但在一个单独标题下述及国际社会对策将便于分析更为总体的方面，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。

私营部门的对策（专题 13）

10. 如上所述，《萨尔瓦多宣言》还建议在综合研究中对私营部门对策进行分析。

二. 对各专题的详细介绍

专题 1. 网上犯罪现象

背景

11. 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型的犯罪行为。罪名从非法内容到某些形式的经济犯罪不等。与这类犯罪行为有关的挑战包括：所涵盖的罪行范围广泛，犯罪手法不断翻新。

计算机犯罪和网上犯罪的发展

12. 在 1960 年代，首次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

---

[1] 关于有关的挑战，见 Slivka/Darrow 著，Methods and Problems in Computer Security, Journal of Computers and Law, 1975 年，第 217 页及以下。

[2] McLaughlin 著, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978 年，Vol. 2，第 217 页及以下。

[3] Gemignani 著, Computer Crime: The Law in ‘80, Indiana Law Review, Vol. 13, 1980 年，第 681 页。

[4] McLaughlin 著, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978 年, Vol. 2，第 217 页及以下。

[5] Freed 著，Materials and cases on computer and law，1971 年，第 65 页。

[6] Bequai 著, The Electronic Criminals – How and why computer crime pays, Barrister, Vol.4, 1977 年，第 8 页及以下。

[7] Criminological Aspects of Economic Crimes, 12th Conference of Directors of Criminological Research Institutes, 欧洲委员会，斯特拉斯堡, 1976 年, 第 225 页及以下; Staff Study of Computer Security in Federal Programs; Committee on Governmental Operations, the 95th Congress 1 Session, United States Senate，1977 年 2 月。

[8] McLaughlin 著, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978, Vol. 2, 第 217 页及以下; Bequai 著, Computer Crime: A Growing and Serious Problem, Police Law Quarterly, Vol. 6, 1977 年，第 22 页。

[9] Computer Abuse: The Emerging Crime and the Need for Legislation, Fordham Urban Law Journal，1983 年，第 73 页。

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，互联网用户迅速增加，随之出现了新的犯罪方法。例如，儿童色情材料的传播从书籍和录像带的实物交流转为通过网站和互联网服务传播。[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”攻击，[14]以及新出现的“互联网协议语音技术（VoIP 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

13. 对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) 尚未加以刑事定罪的罪行盘点；

(c) 复合犯罪（如“网络钓鱼”）和未来趋势概览；

---

[10] Bloom Becker 著, The Trial of Computer Crime, Jurimetrics Journal, Vol. 21, 1981 年,第 428 页; Schmidt 著, Legal Proprietary Interests in Computer Programs: The American Experience, Jurimetrics Journal, Vol. 21, 1981 年，第 345 页及以下。Denning 著, Some Aspects of Theft of Computer Software, Auckland University Law Review, Vol. 4, 1980 年，第 273 页及以下; Weiss 著, Pirates and Prizes: The Difficulties of Protecting Computer Software, Western State University Law Review, Vol. 11, 1983 年，第 1 页及以下； Bigelow 著, The Challenge of Computer Law, Western England Law Review, Vol. 7, 1985 年,第 401 页及以下; Thackeray 著, Computer-Related Crimes, Jurimetrics Journal, 1984 年，第 300 页及以下。

[11] Yee 著, Juvenile Computer Crime – Hacking: Criminal and Civil Liability, Comm/Ent Law Journal, Vol. 7, 1984 年,第 336 页及以下；Who is Calling your Computer Next? Hacker!, Criminal Justice Journal, Vol. 8, 1985 年,第 89 页及以下; The Challenge of Computer-Crime Legislation: How Should New York Respond?, Buffalo Law Review, Vol. 33，1984 年，第 777 页及以下。

[12] Child Pornography, CSEC World Congress Yokohama Conference, 2001 年,第 17 页; Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, United States House of Representatives, 109th Congress，2007 年，第 9 页。

[13] “网络钓鱼”一词系指为使受害人透露个人/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 Understanding Cybercrime: A Guide for Developing Countries，国际电信联盟 2009 年，第 2.8.4 章。

[14] “僵尸”是简称，系指一组受害后在外部控制下运行软件的计算机。更多详细信息见 Wilson 著，Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress，2007 年，第 4 页。

[15] Simon/Slay 著，“Voice over IP: Forensic Computing Implications”，2006 年。

[16] Velasco San Martin 著, Jurisdictional Aspects of Cloud Computing, 2009 年; Gercke 著, Impact of Cloud Computing on Cybercrime Investigation, 发表于 Taeger/Wiebe, Inside the Cloud, 2009 年，第 499 页及以下。

(d) 相关案例盘点；

(e) 网上犯罪的定义和类型学；

(f) 预防犯罪机制（技术性）；

(g) 网上犯罪定义的重要性探讨；

(h) 某些网上犯罪非刑事定罪解决办法可能性考虑。

专题 2. 统计数据信息

背景

14. 犯罪统计数据为决策者和学者的讨论和决策提供了依据。[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。

网上犯罪统计数据目前的状况

15. 关于犯罪程度的信息通常取自犯罪统计数据和调查。[18]若使用这两种来源制定政策建议，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结合起来，但这种方法不会产生可靠的信息，因为各国的法律和记录办法各不相同。[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]

16. 其次，统计数据所能反映的只有已经侦破和报案的犯罪。[22]特别在网上犯罪

---

[17] Collier/Spaul 著, Problems in Policing Computer Crime, Policing and Society, 1992 年, Vol. 2, 第 308 页，可在以下网址查阅：http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf。

[18] 关于犯罪统计数据新表现出的重要性，见 Osborne/Wernicke 著, Introduction to Crime Analysis, 2003 年，第 1 页及以下，可在以下网址查阅：www.crim.umontreal.ca/cours/cri3013/osborne.pdf。

[19] 在这方面见 Overcoming barriers to trust in crimes statistics, UK Statistics Authority, 2009 年, 第 9 页，可在以下网址查阅：www.statisticsauthority.gov.uk/.../overcoming-barriers-to-trust-in-crime-statistics--england-and-wales---interim-report.pdf。

[20] Alvazzi del Frate 著，Crime and criminal justice statistics challenges 载于 Harrendorf/Heiskanen/Malby 编, International Statistics on Crime and Justice, 2010 年，第 168 页，可在以下网址查阅：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. 271，2006 年 10 月，第 3 页。

[22] 关于有关的挑战见 Kabay 著, Understanding Studies and Surveys of Computer Crime, 2009 年，可在以下网址查阅： www.mekabay.com/methodology/ crime_stats_methods.pdf。

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誉。[24]一家公司如果宣称有黑客侵入了自己的服务器，可能会失去用户的信任，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。在实务中，所报案件牵涉的费用通常极高。[28]

研究范围

17. 对这一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；

---

[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沉默，而要向主管机关通报，使主管机关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 Heise News, 27.10.2007，可在以下网址查阅：www.heise-security.co.uk/news/80152。另见 Comments on Computer Crime – Senate Bill S. 240, Memphis State University Law Review，1980 年，第 660 页。

[24] 见 Mitchison/Urry 著, Crime and Abuse in e-Business, IPTS Report，可在以下网址查阅：www.jrc.es/home/report/english/articles/vol57/ICT2E576.htm; Collier/Spaul 著, Problems in Policing Computer Crime, Policing and Society, 1992 年, Vol. 2, 第 310 页, 可在以下网址查阅：http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf。

[25] 见 Collier/Spaul 著, Problems in Policing Computer Crime, Policing and Society, 1992, Vol. 2, 第 310 页，可在以下网址查阅：http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf; Smith 著，“Investigating Cybercrime: Barriers and Solutions”，2003 年,第 2 页，可在以下网址查阅： www.aic.gov.au/conferences/other/smith_russell/2003-09-cybercrime.pdf。

[26] 实际上，报纸和电视台对成功的互联网侦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, 09.10.2007, 可在以下网址查阅：www.nytimes.com/2007/10/09/world/europe/09briefs-pedophile.html?_r=1&oref=slogin，以及国际刑警组织网站所提供的信息，可在以下网址查阅：www.interpol.int/Public/THB/vico/Default.asp。

[27] 见 SOCA，“International crackdown on mass marketing fraud revealed, 2007”，可在以下网址查阅：www.soca.gov.uk/downloads/massMarketingFraud.pdf。

[28] 在 2006 年《国家白领犯罪中心互联网犯罪报告》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，但平均造成的损失很高。

(d) 确定有哪些国家专门收集了关于网上犯罪行为的统计数据；

(e) 评估收集网上犯罪统计数据信息的必要性和益处；

(f) 研究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。

专题 3. 网上犯罪的挑战

背景

18. 目前十分注重制定战略处理网上犯罪的各种具体挑战。这一发展情况的原因有二：首先，侦查网上犯罪需要一些新工具，因此需要进行深入细致的研究，其次，涉及网络技术的犯罪侦查工作有一些独特的挑战，是传统的侦查工作不会遇到的。

打击网上犯罪工作的挑战

19. 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侦查工作。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。对付网上犯罪的侦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结构，力求保持其主要功能完好，即使是在网络的组成部分受到攻击时。这种分散自立方式的原始设计并不方便犯罪侦查或防止从网络内部发起的攻击，侦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]

---

[29] “Websense Security Trends Report 2004”，第 11 页; Information Security – Computer Controls over Key Treasury Internet Payment System，美国审计总署 2003 年，第 3 页，Sieber 著, Council of Europe Organised Crime Report 2004，第 143 页。

[30] Ealy 著，“A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention”，第 9 页。

[31] 互联网简史，包括其军事起源，见 Leiner, Cerf, Clark, Kahn, Kleinrock; Lynch, Postel, Roberts, Wolff 著，“A Brief History of the Internet”，可在以下网址查阅：www.isoc.org/internet/history/brief.shtml。

[32] Lipson 著，“Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues”。

研究范围

20. 对这一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。

专题 4. 统一法律

背景

21. 在过去 20 年间，各国和区域组织为处理网上犯罪问题制定了法律和法律框架。尽管已经形成了某些共同趋势，但各国法律之间仍然存在很大差异。

国家间和区域间的差异

22. 各国家和区域在法律框架上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]

---

[33] Understanding Cybercrime: A Guide for Developing Countries, 国际电信联盟 2009 年，第 2.6.7 章。

[34] 见 Spam Issue in Developing Countries，第 4 页，可在以下网址查阅：www.oecd.org/dataoecd/5/47/34935342.pdf。

[35] 关于言论自由原则，见 Tedford/Herbeck Haiman 著, Freedom of Speech in the United States, 2005 年; Barendt 著, Freedom of Speech, 2007 年; Baker 著，Human Liberty and Freedom of Speech; Emord 著, Freedom, Technology and the First Amendment, 1991 年; 关于这一原则对于电子监视的重要性，见 Woo/So 著, The case for Magic Lantern: September 11 highlights the need for increasing surveillance, Harvard Journal of Law and Technology, Vol. 15, No. 2, 2002 年, 第 530 页及以下; Vhesterman 著, Freedom of Speech in Australian Law; A Delicate Plant, 2000 年; Volokh 著, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001 年，第 57 页及以下，可在以下网址查阅： www.law.ucla.edu/volokh/harass/religion.pdf; Cohen 著, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007 年，可在以下网址查阅：www.fas.org/sgp/crs/misc/95-815.pdf。

[36] 人们对于表达意见自由的关切解释了为什么某些种族主义行为在《网上犯罪公约》中没有定为非法，而第一附加议定书将其定为刑事犯罪。见 Explanatory Report to the First Additional Protocol, No. 4。

23. 由于网上犯罪是一种真正的跨国犯罪，[37]侦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一定程度的共识和法律上的统一，以防止产生安全庇护所。[39]

研究范围

24. 对这一专题的研究将包括以下内容：

(a) 对统一网上犯罪法律方面的现有工作的成功和局限之处进行分析；

(b) 编辑各国执行区域组织法律标准的所有方法，并分析确定哪些技术可有助于确保这些方法保持协调一致；

(c) 分析法律标准上的差异对国际合作有多大程度的影响；

(d) 确定法律起草方面的哪些方法可确保必要的灵活性，以便在统一的过程中保持基本的法律传统。

专题 5. 将网上犯罪行为定为刑事犯罪

背景

25. 要有效侦查和起诉网上犯罪，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侦查工作有关，如上所述，还影响到国际合作。

实体刑法

26. 为处理网上犯罪问题而制定的综合性区域框架大多包含一整套实体刑法条文，其目的是缩小国内法方面的差距。这些框架中的标准条文包括将非法侵

---

[37] 关于跨国攻击在破坏性最大的攻击中所占部分的大小，见 Sofaer/Goodman 著, Cyber Crime and Security – The Transnational Dimension 载于 Sofaer/Goodman 著, The Transnational Dimension of Cyber Crime and Terrorism, 2001 年, 第 7 页，可在以下网址查阅：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 Putnam/Elliott 著, International Responses to Cyber Crime, 载于 Sofaer/Goodman 著, The Transnational Dimension of Cyber Crime and Terrorism, 2001 年, 第 35 页及以下，可在以下网址查阅：http://media.hoover.org/documents/0817999825_35.pdf; Sofaer/Goodman 著, Cyber Crime and Security – The Transnational Dimension 载于 Sofaer/Goodman 著, The Transnational Dimension of Cyber Crime and Terrorism, 2001 年, 第 1 页及以下，可在以下网址查阅：http://media.hoover.org/documents/0817999825_1.pdf。

[39] 关于国际侦查工作中的两国共认罪行原则，见《联合国预防和控制与计算机有关的犯罪手册》，269，可在以下网址查阅：www.uncjin.org/Documents/EighthCongress.html; Schjolberg/Hubbard 著, Harmonizing National Legal Approaches on Cybercrime, 2005 年, 第 5 页, 可在以下网址查阅：www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf。

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。而一些方法则更进一步，将制造和传播可用于实施网上犯罪的工具（如软件或硬件）、与儿童色情材料有关的行为、“诱骗”或煽仇言论定为刑事犯罪。

研究范围

27. 对这一专题的研究将以关于网上犯罪现象的专题 1 的研究为基础，包括以下内容：

(a) 国家和区域网上犯罪刑事定罪方法盘点；

(b) 刑事定罪方面最佳做法评价；

(c) 英美法系国家和大陆法系国家网上犯罪刑事定罪方法差异分析。

专题 6. 侦查程序

背景

28. 为了进行有效侦查，执法机关需要进入侦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侦查使用的措施相同。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，网上犯罪侦查工作很可能需要以不同于传统侦查的方式进行。[41]

侦查措施

29. 除了与实质性的网上犯罪行为有关的条文之外，为处理网上犯罪问题所制定的综合性区域框架大多还包含为便利对网上犯罪的侦查工作而专门制定的一整套条文。标准条文包括具体的搜查和没收程序、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信息量数据。

---

[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 Görling 著, The Myth Of User Education, 2006 年，网址为 www.parasite-economy.com/texts/StefanGorlingVB2006.pdf。另见法国内政部长 Jean-Pieree Chevenement 在 2000 年于巴黎举行的八国集团首脑会议上所作的评论：“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连接互联网，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，国际电信联盟 2009 年，第 3.2.7 章。

30. 一些国家除这些标准条文外还通过了一些措施处理具体的挑战，如监听 VoIP 网络电话通讯。[42]尽管多数国家已经规定了用于监听固定电话和移动电话通讯的侦查措施，如在电话线路上安装监听器的电话监听，[43]但这些措施通常不足以对 VoIP 网络电话通讯进行监听。对传统语音电话的监听通常是通过电信服务供应商进行的。[44]执法机关将这一原则适用于 VoIP 网络电话，一般通过互联网服务提供商和 VoIP 网络电话服务提供商开展行动。但是，如果 VoIP 网络电话服务使用的是 P2P 对等网络技术，服务提供商可能无法监听通讯。[45]

研究范围

31. 对这一专题的研究将包括以下内容：

(a) 一些突出表明需要采取具体的网上犯罪侦查措施的侦查案例；

(b) 区域和国内法律框架所含不同侦查规定盘点；

(c) 关于目前执法机关对网上犯罪具体侦查规定的需要的概览；

(d) 英美法系国家和大陆法系国家网上犯罪侦查规定方法的差异分析。

---

[42] “互联网协议语音技术”这一术语系指通过包交换网和相关协议提供语音通信服务的传输技术。更多信息见 Swale 著，Voice Over IP: Systems and Solutions, 2001 年，Black 著，“Voice Over IP”，2001 年。

[43] 关于监听的重要性和技术解决办法，见 Karpagavinayagam/State/Festor 著，“Monitoring Architecture for Lawful Interception in VoIP Networks, in Second International Conference on Internet Monitoring and Protection”，ICIMP 2007.关于与监听数据通信有关的难题，见 SwaleChochliouros/Spiliopoulou/Chochliouros 著，“Measures for Ensuring Data Protection and Citizen Privacy Against the Threat of Crime and Terrorism – The European Response”，载于 Janczewski/Colarik 著，“Cyber Warfare and Cyber Terrorism”，2007 年，第 424 页。

[44] 关于公用电话交换网通讯和 VoIP 网络电话通讯之间的差别，见 Seedorf 著，“Lawful Interception in P2P-Based VoIP Systems”，载于 Schulzrinne/State/Niccolini 编，Principles, Systems and Applications of IP Telecommunication。Services and Security for Next Generation Networks，2008 年，第 217 页及以下。

[45] 关于执法机关对 VoIP 网络电话的监听，见 Bellovin 等著，“Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP”，Simon/Slay 著，“Voice over IP: Forensic Computing Implications”，2006 年; Seedorf 著，“Lawful Interception in P2P-Based VoIP Systems”，载于 Schulzrinne/State/Niccolini 编，Principles, Systems and Applications of IP Telecommunication。Services and Security for Next Generation Networks，2008 年，第 217 页及以下。

专题 7. 国际合作

背景

32. 越来越多的网上犯罪具有国际性的一面，[46]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。[47]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。各国在法律和做法上的差异可能会给国际合作造成困难，可能造成国际合作困难的还有，可供各国利用的关于国际合作的条约和协议数量较为有限。[48]

国际合作文书

33. 正式的国际合作，如引渡、刑事事项司法合作、为没收目的而进行的合作等形式，所必需的法律依据有四个主要来源。

34. 首先，关于国际合作的规定可能是处理特定国际犯罪的国际协议和区域协议如《联合国打击跨国有组织犯罪公约》[49]、[50]和《欧洲委员会网上犯罪公约》的一部分。[51]其次，有一些关于国际合作的区域条约，如欧洲理事会、美洲和南部非洲发展共同体关于引渡或刑事事项司法协助的条约。第三个来源是关于引渡或司法协助的双边协议。这些协议一般载有与可提交的各类请求有关的具体信息，规定相关程序和联络方式，以及请求国和被请求国的权利和义务。[52]国际

---

[46] 关于网上犯罪跨国性的一面，见 Keyser 著，The Council of Europe Convention on Cybercrime, Journal of Transnational Law and Policy, Vol. 12, No. 2，第 289 页，可在以下网址查阅：www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf 。Sofaer/Goodman 著, Cyber Crime and Security – The Transnational Dimension，载于 Sofaer/Goodman 著, The Transnational Dimension of Cyber Crime and Terrorism, 2001 年，第 1 页及以下，可在以下网址查阅：http://media.hoover.org/documents/0817999825_1.pdf。

[47] 在这方面见《联合国打击跨国有组织犯罪公约实施立法指南》,2004 年,可在以下网址查阅：www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf。

[48] Gabuardi 著, Institutional Framework for International Judicial Cooperation: Opportunities and Challenges for North America, Mexican Law Review, Vol. I, No. 2, 第 156 页，可在以下网址查阅：http://info8.juridicas.unam.mx/pdf/mlawrns/cont/2/cmm/cmm7.pdf。

[49] 关于该《公约》，见 Smith 著, An International Hit Job: Prosecuting Organized Crime Acts as Crimes Against Humanity, Georgetown Law Journal, 2009 年, Vol. 97, 第 1118 页，可在以下网址查阅： www.georgetownlawjournal.org/issues/pdf/97-4/Smith.PDF。

[50] 《刑事事项互助美洲国家公约》，1992 年，《条约汇编》，美洲国家组织，No. 75。该《公约》的案文以及签署和批准情况一览表可在以下网址查阅：www.oas.org/juridico/english/sigs/a-55.html。

[51] 《欧洲委员会网上犯罪公约》, ETS 185。

[52] 这方面见《联合国刑事事件互助示范条约》，1990 年, 第 45/117 号决议；《联合国打击跨国有组织犯罪公约实施立法指南》，2004 年，第 217 页，可在以下网址查阅：www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf。

合作的第四种来源是国内法，其中可能允许在互利基础上或视具体案件而定进行国际合作。

研究范围

35. 对这一专题的研究将包括以下内容：

(a) 网上犯罪案件侦破行动国际合作上的相关挑战；

(b) 适合网上犯罪侦查和起诉的国际合作规定盘点；

(c) 双边协议中最佳做法实例盘点；

(d) 国际合作破获网上犯罪案例盘点；

(e) “情报共享”等非正式合作手段的作用；

(f) 有关机关目前在国际合作方面的需要的概览。

专题 8. 电子证据

背景

36. 由于越来越多的信息以电子形式储存，电子证据对于网上犯罪侦查和传统侦查工作都有重要意义。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[53]的储存能力不断增大，电子文件储存[54]与纸质文件的储存相比费用低廉，因此数字化文件日渐增多。[55]今天，大量数据仅以数字化形式储存。[56]由于这种增长，文本文件、电子视频和电子图

---

[53] 见 Abramovitch 著, A brief history of hard drive control, Control Systems Magazine, EEE, 2002 年, Vol. 22, Issue 3, 第 28 页及以下; Coughlin/Waid/Porter 著, The Disk Drive, 50 Years of Progress and Technology Innovation, 2005 年，可在以下网址查阅：www.tomcoughlin.com/Techpapers/DISK%20DRIVE%20HISTORY,%20TC%20Edits,%20050504.pdf。

[54] Giordano 著, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006 年, 第 161 页; Willinger/Wilson 著, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law and Technology, 2004 年, Vol. X, No. 5。

[55] Lange/Minster 著, Electronic Evidence and Discovery，2004 年, 6。

[56] Homer 著, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002 年，Vol. 1, No. 1, 第 1 页，可在以下网址查阅：www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf。

片等电子文件[57]正在网上犯罪侦查和相关的法院程序中发挥着作用。[58]

电子证据的作用

37. 电子证据造成了若干难题，有的是在证据收集阶段，有的是在证据采信阶段。[59]在证据收集过程中，侦查人员必须符合某些程序和要求，如为保护证据完整性而需要进行的特别处理。执法机关需要采取具体措施以便成功进行侦查。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，尤其有重要意义。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估数字化证据。[60]

38. 数字化还影响着执法机关和法院处理证据的方式。[61]传统文件在法庭上出示即可，而数字化证据所需的特别程序可能不适合将其转换为传统证据，如文件的打印本。[62]

研究范围

39. 对这一专题的研究将包括以下内容：

(a) 电子证据处理和可采性规定盘点；

---

[57] 关于数字图像的可接受性和可靠性，见 Kwiatkowski 著, Can Juries Really Believe What They See? New Foundational Requirements for the Authentication of Digital Images, Journal of Law and Policy，第 267 页及以下。

[58] Harrington 著, A Methodology for Digital Forensics, T.M. Cooley J. Pac. and Clinical L., 2004 年, Vol. 7, 第 71 页及以下；Casey 著, Digital Evidence and Computer Crime, 2004 年，第 14 页。关于不同国家的法律框架，见 Rohrmann/Neto, Digital Evidence in Brazil, Digital Evidence and Electronic Signature Law Review, 2008 年, No. 5; Wang 著, Electronic Evidence in China, Digital Evidence and Electronic Signature Law Review, 2008 年, No. 5; Bazin 著, Outline of the French Law on Digital Evidence, Digital Evidence and Electronic Signature Law Review, 2008 年, No. 5; Makulilo 著, Admissibility of Computer Evidence in Tanzania, Digital Evidence and Electronic Signature Law Review, 2008 年, No. 5。Winick 著, Search and Seizures of Computers and Computer Data, Harvard Journal of Law and Technology, 1994 年, Vol. 8, No. 1, 第 76 页; Insa 著, Situation Report on the Admissibility of Electronic Evidence in Europe, 载于 Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008 年, 第 213 页。

[59] Casey 著, Digital Evidence and Computer Crime, 2004 年，第 9 页。

[60] 关于确定计算机法医学形式的必要性，见 Leigland/Krings 著, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004 年, Vol. 3, No. 2。

[61] 关于根据传统程序和原则处理数字证据方面的困难，见 Moore 著, To View or not to View: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004 年，第 57 页及以下。

[62] 见 Vacca 著, Computer Forensics, Computer Crime Scene Investigation, 第二版, 2005 年, 第 3 页。关于早期对打印件使用问题进行的讨论，见 Robinson 著, The Admissibility of Computer Printouts under the Business Records Exception in Texas, South Texas Law Journal, Vol. 12, 1970 年，第 291 页及以下。

(b) 英美法系国家和大陆法系国家电子证据处理方法差异进行分析和共同原则鉴别。

专题 9. 互联网服务提供商的赔偿责任

背景

40. 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商的服务：电子邮件服务提供商、接入服务提供商和向收件人转发电子邮件信息的路由网段服务提供商。[63]下载含有儿童色情内容的电影的情形与之类似。下载过程涉及（例如在网站上）上传图片的内容提供商、为网站提供储存器的寄存托管商、向用户转发文件的路由网段服务提供商，最后是用户得以进入互联网的接入服务提供商。

互联网服务提供商的作用

41. 实际上，网上犯罪若无提供商的参与便无法实施，而且提供商往往并无能力预防网上犯罪，因而产生的问题是，是否应当对互联网提供商的责任加以限制。[64]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。

42. 执法机关的努力往往有赖于互联网提供商的合作。这不禁令人关切，因为限制互联网提供商为用户行为而承担的赔偿责任可能会影响到互联网服务提供商对网上犯罪侦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。

研究范围

43. 对这一专题的研究将包括以下内容：

(a) 互联网服务提供商责任规范方法盘点，区分不同类型的互联网服务提供商；

(b) 互联网服务提供商责任限制的概念；

(c) 互联网服务提供商协助执法和预防网上犯罪的能力。

---

[63] 关于网络结构和与服务提供商参与有关的后果，见 Black 著, Internet Architecture: An Introduction to IP Protocols, 2000; Zuckerman/McLaughlin 著, Introduction to Internet Architecture and Institutions, 2003,可在以下网址查阅：http://cyber.law.harvard.edu/digitaldemocracy/internetarchitecture.html。

[64] 对该讨论的介绍见 Elkin-Koren 著, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Vol. 9, 2005 年，第 15 页及以下，可在以下网址查阅: www.law.nyu.edu/journals/legislation/articles/current_ issue/NYL102.pdf。

专题 10. 处理网上犯罪的法律外对策

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全面的办法。

法律外对策

45. 处理网上犯罪的法律外对策包括诸如为侦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，对互联网用户进行教育，以及预防或侦查网上犯罪的技术解决办法。

研究范围

46. 对这一专题的研究将包括以下内容：

(a) 用于应对网上犯罪的法律外办法概览；

(b) 确定这些办法成功与否的衡量手段；

(c) 不同法律外对策之间的关系分析及其结合并用的可能性分析。

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大多是在国家一级制定的。在 1990 年代，区域组织和国际组织开始处理网上犯罪问题，包括通过联合国大会（多年来联合国大会已经通过了关于网上犯罪的若干决议）、[65]英联邦（《网上犯罪示范法》）、欧洲委员会（《网上犯罪公约》）和欧洲联盟（《关于攻击信息系统问题的框架决定》）。

统一各种标准

48. 实践证明，在网络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方法之间的冲突。[66]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。可以在本专题下对现有的各个框架进行研究，以确定其范围、优缺点和可能存在的任何差距。

---

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

[66] 详细情况见 Gercke 著，National, Regional and International Legislative Approaches in the Fight Against Cybercrime, Computer Law Review International，2008 年，第 7 页及以下。

研究范围

49. 对这一专题的研究将包括以下内容：

(a) 区域组织和国际组织最佳做法盘点；

(b) 现有办法的优缺点；

(c) 现有国际法律办法的差距分析。

专题 12. 技术援助

背景

50. 人们有时会认为，网上犯罪这一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。[67]由于打击网上犯罪战略的基本目标之一便是防止用户成为网上犯罪的受害人，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，[68]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，需要所有国家协调行动。防止为网上犯罪分子建立安全庇护所是打击网上犯罪的主要挑战之一。[69]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。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》也体现了这一点，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处理网上犯罪问题。其中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。

---

[67] 见“Development Gateway’s Special Report, Information Society – Next Steps?”，2005 年，可在以下网址查阅：http://topics.developmentgateway.org/special/informationsociety。

[68] “Spam Issue in Developing Countries”, 可在以下网址查阅：www.oecd.org/dataoecd/5/47/34935342.pdf。

[69] 有若干国际组织处理了这一问题。联合国大会第 55/63 号决议规定：“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”。决议全文可在以下网址查阅：www.unodc.org/pdf/crime/a_res_55/res5563e.pdf。《八国首脑会议 10 点行动计划》强调：“决不为滥用信息技术者提供安全庇护所”。

研究范围

52. 对这一专题的研究将包括以下内容：

(a) 确定处理网上犯罪方面的技术援助的基本内容和原则；

(b) 确定在处理网上犯罪方面提供技术援助的最佳做法。

专题 13. 私营部门

背景

53. 防止和侦查网上犯罪取决于若干不同要素。尽管经常强调要确保有适当的立法，但私营业界仍然在预防和协助侦查网上犯罪方面发挥着重要的作用。然而私营业界在网上犯罪侦查工作中的参与往往也伴有若干难题。

业界的作用

54. 业界在处理网上犯罪问题方面的作用是复杂的；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侦查工作。业界采取的自我保护措施通常是综合性企业战略中的合理内容，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。但业界在犯罪侦查中的参与在许多国家造成了难题，对此也采取了各种办法。一些国家允许业界自愿参与犯罪侦查，并为便利业界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，规定业界在法律上有义务与执法机关合作进行犯罪侦查。

研究范围

55. 对这一专题的研究将包括以下内容：

(a) 私营部门预防和侦查网上犯罪的最佳做法盘点；

(b) 分析业界的需要和执法工作的需要；

(c) 现有办法的优缺点评估。