23 January 2013
Chinese
Original: English

全面研究网上犯罪问题专家组
2013 年 2 月 25 日至 28 日，维也纳

关于网上犯罪问题及会员国、国际社会和私营部门采取的对策的全面研究报告

内容提要

一. 导言

1. 大会第 65/230 号决议请预防犯罪和刑事司法委员会按照《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》第 42 段设立一个不限成员名额政府间专家组，全面研究网上犯罪问题及会员国、国际社会和私营部门采取的对策，包括就国家立法、最佳做法、技术援助和国际合作交流信息，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。[1]此外，大会第 67/189 号决议赞赏地注意到不限成员名额政府间专家组已开展工作，全面研究网上犯罪问题，并鼓励专家组加强努力，以完成工作并在适当时向预防犯罪和刑事司法委员会提出此项研究的结果。

2. 专家组第一次会议于 2011 年 1 月 17 日至 21 日在维也纳举行。在此次会议上，专家组审查并通过了专题集和研究方法。[2]研究方法安排向会员国、政府间组织及来自私营部门和学术机构的代表分发一份调查表。2012 年 2 月至 7 月，联合国毒品和犯罪问题办公室根据商定的方法开展了信息搜集工作。[3]本报告载有秘书处根据所搜集的信息编制的全面研究报告草案的内容提要，供网上犯罪问题政府间专家组第二次会议审议。

---

[1] 大会第 65/230 号决议，附件。

[2] E/CN.15/2011/19。

[3] 收到了 69 个会员国提供的信息，区域分布如下：非洲(11)、美洲(13)、亚洲(19)、欧洲(24)，以及大洋洲(2)。收到了 40 个私营部门组织、17 个学术组织和 11 个政府间组织提供的信息。秘书处还对 500 多份从公开来源获得的文件进行了审查。

V.13-80338 (C) GL 110213 110213

二. 全球连通和网上犯罪

3. 2011 年,全世界至少有 23 亿人使用互联网，相当于人口总数的三分之一以上。在所有互联网用户中，超过 60%来自发展中国家，45%的年龄低于 25 岁。据估计，到 2017 年，移动宽带用户将接近全世界人口总数的 70%。到 2020 年，联网设备（“互联网物件”）数量将超过人口数量达到 6 比 1 之多，这将使当前的互联网概念发生改变。在超级连接的明日世界中，将很难想象“计算机犯罪”乃至可能发生的任何犯罪不涉及与网际协议（IP 协议）连接相关的电子证据。

4. 网上犯罪的“定义”主要依据该术语的用途而定。数目有限的损害计算机数据和系统的保密性、完整性和可用性的行为是网上犯罪的核心。不过，除此之外，还有以谋取个人或经济利益或者造成个人或经济损害为目的的与计算机有关的行为（包括与身份有关的犯罪形式）及与计算机内容有关的行为（均属“网上犯罪”更为广泛的含义范畴），这使得不容易就这一总术语订立法律定义。需要对网上犯罪行为的核心制定某些定义。不过，对于界定专门的调查和国际合作权限范围等其他目的而言，网上犯罪的“定义”并不如此相关，这些领域更多地侧重于任何犯罪的电子证据，而非人为的广义的“网上犯罪”概念。

三. 全球网上犯罪情况

5. 在经济转型和人口变化时期，随着收入差距日趋加大、私营部门支出紧缩及财务周转力下降，许多国家的全球连通程度迅猛提高。在全球一级，对研究作出答复的执法机构认为网上犯罪率日益上升，原因是受利润和私利的驱动，个人和有组织犯罪集团都在寻找新的犯罪机会。据估计，超过 80%的网上犯罪行为起源于某种形式的有组织活动，网上犯罪黑市建立在制作恶意软件、计算机传染、僵尸网络管理、获取个人和金融数据、数据买卖，以及金融信息“套现”这整套流程上。网上犯罪实施者不再需要复杂的技能或技术。特别是发展中国家出现了青年参与计算机有关的金融诈骗行为的亚文化，其中许多青年在青春期后期便开始参与网上犯罪。

6. 在全球范围内，网上犯罪行为的广泛分布涉及金钱驱动的行为、与计算机内容有关的行为，以及损害计算机数据和系统的保密性、完整性和可用性的行为。不过，各国政府和私营部门企业对相关风险和威胁的认知存在差异。目前，警方记录在案的犯罪统计数据对国家一级的政策制定通常都比较重要，但这些统计数据并非进行跨国比较的可靠依据。三分之二的国家认为其警方统计制度不能充分记录网上犯罪情况。警方记录在案的网上犯罪率与一国的发展水平及警方的专业能力相关，而非与基本的犯罪率相关。

7. 受害情况调查是更为可靠的比较依据。这些调查表明，个别网上犯罪的受害率大大高于“常规”犯罪形式。在世界各地的 21 个国家中，因网上信用卡诈骗、身份盗窃、对网络钓鱼企图做出回应及未经授权进入电子邮件账户行为而受害的比率占网民人数的 1-17%不等，而这些国家一般入室盗窃、抢劫和偷车

行为造成的受害率则低于 5%。发展水平较低的国家的受害率更高，这突出表明需要加强这些国家的预防工作。

8. 欧洲的私营部门企业报告，入侵或网络钓鱼导致数据泄漏等行为造成的受害率类似，在 2-16%之间。这些犯罪选择的犯罪工具具有全球影响力，诸如僵尸网络。2011 年，全球 100 余万个独立的 IP 地址在作为僵尸网络的命令和控制服务器运行。互联网内容也是各国政府的一个重要关切。要删除的材料包括儿童色情制品和仇恨言论，而且还包括与诽谤和批评政府及一些情况下提出的人权法忧虑相关的内容。据估计，全球近 24%的互联网流量侵犯版权，非洲、南美及西亚和南亚各国以点对点对等网络方式（P2P）下载共享材料的现象尤为严重。

四. 网上犯罪问题立法

9. 法律措施在防止和打击网上犯罪方面发挥着关键作用。所有方面都需要这些措施，包括刑事定罪、程序权力、管辖权、国际合作及互联网服务提供方的职责和责任方面。在国家一级，现有的及新的（或计划制定的）网上犯罪法律最常涉及刑事定罪问题，这表明主要集中于将核心网上犯罪行为确定为具体犯罪。不过，各国日益认识到需要在其他方面进行立法。与现有的法律相比，新的或计划制定的网上犯罪法更多地涉及调查措施、管辖权、电子证据和国际合作。在全球范围内，不到一半的答复国家认为其刑法和程序法框架充分，但这掩盖了巨大的区域差异。超过三分之二的欧洲国家报告有充分的立法，但非洲、美洲、亚洲和大洋洲的情况却正相反，这些区域超过三分之二的国家认为本国法律只有部分充分或一点都不充分。在报告法律不够充分的国家中，仅有三分之一还表明制定新的法律或计划制定法律，因此突出表明急需加强这些区域的立法。

10. 过去十年，在颁布旨在打击网上犯罪的国际和区域文书方面有了重大发展。这些文书包括具有约束力的文书和不具约束力的文书。可将这些文书分为五组，其中包括以下列组织为背景或受其启发而制定的文书：㈠欧洲委员会或欧洲联盟，㈡独立国家共同体或上海合作组织，㈢非洲政府间组织，㈣阿拉伯国家联盟，以及㈤联合国。所有文书间存在大量互补成份，包括特别是《欧洲委员会网上犯罪问题公约》中制定的概念和方法。对 19 份与网上犯罪相关的多边文书条款的分析表明有共同的核心条款，但也表明涉及的实质性领域存在巨大差异。

11. 在全球范围内，82 个国家已签署和（或）批准一份具有约束力的网上犯罪问题文书。[4]除正式加入和实施以外，网上犯罪问题多边文书还通过被非缔约国用作范本或通过缔约国的立法影响其他国家，对国家的法律有着间接影响。加入一份网上犯罪问题多边文书的做法与提高国家刑法和程序法的充分性的观点

[4] 《欧洲委员会网上犯罪问题公约》、《阿拉伯国家联盟打击信息技术犯罪公约》、《独立国家联合体打击计算机信息领域犯罪的合作协定》，或者《上海合作组织国际信息安全领域的协议》，其中的一份或多份。

相符合，这表明这些方面现有的多边条款被普遍认为有效。对于 40 多个提供信息的国家而言，《欧洲委员会网上犯罪问题公约》是制定网上犯罪问题立法最常用的多边文书。总的说来，约一半国家使用其他“集团组”的多边文书。

12. 总体而言，三分之一的答复国报告，其立法与认定的国际合作重要伙伴国的立法高度统一或极为统一。不过，这种情况因区域而异，美洲和欧洲报告的统一程度较高。原因可能是一些区域使用多边文书，这些文书本身意在对统一方面发挥一定作用。在已进行刑事定罪的网上犯罪、管辖权依据和合作机制方面，国际一级的不成体系和国家法律多种多样可能与存在多种具有不同主题和地域范围的网上犯罪问题文书有关。各项文书和各区域目前都反映出法律和宪法根本上的不同导致存在差异，包括权利和隐私概念的不同。

五. 刑事定罪

13. 通过研究调查表，并通过对秘书处收集的现有立法的主要来源分析，搜集了与网上犯罪有关的刑法信息。[5]研究调查表提及了网上犯罪概念通常包含的 14 种行为。[6]答复国指出已对上述 14 种行为进行普遍刑事定罪，但垃圾邮件犯罪以及某种程度上与计算机滥用工具、种族主义和仇外心理及网上教唆或“诱骗”儿童有关的犯罪基本除外。这表明已对应惩处的网上犯罪行为达成基本共识。各国报告了调查表未提及的少数其他犯罪。这些犯罪大部分涉及计算机内容，包括对淫秽材料、网上赌博及网上非法市场（诸如毒品和人口市场）的刑事定罪。就 14 种行为而言，各国报告，对损害计算机系统的保密性、完整性和可用性的网上犯罪核心行为采用专门的网上犯罪。更常对其他网上犯罪形式采用一般性（非专门的网络）犯罪。不过，对于涉及侵犯隐私、诈骗或伪造及身份犯罪的与计算机有关的行为而言，这两种方法都采用。

14. 已就刑事定罪的主要方面取得高度共识，但对信息源立法条款的详细分析表明方法并不相同。按犯罪对象（数据、系统或信息）、对“仅仅”进入行为的刑事定罪或造成损失或损害等进一步意图的要求上的区别，涉及非法进入计算机系统及非法获取数据的犯罪各有不同。犯罪的必要意图也因对干扰计算机系统或数据行为进行刑事定罪的方法的不同而异。多数国家要求干扰必须是有意的，而其他国家却包括随意的干扰。就干扰计算机数据而言，构成干扰行为的范围包括损坏或删除数据，以及修改、封锁、输入或传送数据。对非法截取的刑事定罪的不同之处在于这一犯罪是否限于非公开数据的传送，以及该犯罪是否限于通过“技术手段”进行的截取。并非所有国家都对计算机滥用工具行为

[5] 对 97 个会员国的立法进行了主要来源分析，其中包括对调查表作出了答复的 56 个国家，区域分布如下：非洲(15)、美洲(22)、亚洲(24)、欧洲(30)及大洋洲(6)。

[6] 非法进入计算机系统；非法获取、截取或获得计算机数据；非法干扰数据或系统；制作、散发或持有计算机滥用工具；违反隐私或数据保护措施；与计算机有关的诈骗或伪造；与计算机有关的身份犯罪；与计算机有关的版权和商标犯罪；与计算机有关的造成人身伤害的行为；与计算机有关的涉及种族主义和仇外心理的行为；与计算机有关的制作、散发或持有儿童色情制品的行为；与计算机有关的教唆或“诱骗”儿童的行为；以及与计算机有关的支持恐怖主义犯罪的行为。

进行刑事定罪。对进行定罪的国家而言，在该犯罪是否涵盖持有、传播或使用软件（诸如恶意软件）和（或）计算机访问码（诸如受害人密码）问题上存在着差异。从国际合作的角度来看，这些差异可能对各国间两国公认犯罪的认定有着影响。

15. 若干国家对与计算机有关的诈骗、伪造和身份犯罪采用专门的网上犯罪。其他国家采用关于诈骗和盗窃的一般性条款，或依据涵盖相关构成要素——诸如身份犯罪情况下的非法进入、数据干扰和伪造——的犯罪。答复者表明已对一些与内容有关的犯罪进行普遍刑事定罪，特别是涉及儿童色情制品的犯罪。不过，在“儿童”的定义、与“视频”材料相关的限制或模拟材料的排除及所涵盖的行为方面存在差异。例如，虽然绝大多数国家涵盖制作和传播儿童色情制品的行为，但对持有和获取的刑事定罪却存在较大的差异。就与计算机有关的版权和商标侵权行为而言，各国最经常报告对有意和以商业规模实施的行为适用一般性刑事犯罪。

16. 对社交媒体及用户生成的互联网内容的使用越来越多促使各国政府在监管上做出了应对，包括通过刑法，这种情况还要求尊重言论自由权利。答复国报告言论的范围各不相同，其中包括与诽谤、藐视、威胁、煽动仇恨、侮辱宗教感情、淫秽材料及危害国家相关的言论。对社会文化要素的一些限制不仅载于国家法律，而且还载于多边文书中。例如，一些区域网上犯罪问题文书载有涉及违反公共道德、色情材料及违反宗教或者家庭原则或价值观的广泛罪行。

17. 国际人权法既是矛，又是盾，要求对（有限的）极端形式言论进行刑事定罪，而同时保护其他言论形式。因此，加入相关国际人权法文书的国家须对言论自由实行一些限制，其中包括煽动灭绝种族的言论、构成煽动歧视、敌对或暴力的仇恨言论、煽动恐怖主义的言论及为战争宣传的言论。对其他国家而言，“判断限度”为各国根据本国文化和法律传统确定可接受的言论范围留有回旋空间。然而，国际人权法在一定的时候将会介入。例如，如何证明各项措施相称、适当和达到尽可能最低限度的干预，对网上言论适用的关于诽谤、不尊重当局和侮辱行为的刑法将面临很高的门槛。如若某一内容在一国是非法内容，但其制作和传播在另一国合法，这种情况下，各国需将刑事司法应对的重点放在本国法域内获取该内容的人员上，而非放在境外制作的内容上。

六. 执法和调查

18. 超过 90%的答复国报告，引起执法机关注意网上犯罪行为的最常见方式是受害个人或受害公司的举报。答复国估计向警方举报的实际网上犯罪受害案比例在 1%以上。一项全球私营部门调查显示，约 80%的核心网上犯罪受害者未向警方举报此罪行。导致少报的原因是对受害行为和举报机制缺乏认识、受害人感到羞耻和难堪，以及公司认为信誉会受损。世界各区域当局着重介绍了增加举报的各项举措，包括设立网上和热线举报制度，开展公共宣传运动，建立私营部门联络处，以及加强警方的外联和信息共享。不过，必须对由事件驱动的对网上犯罪的应对辅以重点关注犯罪市场和犯罪阴谋策划者的中长期策略调查。发达国家的执法机关开展了这方面的工作，包括通过把涉及社交网站、聊

天室及即时通讯和点对点服务的罪犯作为打击目标的特工部门。罪犯的犯罪手法翻新、难以获得电子证据及内部资源，以及能力和后勤方面受到限制，这些给网上犯罪调查带来了挑战。嫌疑人通常利用匿名和混淆技术，新的伎俩通过网上犯罪市场迅速深入广泛的犯罪分子中间。

19. 要开展网上犯罪执法调查，则须将传统的执法技术与新的技术相结合。虽然可以利用传统权力开展某些调查活动，但许多程序条款没有从着重于空间和对象的方法很好地转化为涉及电子数据储存和实时数据流通的方法。研究调查表提及了 10 项网上犯罪调查措施，包括一般性搜查和扣押及特别权限，诸如保存计算机数据。[7]各国最常报告的是所有调查措施都具有一般性（非专门的网络）权限。一些国家也报告了专门的网络立法，特别是确保快速保存计算机数据和获得储存的用户数据的立法。许多国家报告关于先进技术的措施没有法律授权，诸如远程计算机取证。虽然可将传统的程序权限适用于网络的情况，但在许多情况下，这种做法还会在证据收集方法的合法性及由此产生的证据是否可采信方面，造成法律不确定性并带来挑战。总之，各国关于网上犯罪调查权限的做法，相对于许多网上犯罪行为的刑事定罪而言，所表现出的核心共同点少些。

20. 不论调查权限的法律形式为何，所有答复机关均使用搜查和扣押方法，收用该计算机设备并获得计算机数据。绝大多数国家还通过命令获得互联网服务提供方储存的计算机数据。不过，在欧洲以外的区域，约三分之一的国家报告调查期间在迫使第三方提供信息方面遇到了挑战。约四分之三的国家采用专门的调查措施，诸如实时收集数据，或者快速保存数据。采用调查措施一般需要至少有初步的证据或网上犯罪行为举报。要采用涉及实时收集数据或获取数据内容等干预性较强的措施，通常需满足更高的门槛，诸如有严重行为的证据，或者表明可能的原因或合理理由。

21. 执法机构与互联网服务提供方之间的互动尤为复杂。服务提供方持有用户信息、收款账单、一些连接日志、位置信息（诸如移动服务提供商的信号塔数据），以及通信内容，所有这些信息都能够成为犯罪的关键电子证据。国家法律义务及私营部门的数据保留和披露政策因国家、行业和数据类型的不同而迥异。各国最常报告的是通过法院命令从服务提供方获得证据。不过，在一些情况下，执法机构可能能够直接获得所储存的用户数据、流量数据以及甚至是内容数据。在这方面，私营部门组织通常报告，实行的基本政策是，要求数据的披露必须遵守适当的法律程序，但也有在一些情形下自愿遵守直接执法请求的情况。超过半数的答复国报告执法机构与服务提供方之间已建立非正式关系，这种关系有助于信息交流和建立信任的过程。答复表明，需要对隐私和适当程序与及时披露证据加以平衡，以确保私营部门不会成为调查的一个“障碍”。

---

[7] 搜查计算机硬件或数据；扣押计算机硬件或数据；提供用户信息的命令；提供所储存流量数据的命令；提供所储存的内容数据的命令；实时收集流量数据；实际收集内容数据；快速保存计算机数据；利用远程取证工具；以及跨界进入计算机系统或获取计算机数据。

22. 网上犯罪调查始终应考虑到国际人权法规定的隐私问题。人权标准明确指出，法律必须足够明确，使能够适当表明主管机关在何种情形下有权采取调查措施，并明确指出必须适当且有效地保证防止滥用。各国报告，国家法律保护隐私权利，并报告对调查有一系列的限制和保障措施。不过，在跨国调查时，保护程度上的差异会在外国执法机构获取数据方面引起无法预测的情况，并可能导致隐私保护制度出现管辖权漏洞。

23. 在对调查作出答复的国家中，约 90%已开始建立调查网上犯罪及涉及电子证据犯罪的专门机构。不过，在发展中国家，此方面没有足够的资源并且面临能力不足的问题。发展水平较低的国家专业警察的人数明显较少，每 100,000 名国内互联网用户中约 0.2 人。在较为发达的国家，这一比率要高出二至五倍。据报告，较不发达国家 70%的专业执法官员缺乏计算机技能和设备，只有半数官员每年接受一次以上的培训。非洲超过一半的答复国及美洲三分之一的答复国报告调查网上犯罪的执法资源不足。在全球范围内，这一情况可能更为糟糕。例如，在全世界 50 个最不发达国家中，研究仅从 20%的国家收到了答复。非洲所有的答复国及美洲、亚洲和大洋洲 80%的答复国报告需获得技术援助。最常提到的需要技术援助的领域是一般性网上犯罪调查技术。在需要援助的国家中，60%的国家表明执法机构需要这些援助。

七. 电子证据和刑事司法对策

24. 证据是确定受审人员有罪或无罪相关事实的工具。电子证据系指以电子或数字形式存在的所有此类材料。此类证据可以储存或瞬时即逝。它能够以计算机文件、传送数据、日志、原数据或网络数据的形式存在。数字取证涉及恢复可能具有证据价值——通常具有不稳定性且容易被篡改——的信息。取证技术包括“逐点”创建所储存和所删除信息分毫不差的副本、“封阻续写功能”以确保原始信息不被更改，以及加密文档“混列码”，或称数字签名，从而能够显示信息的改动。几乎所有国家都报告拥有一些数字取证能力。不过，各区域的多个答复国都指出取证的鉴定人员不够，联邦和州一级的能力存在差异、缺乏取证工具，以及需要分析的数据量庞大而出现积压。一半国家报告嫌疑人利用加密技术，这导致没有解密密钥便很难获取此类证据而且非常费时。多数国家由执法机关承担分析电子证据的任务。不过，检察官必须查看并了解电子证据，以构筑对所审案件的完整理解。非洲所有国家及其他区域三分之一的国家报告，检察官没有开展此项工作的足够资源。检察机关的计算机技能一般都低于侦查人员的技能。在全球范围内，约 65%的答复国报告有某种形式的关于起诉网上犯罪的专门分工。只有 10%的国家报告有专门的司法机关。绝大多数网上犯罪案件由非专业法官审理，在 40%的答复国中，这些法官没有受过任何种类的网上犯罪相关培训。开展与网上犯罪法、证据收集及基础和高级计算机知识相关的司法培训是一个特别优先的事项。

25. 超过 60%的答复国未在法律上对电子证据与物证作任何区分。虽然方法各不相同，但许多国家认为这是一项良好做法，因为它能够确保与所有其他类型的证据一并予以公平采信。欧洲以外的一些国家根本不承认电子证据，这使得无法起诉网上犯罪以及以电子信息为证据的其他犯罪。虽然各国普遍没有关于

电子证据的单独证据规则，但一些国家以下列原则为准，例如：最佳证据规则、证据相关性、传闻证据规则、真实性原则，以及完整性原则，所有这些原则都可能对电子证据特别适用。许多国家着重介绍了指认这些行为归咎于具体个人时所面临的挑战，并评论说这通常取决于旁证。

26. 执法调查人员和检察官面临的挑战意味着网上犯罪的罪犯“绳之以法”的比率很低。在警方记录在案的儿童色情制品犯罪中，查明嫌疑人的情况与其他性犯罪的情况相似。不过，在因非法进入计算机及与计算机有关的诈骗或伪造等行为而被记录在案的犯罪案件中，查明嫌疑人的情况在 100 起犯罪中只占约 25%。极少数国家能够提供关于被起诉者或被判刑人员的数据。不过，对一国网上犯罪罪行的计算表明，被判刑人员与记录在案的罪案之比大大低于其他“传统”犯罪案件的比例。

八. 国际合作

27. 对研究报告调查表作出答复的国家称，30-70%的网上犯罪行为具有跨国性，因此涉及跨国调查、主权、管辖权、域外证据及须开展国际合作的问题。如果犯罪的要素或实质性影响发生在另一国领土内，或者犯罪的部分作案手法是在另一国境内实施的，网上犯罪便具有了跨国性质。国际法对此类行为规定了一些管辖权依据，其中包括属地管辖权形式和属人管辖权形式。其中一些准据原则也载于网上犯罪问题多边文书。虽然欧洲所有国家都认为，国家法律为将域外网上犯罪行为进行刑事定罪并予以起诉提供了充分的框架，但世界其他区域约三分之一到一半的国家报告本国框架不够充分。在许多国家，法规条款反映的观念是，无需“全部”犯罪在本国境内发生即可认定属地管辖权。属地联系的认定可参照行为的要素或影响，或者犯罪所用计算机系统或数据的位置。如果产生了管辖权冲突，一般通过各国间的正式和非正式协商解决。国别答复表明，目前没有任何必要对推定的“网络空间”领域确定其他形式的管辖权。而且，属地管辖权形式和属人管辖权形式几乎总能确保网上犯罪至少与一个国家有充分的关系。

28. 国际合作形式包括引渡、司法协助、互相承认外国判决，以及警方与警方的非正式接触。由于电子证据易于消失的性质，因此要在网上犯罪方面开展刑事事项上的国际合作，则须获得及时回应，并有能力请求开展专门的调查行动，诸如保存计算机数据。在网上犯罪案件中，主要利用传统形式的合作获取域外证据，超过 70%的国家报告为此使用正式司法协助请求。在此类正式合作中，近 60%的请求将双边文书作为法律依据。20%的案件将多边文书作为法律依据。据报告，对引渡和司法协助请求这些正式机制作出回应的时间约为数月，这一时限给收集易于消失的电子证据带来了挑战。60%的非洲、美洲和欧洲国家及 20%的亚洲和大洋洲国家报告已有处理紧急请求的渠道。不过，尚不清楚这些渠道对回应时间的作用。虽然各国很少有关于使用非正式合作机制的政策，但对于约三分之二的报告国，可以采用这种合作模式。非正式合作及便利非正式合作的各项举措，诸如“昼夜服务”网络，在缩短回应时间方面具有重要的潜在作用。不过，这些举措未得到充分利用，其处理的案件数量占报告国家组执法机构遇到的网上犯罪案件总数的约 3%。

29. 正式和非正式合作模式的目的是管理由国家表示同意开展影响该国主权的外国执法调查的过程。不过，在搜集证据期间，调查人员未经证据实际所在国同意而知情或不知情地获取域外数据的情况越来越多。云计算技术尤其会造成这种状况，因为该技术在位于不同地理位置的多个数据中心储存数据。尽管在技术上可知，但数据“位置”正日趋人为化，以至甚至将通常向服务提供方所在国而非数据中心实际所在国发送传统司法协助请求。外国执法机构可在调查人员利用来自嫌疑人设备的现有实时连接或利用合法获取的数据访问凭证的情况下直接获取域外数据。虽然服务提供方通常须遵守适当的法律程序，但执法调查人员有时可能通过非正式直接请求从域外服务提供方获取信息。《欧洲委员会网上犯罪问题公约》及《阿拉伯国家联盟信息技术犯罪问题公约》所载的现有关于“跨界”获取的相关条款没有适当涵盖此类情况，原因是其侧重于是否获得具有数据披露合法权限的人员的“同意”，以及假定在获取或接受时知悉数据的位置。

30. 目前的国际合作形势有可能导致出现一类国家群体，这类国家拥有在其自身间开展合作的必要权力和程序，但对所有其他国家仅限于未能顾及电子证据特性及网上犯罪全球性的“传统”国际合作形式。调查行动方面的合作情况尤其如此。缺少共同的方法，包括在现有网上犯罪问题多边文书范围内缺少这种方法，意味着可能很难满足各种行动请求，诸如在负有国际义务确保有这一设施并应请求予以提供的这些国家外，快速保存数据。在《非洲联盟网络安全公约》草案中纳入这一权力可能在某种程度上有助于弥补这一空白。在全球范围内，多边和双边文书合作条款的范围不同，缺少与回应时间相关的义务，没有就可允许直接获取域外数据的情况达成一致，非正式执法网络很多，以及合作保障措施存在差异，这些给刑事事项上电子证据方面的有效合作带来了重大挑战。

九. 预防网上犯罪

31. 预防犯罪包括谋求降低犯罪发生的风险及减轻其可能对个人和社会造成的有害影响的各种战略和措施。近 40%的答复国报告有关于预防网上犯罪的国家法律或政策。还有 20%的国家报告正在编制相关举措。各国强调，预防网上犯罪的良好做法包括颁布立法，进行有效领导，发展刑事司法和执法能力，开展教育和宣传，开发一个强大的知识库，以及在政府、社区、私营部门和国际范围内开展合作。超过一半的国家报告有网上犯罪问题战略。在许多情况下，网上犯罪问题战略与网络安全战略紧密地结合在一起。报告的约 70%的国家战略包括与提高认识、国际合作和执法能力相关的内容。为进行协调，最常报告由执法机构和检察机构担当打击网上犯罪的主要机构。

32. 包括发展中国家的调查在内的相关调查表明，目前个人互联网用户大都采取基本的安全防范措施。作出答复的国家政府、私营部门实体及学术机构强调提高公众认识运动依然重要，其中包括认清新出现威胁的广泛运动及面向儿童等具体人群的运动。在同有助于用户以安全方式实现其目标的系统相结合时，对用户开展教育的活动最为有效。如果用户的使用成本高于其直接的获益，他们便没有多少遵循安全措施的动力。私营部门实体还报告，必须在全面的安全

方法中纳入提高用户和雇员认识的部分。提及的基本原则和良好做法包括承担在宣传、风险管理政策和做法、董事会指导运营及员工培训方面采取行动的责任。三分之二的私营部门答复者开展了网上犯罪评估，它们大都报告使用防火墙、数字证据保存、内容识别、入侵检测及系统监督和监测等网络安全技术。不过，答复者表示关切的是中小企业要么不采取足够措施保护系统，要么错误地认为它们不会成为犯罪的目标。

33. 对于整个私营部门特别是服务供应方而言，监管框架在预防网上犯罪方面发挥着重要作用。近一半国家已通过数据保护法，这些法律对保护和使用个人数据做了具体要求。一些制度载有针对互联网服务提供方和其他电子通信提供方的具体要求。虽然数据保护法要求删除不再需要的个人数据，但一些国家对刑事调查目的的情况做例外处理，要求互联网服务提供方将特定类型的数据储存一段时间。许多发达国家还出台规则，要求相关组织通知个人和监管人员数据泄漏情况。互联网服务提供方一般承担仅作为数据“中转站”的有限责任。所传送内容被更改会增加其责任，这与实际知悉或推定知悉非法活动的情况相同。另一方面，通知后迅速采取行动会减少其责任。虽然服务提供方有过滤互联网内容的技术可能性，但对接入互联网的限制须遵守关于保护查找、接受和传递信息的权利的国际人权法中对可预见性和相称性的要求。

34. 公私伙伴关系对预防网上犯罪非常关键。超过一半的国家报告建立了伙伴关系。根据非正式协定建立的伙伴关系数量与根据法律依据建立的数量相同。建立伙伴关系最多的是私营部门实体，其次是学术机构，以及国际组织和区域组织。大都通过伙伴关系便利交流关于威胁和趋势的信息，而且还通过这种关系开展预防活动及具体案件中的活动。在一些公私伙伴关系背景下，私营部门实体采取积极主动的方法调查网上犯罪活动，以及开展打击此类活动的法律行动。这些活动补充了执法机构的活动，并能够帮助减轻对受害人造成的伤害。学术机构通过向专业人员提供教育和培训，制定法律和政策，以及开展制定技术标准和解决方法的工作等方式，在预防网上犯罪方面发挥着各种作用。大学拥有网上犯罪问题专家、一些计算机应急系统及专门研究中心，并为其开展工作提供便利。

十. 主要结论和备选方案

35. 网上犯罪问题全面研究的主要结论是：

(a) 国际上分散不一和各国网上犯罪问题法律多种多样可能与存在多种具有不同主题和地域范围的网上犯罪问题文书有关。虽然这些文书合理反映了社会文化及区域差异，但司法程序权及国际合作条款范围的不同可能导致出现国家合作“群类”，这种情况通常并不十分适合网上犯罪的全球特点。

(b) 在网上犯罪事项上依赖传统的正式国际合作方式目前并不能对获取而消失的电子证据作出所需的及时回应。随着涉及地理广为分布的电子证据的犯罪日益增多，这不仅会成为打击网上犯罪要面对的一个问题，而且也会成为打击所有犯罪要面对的一个问题。

(c) 在云计算和数据中心的世界里， 需要重新思考证据“所在地”作用的概念，其目的包括在与执法机关直接获取域外数据相关的问题上达成共识。

(d) 对现有各国法律框架的分析表明，关于“核心”网上犯罪罪行、调查权及电子证据是否可采信这些问题上，没有足够的统一。国际人权法是刑事定罪和程序条款一个重要的外部基准参照点。

(e) 发展中国家的执法机关、检察官及司法机构在调查和打击网上犯罪方面需要获得长期、可持续和全面的技术支持和援助。

(f) 需通过采用一种整体方法加强所有国家的网上犯罪预防活动，涵盖进一步提高认识，建立公私伙伴关系，以及将网上犯罪问题战略与更为广泛的网络安全观念相结合。

36. 为加强现有并提出新的国家和国际应对网上犯罪的法律和其他对策，备选方案可以包括以下一项或多项内容：

(a) 制定对核心网上犯罪行为实行刑事定罪的国际示范条款，以通过采用共同的犯罪要件支持各国消除安全庇护所。

㈠ 这些条款可以保留现有文书中与损害计算机数据和系统的保密性、完整性和可用性的犯罪有关的做法。

㈡ 这些条款还可以涵盖利用计算机系统实施或便利其实施的“传统”犯罪，但前提只能是认为现有的刑事定罪做法不充分。

㈢ 这些条款可以涉及现有文书没有涵盖的方面，诸如对垃圾邮件行为的刑事定罪。

㈣ 可以根据关于刑事定罪的最新国际人权标准制定这些条款，这些标准尤其包括基于条约的言论自由权利保护。

㈤ 各国采用这些条款将最大限度地减少国际合作方面与两国共认犯罪相关的难题。

(b) 制定与电子证据调查权相关的国际示范条款，以支持各国确保有必要的程序工具，调查涉及电子证据的犯罪。

㈠ 这些条款可以借鉴现有文书的做法，包括下令迅速保存数据的做法，以及下令获取储存的数据和实时数据的做法。

㈡ 这些条款可以就搜查和扣押等传统权力范围扩大到电子证据方面提供指导。

㈢ 这些条款可以就基于国际人权法对干预性调查技术适用适当的保障措施，包括基于条约的隐私权保护而提供指导。

(c) 制定关于管辖权的示范条款，以便为网上犯罪刑事事项管辖权提供共同的有效依据。

㈠ 这些条款可以包括例如源自客观属地原则和实质性影响规则的司法依据等。

㈡ 这些条款可以为解决共同管辖权问题提供指导。

(d) 根据《第十三届预防犯罪和刑事司法大会讨论指南》中的建议，制定关于电子证据相关国际合作的示范条款，供纳入双边或多边文书，包括经修订的《联合国司法协助示范条约》。

㈠ 这些条款将侧重于能被纳入现有文书的实际合作机制，以便及时保存和提供刑事事项的电子证据。

㈡ 这些条款可以包括确立义务，建立电子证据快速回应联络点和商定的回应时限。

(e) 制定一份关于刑事事项电子证据方面国际合作的多边文书，以期为及时合作保存和获取电子证据提供国际机制。

㈠ 作为对现有国际合作条约的补充，这一文书可以把重点主要放在关于数据迅速保存一段特定期限的请求机制上。

㈡ 该文书还可能载有促进采取进一步调查措施的具体合作条款，其中包括提供储存的数据和实时收集数据。

㈢ 将需要界定适用的范围，但其范围不应限于“网上犯罪”或“与计算机相关的”犯罪。

㈣ 该文书可以要求在特定期限内作出回应，并在现有的“昼夜服务”举措基础上而不是重复工作，建立明确的联络点对联络点沟通渠道。

㈤ 该文书可以载有传统的国际合作保障措施，以及适当的人权除外措施。

(f) 制定网上犯罪问题的综合多边文书，以在刑事定罪、司法程序权、管辖权和国际合作方面制定国际方法。

㈠ 该文书可以采用具有约束力的多边形式包括上述所有备选方案的内容。

㈡ 该文书可以借鉴目前一系列具有约束力和不具约束力的国际和区域文书中现有各项关键共同点。

(g) 加强国际、区域和国家伙伴关系，包括与私营部门和学术机构的伙伴关系，以便为发展中国家的预防和打击网上犯罪工作提供进一步技术援助。

㈠ 可以根据通过上述备选方案所述示范条款制定的标准提供技术援助。

㈡ 可以通过重点由包括私营部门和学术界代表在内的多边利益相关方来提供技术援助。