



# 联合国打击跨国有组织犯罪 公约缔约方会议

Distr.: General  
18 August 2015  
Chinese  
Original: English

## 国际合作工作组

2015年10月27日至28日，维也纳

临时议程\*项目2

## 收集和分享电子证据

### 收集和分享电子证据

#### 秘书处编写的背景文件

#### 一、 导言

1. 涉及电子证据的犯罪在国内（立法者、侦查人员、检察官和法官）和国际合作层面上给负责对其作出适当应对的机构带来了独特的挑战。
2. 一般而言，电子证据可以包括每次使用电脑时生成或储存的数字形式的数据。这包括个人人工输入电子设备的信息、计算交易或个人对请求作出回应的过程中生成的信息（在此情况下，电子设备自动生成信息），或设备在总库中处理信息时产生和储存的信息。因此，电子证据系指从数据库、操作系统、应用程序、推断结果的计算机生成的模型、电子和语音邮件信息，甚至是在计算机存储体不常用的指令中获取、生成或保留的信息。<sup>1</sup>
3. 秘书处编写本文件，是为了提供与电子证据相关的关键概念和各方面的背景信息，并协助工作组针对本会议的相关议程项目开展讨论。

#### 二、 收集和分享电子证据：思考的领域和国家及国际上的对策

4. 电子证据的收集和分享密切相关，因此，国家立法以及区域和国际协定或协议往往规定了可以收集电子证据的调查权力和分享电子证据的合作机制。

\* CTOC/COP/WG.3/2015/1。

<sup>1</sup> 爱尔兰法律改革委员会，“书面和电子证据”，磋商文件，2009年12月，第8页。



## A. 收集电子证据

### 1. 国家法律框架

5. 传统的刑事诉讼法通常载列了关于证据的收集和可采用性的条款。对于电子形式的证据而言，计算机数据和电子记录可轻易被篡改。因此在电子证据的收集和处理过程中，从获取证据到审判中使用证据，整个期间都应确保电子证据的完整性、真实性和连续性。

#### (a) 收集和处理电子证据的法定权力

6. 国家调查权在电子证据收集方面发挥了关键作用。毒品和犯罪问题办公室网络犯罪研究称，为了开展有效的调查并收集电子证据，各国可制定程序立法向相关执法机关授权。调查权可包括适用传统程序权、广义上的一般调查权、专门适用于一系列特定网络举措的一般调查权，以及用于取得电子证据的综合调查权。<sup>2</sup>

7. 网络犯罪研究进一步强调，审查对涉及电子证据的犯罪使用调查权的法律基础，结果显示各国做法上差异很大。这些做法首先与“传统”权力可在多大程度上适用于无形数据有关，其次与在多大程度上存在对特别侵入性措施的法定权力有关，例如远程取证调查。

8. 尽管如此，虽然法定权力各有不同，但是为了网络犯罪研究提交报告的各个国家似乎就电子证据收集中能使用的调查措施类型达成了大量共识。此类措施可能包括加速保存计算机数据；储存内容数据命令；存储流量数据命令；用户信息命令；实时收集内容数据；实时收集流量数据；搜索计算机硬件或数据；获取计算机硬件或数据；跨境访问计算机系统或数据；使用远程取证工具。<sup>3</sup>

9. 为了使执法机关有效调查并收集有关网络犯罪的电子证据，过去若干年中各国特别重视与其他相关行动方（包括来自私营部门的行动方）的合作。总之，互联网服务提供商在获取电子证据方面发挥了重要作用。国家隐私法也会影响互联网服务提供商在调查中与相关机构分享信息的能力。例如，各个国家可能限制可获取的数据类型，规定时限，提出“正当理由”要求，并进行起诉和司法监督。<sup>4</sup>由于国家立法对隐私进行保护，互联网服务提供商可能不得泄露关于用户个人信息、内容数据和流量数据的信息。除了国家法律，国际人权法还针对受到执法调查的个人的隐私权制定了专门标准。

---

<sup>2</sup> 毒品和犯罪问题办公室，关于网络犯罪的综合研究：草案——2013年，由毒品和犯罪问题办公室编制并供网络犯罪问题全面研究专家组审议（[www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME\\_STUDY\\_210213.pdf](http://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf)），第5章，第125页。

<sup>3</sup> 可从网络犯罪资料库（<http://cybrepo.unodc.org>）和福尔摩斯刑侦交流站（<http://sherloc.unodc.org>）获取关于这些调查措施的国家法律的实例。

<sup>4</sup> 网络犯罪研究，第5章，第134页。

10. 鉴于互联网服务提供商在收集电子证据方面的重要性，欧洲委员会通过了“执法机构与互联网服务提供商合作打击网络犯罪准则”。准则旨在帮助执法机构和互联网服务提供商在处理网络犯罪问题时，合理地安排其互动结构。准则应是灵活的，可根据国家立法在任何国家适用，并尊重公民的基本权利。除了其他事项以外，还鼓励执法机构和互联网服务提供商参与信息交换；促进合作文化；为相互合作制定书面程序；考虑建立正式伙伴关系；保护公民的基本权利。<sup>5</sup>

## (b) 执法和刑事司法系统处理电子证据方面的能力建设

11. 电子证据本质上十分脆弱。处理或审查不当会导致电子证据的更改、损坏或销毁。因此，记录、收集、保存和审查此类证据时需特别小心。否则可能造成证据无法使用或者导致不准确的结论。

12. 因此，国家执法和刑事司法系统一级的能力建设至关重要。大多数国家已经开始建立专门机构来调查网络犯罪和涉及电子证据的犯罪，但很多国家的这些机构资金不足，而且缺乏能力。由于数字证据越来越多地用于“常规”犯罪的调查工作，执法机构需要明确区分网络犯罪调查人员与数字取证实验室的能力，并为其制定明确的工作流程。工作在第一线的执法人员也越来越需要掌握和利用某些基本技能，例如制作电子存储设备完好取证图像所需的技能。

13. 随着匿名网络等新技术的发展，高级加密和虚拟货币成为涉及电子证据的犯罪中的常见现象，调查人员也必须采用新的战略。例如，执法机构可以设法加强与关注虚拟货币交易的定性和调查等领域的技术方法开发工作的学术研究团体的伙伴关系。<sup>6</sup>调查人员还需要考虑如何将特别调查手段，例如监视、秘密行动、利用线人、以及在网上出售非法货物的案件中实施控制下交货，与互联网调查、数字取证技术结合起来，以收集敏感且脆弱的电子证据。总而言之，随着技术不断飞速发展和犯罪方式不断快速创新，增强执法和刑事司法人员打击网络犯罪和/或涉及电子证据犯罪的能力建设显然会是一项持续不断的工作。<sup>7</sup>

## (c) 专门的网络犯罪机构和部门的作用：国内方法

14. 国家执法机构专门调查网络犯罪和（或）涉及电子证据的犯罪正在变得越来越普遍，这种专门化在推动电子证据的收集、分析和分享方面发挥了关键作用。专门化的主要原因是网络犯罪具有特殊性质，因而在罪行界定、法律适

<sup>5</sup> “执法机构与互联网服务提供商合作打击网络犯罪准则”，见 [www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567\\_prov-d-guidelines\\_provisional2\\_3April2008\\_en.pdf](http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567_prov-d-guidelines_provisional2_3April2008_en.pdf)。

<sup>6</sup> 例如，见 Sarah Meiklejohn 等人，《一把比特币：匿名支付的特点》，载于《2013 年美国计算机协会数据通信专业组关于互联网测算会议的会议记录》（纽约，美国计算机协会，2013 年）

<sup>7</sup> 第十三届联合国预防犯罪和刑事司法大会，秘书处编写的背景文件，题为“讲习班 3：加强针对诸如网络犯罪和文化财产贩运等不断演变的犯罪形式的预防犯罪和刑事司法对策，包括汲取的经验教训和开展国际合作”，A/CONF.222/12，第 37-38 段。

用、证据收集和分析方面提出了特定挑战。因此，执法机构的技术技能和能力水平将直接影响应对网络犯罪的犯罪预防和刑事司法对策的成效。<sup>8</sup>此外，由于日常生活中电子设备、互联网和全球互联日益普遍化，短信、电子邮件和互联网浏览数据等电子证据在许多“常规”刑事调查中已经成为标准做法。<sup>9</sup>因此，也越来越需要各级（无论是地方或国家一级）执法机构拥有至少基本的网络犯罪调查能力。

15. 网络犯罪研究中最常提到的“技术援助干预”领域通常是网络犯罪调查技术领域。在需要援助的国家中，60%的国家表示执法机构需要这些援助。<sup>10</sup>为网络犯罪研究提交报告的国家还指出，在许多情况下，当地警察局将网络犯罪案件移交到专门的国家级执法主管部门。<sup>11</sup>

16. 执法机构内专门的网络犯罪机构或部门可使各国更容易将有限的资源集中到一个地方，以制定专门的调查技术，并充分收集和分析电子证据，包括开展数字取证审查。同时，这些机构或部门可以为当地执法机构提供培训，协调国家应对网络犯罪的办法，促进参与调查的各方的合作，并针对一个国家可能特别关心的网络犯罪形式，如网上虐待儿童行为，与身份相关的犯罪，网络诈骗和欺诈等。

#### (d) 电子证据在法庭上的可采性

17. 一旦收集和分享了电子证据，理想的做法是在刑事诉讼中允许采用这些证据。证据法历来依赖纸质记录，但口头证言和实物也始终在法庭诉讼中使用。但是，电子证据在刑事诉讼中的相关性日益增强，提出了前所未有的挑战，因此网络犯罪研究是一项“绘图工作”，以反映对于此类证据在刑事法庭中的可采性各个国家的法律方法。

18. 在此背景之下，85%的答复国报告称电子证据可在刑事诉讼中采用。更多承认电子证据的国家报告，此类证据与实物证据受到了同等对待。不到40%的国家报告称，法律上区别对待电子证据和实物证据。只有非常少的国家报告称其制定了关于电子证据的特别证据法。对于制定了证据法的国家，这些法律涵盖的领域包括关于电子数据和文件的所有权和著作权的法律假设，还涵盖了电子证据可被认为是真实的情况。<sup>12</sup>

## 2. 国际合作

19. 涉及电子证据的犯罪对国际合作提出了独特挑战。由于电子证据具有易变性，因此，网络犯罪事项上的国际合作需要及时回应，并且能够请求开展专门

<sup>8</sup> 网络犯罪研究，第5章，第152页。

<sup>9</sup> 见上述脚注7，A/CONF.222/12，第16段。

<sup>10</sup> 网络犯罪研究，提要，第xxiii页。

<sup>11</sup> 网络犯罪研究，第5章，第118页。

<sup>12</sup> 网络犯罪研究，第6章，第165-167页。

的侦查行动，包括由私营部门提供商保存和制作数据。向另一个法域请求此类数据时，常见挑战包括延迟回应请求，被请求提供证据的机构缺少承诺和灵活性，提供给请求法域的证据形式，证据是否能用于刑事诉讼，以及各自法域对刑事犯罪的不同定义。<sup>13</sup>

20. 目前虽有一些非正式执法合作模式，包括“24/7”网络，但各国在获取境外电子证据时，仍然严重依赖传统的正式司法途径，特别是双边法律协助工具，70%以上的国家都使用正式双边法律协助请求。<sup>14</sup>针对这类涉及网络犯罪侦查的法律协助请求，做出回应的时长通常约为 150 天。这一时间长度往往会超出服务提供商的数据保留期限，或足以使犯罪者永久性销毁关键的数字证据。

21. 因此，在涉及数字证据的案件中有效开展国际合作需要确立各种机制，以便快速保存数据，然后考虑采取进一步调查措施。就涉及数字证据的案件加强国际合作，还可以借助一些常见方法请求提供特定形式的证据，包括网络证据、链接日志和司法取证图像。

22. 部分现行多边文书建立了旨在协助执法机构获取数据的相关机制，例如网络犯罪调查工作全天候联络点，以及在获得同意或在数据可公开获取的情况下跨境获取存储在计算机中的数据以及提出紧急司法协助请求。

23. 例如，根据《欧洲委员会网络犯罪问题公约》，“24/7”联络点应促进或在国内法律和惯例的允许之下直接开展以下工作：(一)提供技术咨询；(二)保存数据；(三)收集证据、提供法律信息、锁定嫌疑人。

24. 一些国际协定述及与电子证据收集相关的领域。例如，《欧洲委员会网络犯罪问题公约》规定，《公约》所载的程序规定范围应适用于为了收集刑事犯罪的电子证据而行使的权力和采用的程序。

25. 东非和南部非洲共同市场（东南非共同市场）《网络犯罪示范法案草案》（2011 年）中载有关于互联网服务提供商的条款。这些条款包括：监督义务（第 17 条）；自愿提供信息（第 17(b)条）；突然搜查通知（第 16 条）；互联网服务提供商的责任（第 12 条）；缓存（第 13 条）；主机服务（第 14 条）和超链接提供商/搜索引擎（第 15 条）。此外，欧洲联盟第 2000/31/EC 号指令和国际电联/加勒比共同体/加勒比电信联盟(一)《关于网络犯罪/电子犯罪的示范立法文本》以及(二)《电子证据》中都载入了类似条款，但条款数目比东南非共同市场制定的《示范法案》少。

26. 执法机构之间可开展非正式合作，以收集来自其他法域的电子证据。此类合作可促进获取境外证据的各种措施，包括搜索和获取；保存计算机数据，计算机数据指令；实时收集数据；远程取证工具；和执法机构直接获取境外数据。<sup>15</sup>

<sup>13</sup> 毒品和犯罪问题办公室关于对重大有组织犯罪进行调查的现行电子监视做法的比较研究。第 9 页（[www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic\\_surveillance.pdf](http://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf)）。

<sup>14</sup> 网络犯罪研究，提要，第 xxv 页。

<sup>15</sup> 网络犯罪研究，第 5 章，第 126-133 页。

27. 执法机构越来越需要找到具有开拓性的协作方法以开展跨国网络犯罪调查。国际刑警组织全球创新中心<sup>16</sup>和欧洲警察组织欧洲网络犯罪中心<sup>17</sup>等实体参与协调和支持跨国调查工作将在这方面发挥重要作用。其他论坛和举措，例如全球网络空间会议，也为各国提供了机会，以考虑在国际合作打击网络犯罪领域采取创新对策。

28. 云计算也日益对国际合作提出挑战，因为计算机服务日益分布至各地服务器和数据中心，使得难以确定电子证据的位置。<sup>18</sup>例如，谷歌用户可以获取在北美、东南亚或北欧、西欧存储或处理的数据。<sup>19</sup>

## B. 分享电子证据

### 1. 国家法律框架

29. 一些国家已制定国内立法，规定通过国际合作分享证据。例如，许多国家就刑事事项中的互助问题制定了国内立法，这些互助也可用于分享电子证据。

### 2. 国际合作

30. 为了促进各法域之间分享电子证据，各国可达成双边、区域或国际协定。这些协定中可能会载有关于以下内容的条款：协助保存计算机数据；协助获取、访问、收集和披露计算机数据；跨境访问计算机数据；主动提供信息和交换信息；一般司法协助请求。<sup>20</sup>这些协定所载的条款构成了主要法律来源，这些来源涵盖协定各方的权利和义务，并规定各方须遵守有约束力的法律条款。但是，并非所有国家均要求缔结正式的司法合作条约以分享电子证据，而是可能在互惠和礼让的基础上提供协助。

31. 对于区域和国际协定的审查表明各国采取多种形式分享电子证据。此类形式的合作包括：国际合作一般原则；一般司法协助；快速协助机制；协助保存计算机数据；协助获取/访问/收集/披露计算机数据；跨境访问数据；主动提供信息/交换信息。以下协定载列了上文提到的一系列合作形式：

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问题的任择议定书》（2000年）；

独立国家联合体，《合作打击计算机信息领域犯罪协定》（2001年）；

<sup>16</sup> [www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation](http://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation)。

<sup>17</sup> [www.europol.europa.eu/ec3](http://www.europol.europa.eu/ec3)。

<sup>18</sup> 网络犯罪研究，第7章，第216页。

<sup>19</sup> 网络犯罪研究，第7章，第216-217页。

<sup>20</sup> 网络犯罪研究，附件三，第273-274页。

欧洲委员会,《网络犯罪问题公约》和《网络犯罪公约关于宣告利用计算机系统犯下的种族主义和仇外行为为犯罪行为的附加议定书》(2001年);

欧洲委员会,《保护儿童免遭性剥削和性虐待公约》(2007年);

西非国家经济共同体(西非经共体),《西非经共体关于打击网络犯罪问题指令草案》(2009年);

阿拉伯国家联盟,《阿拉伯国家打击信息技术犯罪问题公约》(2010年);

上海合作组织,《国际信息安全领域合作协定》(2010年);东非和南部非洲共同市场(东南非共同市场);

《网络犯罪示范法案草案》(2011年)

非洲联盟,《关于设立一个有助于非洲网络安全的法律框架的公约草案》(2012年)

欧洲联盟,《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》(2001年)

欧洲联盟,《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》(2005年);

欧洲联盟,《欧洲议会和欧洲联盟理事会关于攻击信息系统和取消委员会第2005/222/JHA号框架决定的指令的第COM(2010)517号最终提案》(2010年)。

32. 分享电子证据的主要方法为传统合作,如正式司法协助请求。在解决司法协助程序问题方面存在若干双边、区域和国际协定。上述列举的许多区域和国际网络犯罪文书中都载列了司法协助条款。司法协助程序和请求主要由区域和多边协定决定。有关司法协助的区域协定实例包括东南亚国家联盟(东盟)2004年《刑事事项司法协助条约》和欧洲委员会2000年《关于欧洲联盟成员国之间刑事事项司法协助的欧洲公约》。

33. 鉴于电子证据往往不稳定且易受污染,正式合作机制可能无法始终对此类证据做出及时反应。因此,也可使用非正式合作机制,尤其是“24/7”网络对提高此类非正式合作的效率拥有可观潜力,在以后阶段甚至还能促进正式合作。然而,通过非正式合作采取的侦查行动的可能性大相径庭。通过非正式合作分享电子证据的主要障碍是许多国家禁止在诉讼程序中使用通过非正式机制获得的证据。<sup>21</sup>

34. 利用非正式合作的国家指出,在为编写网络犯罪研究目的提交报告时,相关机制将依赖于是否有一个组织有序的外国同类型机制。各国指出,以某些协定形式开展非正式执法合作时更容易出现此情况。若干国家报告称,通过利用国际和区域组织和机构建立的网络;并在大使馆和领事馆的协助下;同时在执法官员专用网络的支持下,根据区域和双边协定开展非正式合作。

<sup>21</sup> 关于新信息技术对虐待和剥削儿童的影响的研究,第四章第47页(见下文),见 [www.unodc.org/documents/organized-crime/cybercrime/Study\\_on\\_the\\_Effects.pdf](http://www.unodc.org/documents/organized-crime/cybercrime/Study_on_the_Effects.pdf)。

35. 为实现这一目标，《联合国打击跨国有组织犯罪公约》第 27 条包含有关执法合作的条款，并鼓励缔约国考虑加入允许不同执法机构之间合作的双边或多边协定或协议。此外，各国还就执法合作制定了多项法律，包括信息交流、联合侦查、电子或其他形式的监测。

36. 一些国家报告了警方与警方直接合作行动，而其他国家则主要着重通过国际刑警组织渠道展开非正式合作。国际刑警组织在 190 个国家设有国家中心局，经常与国家执法机构进行联系。<sup>22</sup>因此，各国中心局可支持非正式关系，从而提高成功替代正式国际合作程序的可能性。

37. 刑事事项电子证据方面的正式和非正式合作程序面临着一些挑战，这些挑战可能妨碍电子证据的收集与分享。挑战包括多边和双边文书所含合作条款的范围方面存在分歧，缺乏响应时限义务、多重非正式执法网络和合作保障各异。<sup>23</sup>

### 三、联合国毒品和犯罪问题办公室开发的工具。

38. 在过去几年中，毒品和犯罪问题办公室已开发了若干工具，从不同角度、规则和职责方面探讨电子证据主题。就此而言，毒品和犯罪问题办公室的工具包含一种相辅相成的知识范围，而这些知识往往是通过与成员国和利益攸关方开展广泛磋商收集起来的。从对具体犯罪形式的研究型分析到提供直接提供法律资源的电子平台，毒品和犯罪问题办公室的工具就收集和分享电子证据提供了集合多功能的知识工具。

39. 虽然毒品和犯罪问题办公室目前尚无专门针对电子证据的工具，下文概述了毒品和犯罪问题办公室有关讨论主题的指导/研究材料/工具。

#### A. 由联合国毒品和犯罪问题办公室根据联合国决议编写的研究报告

40. 根据经济及社会理事会的相关职责，联合国毒品和犯罪问题办公室在过去几年中启动了下列特别涉及到收集和分享特定犯罪类型的电子证据的研究：(a) 与身份相关犯罪问题手册；<sup>24</sup>和(b)关于新信息技术对虐待和剥削儿童的影响的研究<sup>25</sup>（以下简称为“虐待和剥削儿童问题研究”）。

41. 与此类似，根据大会第 65/230 号和第 67/189 号决议，毒品和犯罪问题办公室为全面研究网络犯罪问题不限成员名额政府间专家组各次会议提供了秘书处和技术支持。因此，毒品和犯罪问题办公室在成员国提供信息的基础上，编写了一份网络犯罪全面研究草案，其在本背景文件的不同部分中被引用为参考材料。

<sup>22</sup> 网络犯罪研究，第 7 章，第 187 页。

<sup>23</sup> 网络犯罪研究，第 7 章，第 197-215 页。

<sup>24</sup> [www.unodc.org/documents/treaties/UNCAC/Publications/Handbook\\_on\\_ID\\_Crime/10-57802\\_ebooke.pdf](http://www.unodc.org/documents/treaties/UNCAC/Publications/Handbook_on_ID_Crime/10-57802_ebooke.pdf)。

<sup>25</sup> 见脚注 21。



## 1. 与身份相关犯罪问题手册

42. 2011 年毒品和犯罪问题办公室根据经济及社会理事会关于国际合作防止、侦查、起诉和惩罚经济诈骗和与身份相关犯罪的第 2007/20 号和 2009/22 号决议发布了该手册，该手册重点关注某些有关与身份相关犯罪有关的法律和政策问题，包括收集和利用电子数据和信息。其主要目标是提出一系列备选办法和考量因素，在解决国内刑事司法问题（犯罪类型/定罪方法/被害人保护）时可加以考虑，并提出刑事事项国际合作领域里的具体挑战或公共和私营部门之间主要在防止与身份有关犯罪领域里潜在的协同增效和合作关系。手册将研究论文和注重实践的材料结合起来，旨在阐明该犯罪形式引发的复杂问题的不同方面和范畴。

43. 由于这些问题的多样性，本手册旨在供以下方面使用：立法者、决策者、检察和执法部门和从业者，以及其他利益攸关方（从事该领域工作的国际和政府间组织的代表、私营部门代表和学术界专家）。

44. 手册也可用作技术援助方案和能力建设活动的参考材料，目的是增加专业知识，以解决作为新型犯罪形式的与身份相关犯罪方面法律、体制和运作问题。

45. 此外，《与身份相关犯罪问题手册》载列的国际合作打击与身份有关犯罪实用指南，概述了与身份有关的犯罪的跨国层面问题，并重点关注包括通过相关案例研究如何最佳地处理此领域里国际合作请求的基本信息和准则。

## 2. 关于新信息技术对虐待和剥削儿童的影响的研究

46. 按照经济及社会理事会题为“预防、保护和开展国际合作，反对使用新信息技术虐待和/或剥削儿童”的第 2011/33 号决议，毒品和犯罪问题办公室于 2015 年发布了一项关于新信息技术对虐待和剥削儿童的影响的研究（最初于 2014 年 5 月在防止犯罪和刑事司法委员会第二十三届会议上发布）。毒品和犯罪问题办公室的研究以关于该问题的公开资料研究和毒品和犯罪问题办公室 2013 年 9 月 23 日至 25 日在维也纳召开的非正式专家小组会议有关此问题的工作为基础，该会议召集了来自国际组织、执法、其他相关从业者和学术界的专家。该研究为下列问题提供了相关背景信息：

- (a) 新出现的定义和条款；
- (b) 犯罪类型；
- (c) 相关行为的最常见类型和形式；
- (d) 助长虐待和剥削儿童犯罪等某些犯罪类型的信息通讯技术的主要形式；
- (e) 罪犯概况和精通技术；
- (f) 受害风险因素；
- (g) 照片、底片、投影片、杂志、书籍、绘画、电影、录像带和计算机硬盘或文件夹等材料的性质；

(h) 用于犯罪目的设备和平台类型，例如：移动电话、远程储存设施（包括内置加密技术）、云计算和阅后即焚与 Wickr 等使用户可发布在接收数秒后即自动销毁的临时图像的新应用程序。

47. 此外，该研究第三章专门阐述侦查信息通信技术协助虐待和剥削儿童的问题。

48. 该研究阐述了与图像有关软件和技术可获得性和实际应用，这些软件和技术使执法机构能够确认和营救在网络材料中被发现的身份不明被害人，并通过将嫌疑人的电子材料和数据库的图像进行比较，对其取证侦查结果进行分类。这针对精简侦查工作的创新技术提供了有利信息，并有利于保护被害人。例如，这包括：

微软公司的“PhotoDNA”：一款用于为电子图像创建类似于指纹的独特签名的免费软件，可与其他图像的签名进行对比，找出该图像的复制件。

含有身份明确和身份不明被害人信息的虐待图像数据库<sup>26</sup>和

国际刑警组织的国际儿童性剥削图像数据库：用于确认和营救原身份不明被害人的数据库，通过使用复杂图像比较软件以发现被害人和地点之间的联系。

49. 互联网服务提供商也使用上述技术创新，用算法找出并移除他们的服务器上的儿童性虐待内容。

50. 此外，该研究对数字取证进行了描述，作为有关恢复和侦查由计算机生成的数字痕迹的法证科学的一个分支。就这点而言，该研究阐明了与犯罪行为有潜在关系的计算机数据和电子通讯的类型，用于归档的可能格式和系统的种类以及数据检测工具。

51. 该研究还述及在取证侦查方面利用“自动搜索”软件。它强调使用该工具可便捷地寻找出现了常用关键词的网站和内容。

52. 该研究进一步探讨过去十年中在开发和部署技术工具和软件方面所取得的进展，这些工具和软件使人们可以在成千上万的不同数据库、财务记录、DNA 样本、声音样本、录像片段、地图、平面图、人工智能报告和社交网络中迅速搜索相关数据。这些工具将相关数据集成一条准确、连贯和有用的轨道，提供概念上的联系分析。

53. 此外，该研究探讨有关网络犯罪的秘密侦查工作的适用性和特殊性。

### 3. 网络犯罪全面研究草案

54. 网络犯罪全面研究草案第 6 章从必须以数字取证方式确认、收集和分析电子证据这一点着手，对电子证据和刑事司法专题进行了阐述。这一章审查了电子证据在刑事审判中的可采用性和应用，并演示了一系列检察方面的挑战将如

<sup>26</sup> 如国际刑警组织和设在美国的国家失踪及被剥削儿童中心设立的数据库。

何影响刑事司法系统的运行。针对已完成的和要求的技術援助活动，它将执法与刑事司法能力需要联系起来。

55. 此外，从执法和国际合作的范围探讨了与电子证据有关的某些方面问题。就此而言，第 5 章（执法与侦查）探讨了以下方面：检测、使用、储藏、保留和保存可作为电子证据的电子数据；实时收集数据；远程取证工具；访问域外数据的直接执法途径；人权和执法侦查与从私人服务提供商获得数据。另一方面，第 7 章（国际合作）涉及到下列问题：云端和服务供应商在数据定位等方面提供域外证据；在收集证据期间访问域外数据；从域外服务提供商获得数据。

## B. 联合国毒品和犯罪问题办公室开发用于技术援助活动的工具

56. 毒品和犯罪问题办公室技术援助方案促进了从执行人员角度开发解决数字证据的实用工具。在此方面，第二届关于分享在有组织犯罪侦查和起诉<sup>27</sup>中请求和提供数字证据做法的区域间会议的与会者为侦查人员和检察官请求外国管辖区提供电子/数字数据/证据制定了一套基本技巧。

57. 这套基本技巧就请求外国管辖区提供电子证据提供了切实建议，包括从公开来源获得电子证据或直接从作为外国互联网服务提供商子公司而在请求国成立或注册的互联网服务提供商处获得；在发送披露消息请求之前，先保存电子证据；如有可能，直接向互联网服务提供商发送请求，并向被请求国的侦查和检察机关发送请求副本；就请求的技术问题向网络犯罪部门咨询。

58. 根据打击有组织犯罪公约缔约方会议第 7/4 号决议，毒品和犯罪问题办公室继续开发国际合作工具，包括司法互助写作工具。在此方面，毒品和犯罪问题办公室已组织若干非正式专家小组会议，审议和讨论该工具的二次开发问题，并审议工具使用的未来方向。

59. 在 2015 年 5 月召开的最后一次专家小组会议期间，与会者商定在重新开发的工具中纳入一个数字证据模块，可协助各国请求与此类证据有关的援助。在此方面，专家分享了各国请求和获得数字证据的经验，包括数字证据范本的可得程度和是否存在描述数字证据的标准化方式。该会议为数字证据模块的可能形式和结构提供了指导，重点关注数字证据的不同类型，如设备数据、网络数据、用户信息和内容数据。司法互助写作工具的二次开发版本将在 2015 年 10 月 22 日至 23 日于维也纳举行的一次新的非正式专家小组会议以后最终确定。

<sup>27</sup> 2014 年 12 月 9 日至 11 日，格鲁吉亚，第比利斯。开发这一工具是毒品和犯罪问题办公室的举措的一部分，该举措的目的是建立并加强来源国、过境国和目的地的检察官和中央主管部门网络，以应对中亚和南高加索的跨国组织犯罪。

## C. 联合国毒品和犯罪问题办公室知识管理平台

### 1. 分享打击犯罪电子资源和法律（福尔摩斯刑侦交流站）

60. 毒品和犯罪问题办公室继续致力于发展福尔摩斯刑侦交流站，这是一个旨在分享有关犯罪的法律资源的知识管理门户。福尔摩斯刑侦交流站主要就不同犯罪类型和相关主题汇编资料，其中包括电子证据资料。截至 2015 年 8 月 18 日，该交流站收集了有关电子证据的 44 项立法制定标准。

### 2. 网络犯罪资源库

61. 除了福尔摩斯刑侦交流站，毒品和犯罪问题办公室还建立了网络犯罪资源库，这是一个收藏法律和所得经验教训的中央数据库，旨在促进继续评估需求和刑事司法能力并提供和协调技术援助。

62. 该资源库于 2015 年启动，根据成员国提供和更新的信息，成为首个收藏网络犯罪和电子证据方面法律、案例和所得经验教训的可用全球工具。该资源库有多重目的，其中包括：使立法者能够在起草有关网络犯罪或电子证据方面法律时利用立法数据库；通过协助执法人员和检察官确认其他成员国适用的网络犯罪立法条款，以促进国际合作；并为用户提供防止、侦查和起诉网络犯罪方面的良好做法实例。并非所有司法互助方面的国家立法均述及或规定了中央主管部门的职能。如果国家立法述及或作出规定，就可能指定一个政府机构作为中央主管部门，提出一份该部门职能清单，并在某些情况下提出保留条款，确认法律并不限制该部门提出或接收请求或通过其他渠道或方式与外国合作的权力。例如，某一欧洲国家的法律援助法规定，中央主管部门应“(1)接收援助请求……；(2)直接或通过[其他]部门执行请求……；(3)转交援助请求；以及(4)翻译相关文件”。

## 四、结论和建议

63. 国际合作工作组不妨建议缔约方会议：

(a) 请秘书处与相关政府间组织合作，并在可得到预算外资金的情况下，编写一本关于收集和分享电子证据的手册；

(b) 请秘书处将电子证据专题主流化，以作为努力升级国际合作工具的其中部分工作；

(c) 请会员国向秘书处通报是否存在专门处理网络犯罪的部门或机构，以便纳入国家主管部门名录。