联合国 E/CN.15/2018/6

经济及社会理事会

Distr.: General
22February 2018
Chinese
Original: English

预防犯罪和刑事司法委员会
第二十七届会议
2018 年 5 月 14 日至 18 日，维也纳
临时议程*项目 5
专题讨论：采取刑事司法对策预防和打击一切形式的网络犯罪，途径包括加强国家和国际一级的合作

“采取刑事司法对策预防和打击一切形式的网络犯罪，途径包括加强国家和国际一级的合作”专题讨论指南

秘书处的说明

摘要

“采取刑事司法对策预防和打击一切形式的网络犯罪，途径包括加强国家和国际一级的合作”专题讨论将在预防犯罪和刑事司法委员会第二十七届会议上举行，关于该专题讨论的本指南系由秘书处根据委员会第 18/1 号决定编写。经济及社会理事会在其第 2016/241 号决定中决定，委员会第二十七届会议的突出主题是“采取刑事司法对策预防和打击一切形式的网络犯罪，途径包括加强国家和国际一级的合作”。在本说明中，就供专题讨论的相关专题领域提出了一系列问题，为形成讨论框架列出了一些议题，并提供了相关背景资料。

* E/CN.15/2018/1。

一. 导言

1. 经济及社会理事会在其第 2016/241 号决定中决定，预防犯罪和刑事司法委员会第二十七届会议的突出主题为“采取刑事司法对策预防和打击一切形式的网络犯罪，途径包括加强国家和国际一级的合作。”

2. 在 2017 年 12 月 7 日和 8 日举行的第二十六届会议续会上，委员会核可了主席有关第二十七届会议专题讨论的组织办法的建议，即：专题辩论将在一次上午和一次下午会议期间进行。上午的辩论将专门讨论分专题“当前的挑战”，下午的辩论将专门讨论分专题“可能采取的应对措施”。

3. 本说明由秘书处根据委员会题为“预防犯罪和刑事司法委员会专题讨论的准则”的第 18/1 号决定编写而成，在该决定中，委员会决定，关于突出主题的讨论将以一份讨论指南为基础，其中包括一份有待与会者述及的问题清单。

二. 背景资料：为专题讨论做好准备

4. 互联网和计算机技术的快速发展改变了世界各地的社会，同时也给犯罪创造了新的机会。计算机、网络和数据可以以几乎任何能够想到的方式与各种形式的犯罪联系起来。它们同时成为犯罪目标和犯罪工具，并为犯罪扩张创造了新的动机和机会。它们往往降低犯罪分子牟取利益的风险。另外，由于互联网的基础数字架构及信息和通信技术（信通技术）的全球可用性，网络犯罪与有组织犯罪联系在一起，并往往具有跨国性。[1]

5. 在其第 65/230 号决议中，大会核可了第十二届联合国预防犯罪和刑事司法大会通过的《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变化世界中的发展的萨尔瓦多宣言》，并请预防犯罪和刑事司法委员会按照《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，全面研究网络犯罪问题及会员国、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络犯罪的法律和其他对策。

6. 第十三届联合国预防犯罪和刑事司法大会通过的并获大会第 70/174 号决议核可的《关于将预防犯罪和刑事司法纳入更广泛的联合国议程以应对社会和经济挑战并促进国内和国际法治及公众参与的多哈宣言》重申了这一任务授权。

7. 全面研究网络犯罪问题专家组分别于 2011 年、2013 年、2017 年和 2018 年召开了总共四次会议。在其 2013 年 4 月 26 日第 22/7 号决议中，预防犯罪和刑事司法委员会注意到联合国毒品和犯罪问题办公室（毒品和犯罪问题办公室）在专家组主持下编写的网络犯罪问题全面研究报告，以及在 2013 年 2 月 25 日至 28 日在维也纳举行的专家组第二次会议上就研究报告的内容所开展的讨论（见 UNODC/CCPCJ/EG.4/2017/3），讨论时就研究报告所载的内容、结论和备选方案表达了各种看法，并请专家组酌情在秘书处协助下继续为履行其任务授权开展工作。

[1] 《犯罪全球化：跨国有组织犯罪威胁评估》（联合国出版物，出售品编号：E.10.IV.6），第 204 页；和《2017 年世界毒品问题报告：毒品问题和有组织犯罪、非法资金流动、腐败和恐怖主义》（联合国出版物，出售品编号：E.17.XI.11），第 15 页。

8. 在 2017 年 5 月 26 日第二十六届会议通过的第 26/4 号决议中，预防犯罪和刑事司法委员会请专家组跟上不断变化的趋势，并按照《萨尔瓦多宣言》和《多哈宣言》继续开展工作，为此定期举行会议，发挥进一步讨论网络犯罪相关实质问题的平台的作用，还请专家组继续就国家立法、最佳做法、技术援助和国际合作交流信息，以期审查备选方案，加强现有对策并提议新的国家和国际打击网络犯罪的法律对策或其他对策。在同一决议中，委员会决定专家组在今后会议上将在不影响专家组任务授权所包含其他问题的前提下，有序地专门审查研究报告处理的每个主要问题，同时酌情考虑到根据委员会第 22/7 号决议收到的意见和专家组以前会议的审议情况

9. 在更广泛的背景下，人们越来越认识到，正如大会在其第 70/1 号决议中通过的《2030 年可持续发展议程》所反映的那样，减少冲突、犯罪、暴力和歧视，确保包容、善治和法治对保障可持续发展至关重要。《2030 年议程》的目标 16（“创建和平、包容的社会以促进可持续发展，让所有人都能诉诸司法，在各级建立有效、负责和包容的机构”）在这方面特别重要。目标 16 与打击网络犯罪相联系，网络犯罪与包括有组织犯罪在内的其他形式犯罪一起，削弱了善治和法治，威胁安全与发展，并对会员国造成不稳定影响（见 E/CN.7/2016/CRP.1-E/CN.15/2016/CRP.1，第 4 段）。

10. 第十四届联合国预防犯罪和刑事司法大会将于 2020 年 4 月在日本召开。将在该届预防犯罪大会关于“当前犯罪趋势、最新发展动态和新出现的解决方案，特别是新技术作为犯罪手段和打击犯罪的工具”这一专题的第四次讲习班背景下讨论网络犯罪方面的问题及其他问题。

11. 在这一背景下，将在委员会第二十七届会议上举行关于网络犯罪问题的专题讨论，意在评估最新发展动态。该专题讨论将为进一步讨论及会员国交流看法和经验提供平台。为促进该专题讨论，确定了涉及网络犯罪的八个专题领域，其中包括明确纳入突出主题的领域。下文第三节将分别讨论这八个专题领域，每个副标目都涉及当前的挑战和可能的对策（经委员会第二十六届会议续会商定，见上文第 2 段）以及一份指示性问题清单或要点清单以供进一步讨论。

三. 专题领域：供讨论的议题

A. 网络犯罪的类型及相关威胁

当前的挑战

12. “网络犯罪”不是法律或法证术语，它也没有定义或描述一种明确的刑事犯罪类别。目前各方面已就一份与计算机相关的滥用和犯罪类型核心清单达成普遍共识，但除此之外，全世界尚未就“网络犯罪”一词的含义达成共识。这种情况是电脑的普及性和通用性导致的结果，也是信通技术自 1950 年代后期以来的动态演变和使用方式导致的结果。

13. 根据具体情况，“网络犯罪”一词可以指通过信通技术实施的犯罪，对信通技术设备及其用户实施的犯罪，或信通技术起到间接或支持作用的犯罪

情景。[2]“网络犯罪”一词一直用于描述一系列罪行，包括针对计算机数据和系统的罪行（如黑客攻击）、与计算机相关的伪造和诈骗（如网络钓鱼）、与内容相关的罪行（如传播涉及对儿童的性虐待的材料）[3]以及与版权相关的罪行（如传播盗版内容）。

14. 计算机技术的日益广泛使用和数据数字化的趋势增加了计算机数据的重要性。因此，计算机数据已成为从数据干扰到窃取数据等频繁攻击的目标。当前存在一种复杂的数字地下经济，数据就是其商品。窃取的个人和金融数据——例如用于进入现有银行账户和信用卡，或以欺诈手段设立新的信贷额度——具有货币价值。这种状况推动了一系列犯罪活动，包括网络钓鱼、域名欺骗、散布恶意软件以及对企业数据库进行黑客攻击，这些活动以恶意代码编写者、专门的网络主机和能够租用受感染的计算机网络进行自动攻击的个人等一整套非常成熟的基础设施为支持。

15. 尤其是恶意软件的开发和传播，仍然是大部分网络犯罪案件的基石。自 2013 年底以来，cryptoware（使用加密的勒索软件）成为用以威胁和施压的主要恶意软件。跟随信息窃取者的活动趋势，cryptoware 运动越来越多地将公共和私营部门实体作为目标。[4]

16. 犯罪分子不断寻求各种办法和技术，以使其业务模式更为有效，并增加其利润率。网上交易的匿名性和加密货币的使用降低了被执法机关发现的风险。越来越多的地方用到虚拟专用网络、洋葱路由器和运营商级网络地址转换（互联网协议地址由多个用户共享），限制了调查人员考据证据的能力。

17. 随着互联网的扩张，网络犯罪率节节攀升，因而使互联网使用者更加脆弱。另外，不同形式的网络犯罪构成的威胁呈现出多层面，不仅针对平民，还针对企业和政府，并且迅速增多。网络犯罪工具造成直接安全威胁，并在促进大部分形式的有组织犯罪和恐怖主义活动方面发挥着越来越重要的作用。

可能的对策

18. 这一问题空前严重，加上被称为网络犯罪的多种类型行为，威胁当局有效和高效应对的能力。同时，网络空间也可为侦查网络犯罪提供机会和工具。犯罪分子对信通技术的使用为刑事司法系统留下了一系列调查和证据线索。当局掌握的犯罪活动数据比以往任何时候都多，而且现在有机会以使情报收集和调查具有成本效益的方式利用这些信息。一个有关的例子是非法利用加密货币。区块链技术使加密货币成为可能。尽管当前存在技术和法律方面的漏洞，但区块链技术的若干方面可以使其成为有用的执法工具，用以寻找可疑交易模式和追踪证据（见 E/CN.15/2018/CRP.1，第 164 段）。

19. 通过加强能力建设途径培训的熟练数字调查人员能够获取网络犯罪的电子证

[2] 克里斯托弗·拉姆，“网络犯罪”，《劳特利奇跨国刑法手册》，尼尔·博伊斯特、罗伯特·J.·柯里编（纽约，劳特利奇出版社，2015 年），第 379 页。

[3] 见联合国毒品和犯罪问题办公室《关于新信息技术对虐待和剥削儿童行为的影响的研究》（维也纳，2015 年）。

[4] 欧洲警察署组织，《欧洲联盟严重犯罪和有组织犯罪威胁评估：技术时代的犯罪》（海牙，2017 年），第 30 页。

据，即使犯罪分子小心避免留下数字痕迹或将其抹去。根据数据保留时间，可以查阅互联网协议连接日志以确定互联网连接的时间、源头和目的地。

20. 此外，社会越来越依赖互联网和计算机辅助通信，促使执法部门开发工具以便在线调查违法行为，或者使用软件等曝光犯罪方式。执法机构还利用社交媒体工具来改善其与地方社区的关系，并请公众在刑事调查中予以合作。

21. 因此，各国必须考虑制定多学科战略，以应对挑战和提高其在涉及网络犯罪的案件中成功和有效地调查并起诉的能力。多学科战略的范围可包括监管措施、决策举措到预防网络犯罪和培训主管当局，如下文的讨论那样。

讨论要点

22. 委员会不妨考虑以下几点以供进一步讨论：

(a) 从对网络犯罪演变模式的分析中吸取了哪些经验教训？

(b) 利用这些经验教训来制定国家一级针对网络犯罪的有效监管对策和决策战略的最佳方式是什么？

(c) 各种类型的网络犯罪对会员国保存相关罪行的系统记录和为了执法目的在区域和国际层面交换信息，包括交换关于有组织犯罪集团的参与、其作案手法和鉴别网络犯罪形式所使用技术的相关信息的能力有什么影响？

(d) 《联合国打击跨国有组织犯罪公约》中对“有组织犯罪集团”和“有组织结构的集团”的定义可在多大程度上适用网络空间，包括在罪犯往往受匿名保护，相互联络却不知晓另一方是谁的情况下？

B. 打击网络犯罪的法律措施：刑事定罪方面

当前的挑战

23. 评估当前在制定打击网络犯罪的法律对策过程中面临的挑战时，需要牢记这些挑战多年来是如何出现和升级的。历史上，与计算机有关的服务和与互联网有关的技术在投入使用后不久就引发了新形式的犯罪。其中一个例子是 1970 年代计算机网络的发展，以及稍后不久发生的首例未经授权访问计算机网络的事件。同样，1980 年代，个人电脑出现后不久，即发生了第一宗软件违法行为，当时个人电脑被用来拷贝软件产品。到 1990 年代后期，网络已成为信通技术基础设施的重要组成部分，导致人们越来越担心某些形式的网络犯罪，这些犯罪对其造成威胁。这反过来导致使用网络安全手段以及倾向于将针对关键基础设施的某类攻击具体刑事定罪或从重处罚。[5]

24. 由于技术快速发展演变，出现了新的定义和概念，除此之外，一直存在一个

[5] 除其他外，见 AunshulRege-Patwardhan，“针对关键基础设施的网络犯罪：对在线犯罪组织和技术的研究”，《刑事司法研究：犯罪、法律和社会的重点期刊》，第 22 卷第 3 期（2009 年），第 261 页；卢卡·蒙塔纳里和李奥纳多·库尔佐尼编，《关键基础设施的保护：威胁、攻击和对策》（2014 年 3 月）。另见安全理事会关于恐怖行为对国际和平与安全造成的威胁的第 2341 (2017)号决议。

问题，即是否将网络犯罪视为一种新现象，并确定与之相关的新罪行，还是试图适用目前有关罪行的定义，如有必要，则扩展或调整这些定义。一些国家颁布了新的立法，将计算机诈骗作为一种具体的罪行，而另有一些国家将非法复制或损坏数据、阻碍数据获取或数据的不当使用确立为新罪行，因为现有定义只涉及有形财产。另一个例子是在某些司法管辖区内将盗用身份行为确立为具体罪行。

25. 在倾向于对先已存在的刑事立法进行调整的情况下，立法机构往往要经历冗长的程序来审查和更新这些法律。因此，主要的挑战在于，发现新形式的滥用违法行为到颁布处理这些行为所需的立法修正案之间存在延迟。随着信通技术的创新加快，这一挑战仍然像以往那样具有相关性和主题性。

可能的对策

26. 适当的刑事立法是调查和起诉网络犯罪的基础。因此，立法者应能紧跟信通技术的发展，并持续监测现有法律规定的有效性。有必要对当前立法进行详细分析，以确定国际合作背景下在满足双重犯罪要求方面可能的差距并解决由此导致的难题。立法者还可能从具有约束力和不具有约束力的多边文书受益。

27. 为了获得持久效果，新法律和对现行法律的修订在起草时可能需要灵活一些，并保持技术中立，同时考虑到需要法律确定性和准确性。法律还应述及有必要跨国界及时获取信息。最后，立法者可能需要充分的培训和指导，以便他们制定完善的条款并颁布有效的法律。

讨论要点

28. 委员会不妨考虑以下几点以供进一步讨论：

(a) 在国家一级做出努力以制定和实施打击网络犯罪的立法，并将其纳入国家打击网络犯罪战略更广泛的框架，从中吸取了哪些经验教训？

(b) 国家法律是否为有效侦查、调查和起诉所有与网络犯罪有关的犯罪行为提供了充分的法律依据？有哪些需要填补的空白？

(c) 现有多边文书对打击网络犯罪的国家法律框架的范围有什么影响？建立在这些文书基础上的国家法律对策是否已趋于一致？如果是，一致程度如何？

(d) 鉴于双重犯罪要求，国家将网络犯罪行为进行刑事定罪的各种办法是否影响国际合作的范围？

C. 程序权力和电子证据

当前的挑战

29. 国家调查权在收集电子证据方面发挥着关键作用。对国家一级调查权力的研究揭示，使用电子证据调查犯罪的办法差异很大。这些做法与“原已存在的”权力可在多大程度上适用于作为无形证据的数据有关，以及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。虽然法律权力不尽相同，

但应有一系列具体调查措施用于收集电子证据。这些措施可能包括计算机数据的加速保全；获取储存内容数据的命令；获取储存流量数据的命令；获取用户信息的命令；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；以及使用远程取证工具。有关调查措施的国家法律的示例可查阅毒品和犯罪问题办公室网络犯罪资料库和打击犯罪法律和资料电子交流站（夏洛克交流站）知识管理门户网站。调查权力需要紧跟现代技术的发展。这些权力应以法律和体制框架为支持，促进国家、区域和国际各级私营部门和相关政府机构及时和有效的协调与合作，同时遵守人权。由于信通技术影响隐私和表达自由等领域，因此这些框架必须有强有力的人权部分。

30. 理想情况下，法院可受理电子证据。然而，电子证据在刑事诉讼中变得日益具有重要意义，带来了之前未知的挑战。例如，电子证据非常脆弱，很容易被修改或删除。因此，计算机取证的关键步骤之一是保护电子证据的完整性。保护数据完整性对于确保证据的可靠性和准确性也很有必要。此外，为了能被法院采用，应通过维护人权的既定程序收集电子证据。

31. 此外，为了让执法机关有效地调查和收集与网络犯罪有关的电子证据，与其他相关行为体，包括来自私营部门的行为体合作，过去几年来变得特别重要。总体来说，通信服务提供商在获取电子证据方面发挥着重要作用。国家隐私法能够影响提供商与执法机关共享资料以协助调查的能力。

可能的对策

32. 由于电子证据不稳定，因此需要某些标准和要求来处理，并确保其真实性和完整性。这些标准和要求包括一般规则和程序，如保留案件记录、使用广泛接受的技术以及有资质的专家参与调查。

33. 越来越多的网络犯罪调查，包括对涉及虐待和剥削儿童行为案件的调查，都需要第三方提供电子证据。因此，行业和政府必须携手努力，制定各种机制，使执法部门能在紧急情况下及时获取数据。这类机制应与常规调查的公平和透明的法律程序相结合。

34. 2018 年 2 月 12 日和 13 日在维也纳举行了关于合法获取跨境数字数据的专家组会议，此次会议由毒品和犯罪问题办公室和反恐怖主义委员会执行局与国际检察官协会合作联合组织。这次会议旨在为编写有关中央机关、检察官和调查人员在跨境反恐和有关有组织犯罪调查中从国外司法管辖区获取电子证据的实用指南奠定基础。这次会议为分享国家法律和指南、展示从位于外国司法管辖区的通信服务提供商处获取电子证据方面吸取的良好做法和经验教训的真实案例提供了机会。

讨论要点

35. 委员会不妨考虑以下要点以供进一步讨论：

(a) 调查机关在寻求满足使用特殊侦查技术以及收集和共享电子证据来侦查、调查和起诉网络犯罪的要求时遇到了哪些挑战？在应对这些挑战方面有哪些良好做法？

(b) 在法院对这些证据的采用方面，会员国都积累了哪些经验？

(c) 在收集与网络犯罪收益（例如钱骡）有关的电子证据时与金融部门合作有哪些影响？

(d) 从法治和人权角度看，在有效使用和执行与调查和起诉网络犯罪有关的技术方面有哪些主要挑战？

(e) 从促进执法机关和通信服务提供商之间的合作以获取有关侦查、调查和起诉网络犯罪的电子证据的工作中吸取了哪些经验教训？

D. 管辖权问题

当前的挑战

36. 国际法对网络犯罪行为的若干管辖权依据作了规定，主要是属地管辖权形式和国籍管辖权形式。其中一些依据可以在多边网络犯罪文书中找到。扩大的或客观的领土管辖权现在往往以犯罪要件发生、其具有影响或与一国领土具有其他某种重要联系为基础。各国还必须根据证据或犯罪分子所在地等因素，确定哪个国家最能够起诉被指控的犯罪分子。

37. 不同国家对一系列管辖权依据的适用可能使超过一个国家声称对同一网络犯罪行为拥有管辖权。如果属地原则仅适用于用于实施犯罪的基础设施而非罪犯或受害者位于相关国家的案件，那么管辖权冲突的风险将进一步增加。

38. 云计算给刑事司法带来了一系列挑战，特别是在可适用法律和执行刑事司法管辖权方面。对刑事司法机关而言，数据存储在哪个司法管辖区，适用哪些法律制度往往并不明确。一家服务供应商可能将总部设在一个管辖区，但受另一个管辖区的法律制度约束，而又将数据存储在第三个管辖区。通过使用被称为镜像的技术，相同的数据可以保存在若干管辖区，或是可以在管辖区之间移动，从而使得这些问题更加复杂。

39. 此外，云计算服务的提供商是用户所拥有数据的控制者还是处理者往往并不明确，因此适用何种规则也不明确。另一个不确定的因素是，数据是储存下来了还是在传输中，因此是否和基于何种司法管辖依据执行制作命令、搜索和缉获命令、拦截命令或实时收集命令。此外，由于云的架构（数据的多重租赁、分配和隔离）以及与数据收集的完整性和有效性、证据控制、数据所有权或管辖权有关的法律挑战，云计算的非本地化特性导致在线取证和搜索存在问题。[6]

可能的对策

40. 在很多情况下，若干国家可以对网络犯罪罪行提出管辖权，必须进行磋商以决定应由哪个国家起诉。该决定可能涉及法律、外交和实际议题，如各个国家的管辖权主张和其他法律主张，能否将犯罪分子引渡到希望提出起诉的国家的问

[6] 欧洲委员会网络犯罪公约委员会（T-CY），“刑事司法获取云数据：挑战”，网络犯罪公约委员会云证据小组编写的讨论文件，2015 年 5 月 26 日，T-CY (2015)10 号文件，第 10-14 页。

题，以及一些实际考虑因素，如成本和在将证据从一国转移至另一国并确保法庭采用证据和有效地向法院提交证据的过程中遇到的其他阻碍等。如果出现管辖权冲突，往往通过国家间的正式和非正式磋商解决。如果决定应由若干可能国家中的一个国家提出起诉，可有效移交其他国家的管辖权。作为国际合作的独特形式，刑事诉讼的移交为这一做法提供了背景和框架。[7]

41. 还努力在多边层面加强国际和区域合作以获得电子证据。2017 年 6 月，欧洲委员会网络犯罪公约委员会核准编写《网络犯罪公约》第二议定书。该议定书的目的在于提供明确规则和更有效的程序，以在具体刑事调查中获取在“云”储存的电子证据。该职权范围于 2017 年 6 月 8 日得到核准，谈判计划在 2017 年 9 月至 2019 年 12 月期间进行。

讨论要点

42. 委员会不妨考虑以下要点以供进一步讨论：

(a) 为了在网络犯罪案件中执行刑事司法对策，有关管辖权的标准是什么？这些标准如何适用数据往往不是“静止”的云计算情景？

(b) 在开展磋商以解决有关网络犯罪罪行的管辖权冲突方面都积累了哪些经验？有哪些挑战，哪些良好做法，吸取了哪些教训？

E. 国家一级的机构间协调与合作

当前的挑战

43. 多利益攸关方打击网络犯罪战略是打击网络犯罪斗争中的关键要素。网络犯罪构成的法律、技术和体制挑战影响深远，只有通过采取依赖现有举措和不同利益攸关方的作用的连贯策略才能解决。为了取得成效，打击网络犯罪需要高度完善的组织结构，避免重叠，并且有明确界定的权限，能够协调所有相关方，以便采取协调一致的行动。没有适当的组织结构，执行完善的政策和方案举措将异常困难。

44. 威慑网络犯罪也是确保网络安全和保护关键信息基础设施的国家战略必不可少的组成部分。其中特别包括通过立法来打击为了犯罪和其他目的滥用信通技术，并打击意图损害关键国家基础设施完整性的活动。威慑网络犯罪是政府主管机关、私营部门和公民的共同责任，需要他们采取协调一致的行动来预防、做好准备和应对网络安全事件，并从中恢复过来。制定和执行国家打击网络犯罪战略需要一种综合办法，涉及机构层面相关利益攸关方之间的合作与协调。

45. 尽管如此，机构协调带来了很多困难，其中大部分与各国掌握的资源和能力有关。有必要考虑到若干其他因素，包括私营部门支持的程度，例如通过公私伙伴关系或私营部门已采取的自我规范和自我保护措施。

[7] 见秘书处编写的关于移交刑事诉讼作为一种独立的刑事事项国际合作形式方面的实际考虑因素、良好做法和挑战的背景文件（CTOC/COP/WG.3/2017/2）。

可能的对策

46. 建立多机构伙伴关系已成为在战略层面打击网络犯罪，包括打击利用技术对儿童实施的犯罪的常见做法。为应对在打击网络犯罪斗争中遇到的多方面挑战，通信服务提供商和执法及刑事司法机关等公共机构需要建立公私伙伴关系，以建立信任和双向对话。更广泛来说，各国需要增加刑法之外的监管对策并鼓励私营部门积极参与预防犯罪。这一办法可能有助于创造对新出现的威胁具有敏感性和有利于打击这些威胁的环境。

47. 瞄准利用互联网实施的有组织犯罪的工作队可能是采取一致行动打击网络犯罪的有用工具。这些工作队应当对不断变化的犯罪环境作出反应，并能带动建立更多常设小组等来分享信息，并为捣毁僵尸网络等具体行动提供更多特别安排。在所有情况下，当局需要灵活地纳入各种利益攸关方，如执法部门、私营部门、学术界和用户组等，并与他们有效协调，以实现预期成果。

48. 互联网进一步改变了各国政府内部政府信通技术监管的重点。监管信通技术部门的机构已经发现自己参与了一系列打击网络犯罪的活动。这在内容监管、网络安全和消费者保护等领域尤其如此，因为用户变得很容易受到攻击。因此，监管机构参与进来是因为网络犯罪破坏信通技术行业的发展以及提供相关产品与服务的各方的发展。信通技术监管机构在打击网络犯罪方面承担新的职责和责任，可将之视为网络犯罪监管集中模式向灵活体系转变这一更广泛趋势的一部分。[8]

讨论要点

49. 委员会不妨考虑以下要点以供进一步讨论：

(a) 在国家层面加强机构能力和机构间协调以应对网络犯罪时遇到了哪些挑战？

(b) 在制定国家一级相关利益攸关方合作预防和打击网络犯罪的示范框架或指导方针方面是否积累了经验？如有，这些示范框架或指导方针如何促进实际合作？

F. 国际合作

当前的挑战

50. 除了将网络犯罪行为定罪和赋予相关程序权力，现有文书还规定了跨境调查和起诉网络犯罪方面的国际合作机制。为打击网络犯罪开展国际合作表明，刑事司法和执法机关面临日益严峻的挑战。虽然理论上讲，在特定时间点可以确定具体计算机数据的位置，但云计算、加密和对等数据共享与储存的出现意味着数据现在可以有若干副本，分布于若干装置和地点，而且可以在几秒钟内就被转移到另一个地理位置。[9]

[8] 国际电信联盟，《了解网络犯罪：现象、挑战和法律对策》（日内瓦，2012 年），第 101 页。

[9] 关于讲习班 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，包括吸取的经验教训和开展国际合作”的背景文件（A/CONF.222/12），第 32 段。

51. 由于电子证据具有易变性，因而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调查行动，包括由服务提供商保全和制作数据。向另一个管辖区请求这类数据时，遇到的一个常见挑战是延迟回应请求，往往超过了数据保存期限，而且可能使犯罪分子能够永久性地销毁关键的电子证据。其他常见挑战包括收到请求的机构缺乏承诺和灵活性，该机构提供的证据的形式是否可用于刑事诉讼，以及合作国家在刑事犯罪定义方面的差异。[10]

52. 在 2013 年举行的全面研究网络犯罪问题专家组第二次会议上，大部分专家一致认为，需要加大加快国际合作，以解决网络犯罪问题，特别是这个问题不断扩大，而合法事务对技术的依赖导致网络犯罪可能带来更为严重的威胁。除此之外，与会者还就解决网络犯罪相关问题的最佳战略办法和优先事项表达了不同观点。[11]在这一背景下，一直存在的争论是是否应制定新的打击网络犯罪的普遍性法律文书，除其他外，来探讨全球一级的国际合作方面，还是反过来，国际社会应继续依赖包括欧洲委员会《网络犯罪公约》在内的现有多边文书。该问题仍将继续辩论，迄今仍未达成共识。

可能的对策

53. 国际合作机制可以通过研究如何加快司法协助程序得到进一步改进。其他解决办法可能有赖于加强执法合作和继续推进关于跨国获取计算机数据的多边对话。例如，根据欧洲委员会《网络犯罪公约》第 18 条第 3 款中的定义，建立有关获取用户信息的单个制度，区分所搜寻数据的类型，能够大大有助于在网络犯罪和电子证据事项方面的司法协助更为有效。[12]

54. 在重新开发的毒品和犯罪问题办公室“司法协助请求书撰写工具”中纳入电子证据模块等创新可协助精简涉及电子证据的司法协助程序。但与此同时，执法部门可能越来越需要在跨国网络犯罪调查方面找到开创性的合作方式。国际刑事警察组织（国际刑警组织）全球创新中心和欧洲警察署欧洲网络犯罪中心等实体参与协调和支持跨国调查工作，包括通过促进国家执法机关之间的信息共享等，可能在这方面特别重要。

55. 其他解决办法可能包括以下方面：在中央机构中设立单独的反网络犯罪单位；监测和审查司法协助事项上的个案做法，包括通过统计涉及电子证据的司法协助请求，以提高响应能力和效率；更频繁地开展警方间的合作，作为司法协助模式的有益补充，以确保及时响应紧急协助请求；开展重点突出和更密集的培训，以加强有关网络犯罪和电子证据的司法协助、警方间的合作以及其他形式国际合作；加强一周 24 小时联络点网络之间的信息和经验共享；在执行司法协助请求任务的国家机关一级分配资源，并加强它们与中央机关的协调，以便及时作出反应。

---

[10] 见秘书处编写的关于收集和分享电子证据的背景文件（CTOC/COP/WG.3/2015/2），第 19 段。

[11] 2013 年 2 月 25 日至 28 日在维也纳举行的全面研究网络犯罪问题专家组第二次会议的审议情况，报告员的摘要，UNODC/CCPCJ/EG.4/2017/3，第 25 段。

[12] 见欧洲委员会网络犯罪公约委员会云证据小组，“刑事司法获取云中电子证据：供网络犯罪公约委员会审议的建议”，T-CY（2016）5 号文件，第 13 页。

讨论要点

56. 委员会不妨考虑以下要点以供进一步讨论：

(a) 在涉及网络犯罪和电子证据的案件中，如何能改进司法协助程序的及时性？在海外提取电子证据时，警察间合作方面有哪些最佳做法，又有哪些挑战？

(b) 加强区域和国际层面的信息共享如何提高了侦查和评估风险以及有效和及时回应请求的能力？在这方面各国可以提供哪些实例？

(c) 应如何编写、传递和处理保全电子证据的国际请求？在这方面，积累了哪些公私部门合作的经验？

G. 预防网络犯罪

当前的挑战

57. 调查和起诉网络犯罪案件的成本和复杂性表明，合作预防工作可能大有裨益。尤其是，公私伙伴关系是预防网络犯罪的核心。服务提供商可通过以下方式在预防网络犯罪方面发挥作用：(a)储存用户数据，持有授权证的执法官员可以查阅并将之用于调查网络犯罪；以及(b)积极过滤互联网通讯和内容，以防止网络犯罪行为发生。然而，在言论自由的背景下进行分析时，这两项措施会带来许多挑战。

58. 讨论服务提供商在预防网络犯罪方面的作用时，可能需要考虑其作为私营部门实体的局限性。首先，提供商政策往往不稳定，而且对执法部门和消费者而言缺乏可预见性。服务提供商可能随时单方面更改其政策而不会事先通知执法部门。除此之外，政策和做法不仅在提供商之间有很大差异，在不同会员国之间也有很大差异。一家提供商可能回应一国的许多请求却不回应另一国的请求或只回应一部分请求，而另一家提供商的做法可能恰恰相反。[13]

59. 第二，警方的网络犯罪调查可能受数据保护措施的影响，这些措施要求删除无需再用于收集目的的个人资料。因此，虽然数据保留法可能是一种务实的办法，确保通信服务提供商能够通过加强与执法部门的合作，在预防网络犯罪方面发挥更大的作用，但这些法律在执行时必须有适当的程序保护措施和隐私保护。需要考虑关于数据保护的标准和条例，包括欧洲联盟的通用数据保护条例。[14]

60. 学术界面临的巨大挑战是，填补网络犯罪知识方面现有和不断出现的诸多空白，尤其是与信通技术相关的针对儿童的性虐待和性剥削。如果有可持续的供资——这是很多管辖区面临的重大挑战，学术机构就可以在预防网络犯罪方面发挥各种作用，包括通过向专业人士提供教育和培训、制定法律和政策、制定技术标准和解决方案。

---

[13] 同上，“刑事司法查阅云数据：与‘外国’服务提供商合作”，（T-CY (2016)2），第 22 页。

[14] 欧洲议会第(EU) 2016/679 号条例和欧洲委员会 2016 年 4 月 27 日关于在处理个人数据和此类数据的自由流动方面保护自然人的条例，废除了第 95/46/EC 号指令（《欧洲联盟官方公报》，L 119，2016 年 5 月 4 日，第 1-88 页）。

可能的对策

61. 预防网络犯罪方面的良好做法包括颁布立法、有效领导、发展刑事司法和执法能力、建立强大的知识库，以及政府、社区、私营部门和国家之间开展合作。最重要的是要为发展和完善预防性技术提供援助，分享汲取的经验教训和最佳做法，共享发展预防性技术并使其发挥作用所需的信息。

62. 提高认识和教育运动以及各种举措，包括那些涉及新涌现的威胁和针对儿童等特定受众的运动和举措，已被强调为预防网络犯罪政策的重要组成部分。[15]教育促进正义举措是毒品和犯罪问题办公室实施《多哈宣言》全球方案的关键组成部分，其中包括编写和分发针对小学、中学和高校教育阶段、儿童和年轻人的打击网络犯罪材料。

63. 民间社会可在帮助儿童了解和处理网上风险方面发挥关键作用，这对防止利用信通技术虐待和剥削儿童方面的工作特别重要。教育和社会心理预防方法被认为是保护儿童免遭利用信通技术虐待和剥削的关键。教育举措使儿童、其家人以及其他照管者能够了解和正确评估与信通技术有关的风险。。[16]

64. 建立公私伙伴关系促进预防网络犯罪方面有很多模式，例如执法机关和通信服务提供商之间的模式。其中很多依赖基于明确的规则、信任、有限制的成员资格、鼓励互惠互利以及响应能力的信息共享。此外，私营部门在用户能够访问之前就发现和阻止与性虐待儿童有关的在线材料方面的作用将越来越大。[17]

65. 对各国政府而言，一种前瞻的明确办法是与那些会影响今后业务和运营环境的各方合作，以便所有相关各方都能更好地预测犯罪行为和技术滥用方面的变化。在这方面，必须通过情报分析、犯罪学研究和特征分析技术继续深入了解当代网络犯罪行为，以更有效地部署现有资源，并主动确定今后容易用作犯罪用途的通信技术的特点。

讨论要点

66. 委员会不妨考虑以下要点以供进一步讨论：

(a) 关于相关利益攸关方在打击网络犯罪方面所采取的有效预防战略，各国可以提供哪些实例？如何定义和衡量成功？

(b) 学术机构、私营部门和非政府组织如何为网络犯罪领域的知识、立法和政策的发展与共享作出最大贡献？

(c) 会员国在兼顾数据保护和网络犯罪调查的成效方面积累了哪些经验？

---

[15] 见《关于新信息技术影响的研究》，第 54 页。

[16] 同上，第 54 页。

[17] 例如，见《2017 年 *Netclean* 报告》，可查阅：https://www.netclean.com/netclean-report-2017。

H. 能力建设和技术援助

当前的挑战

67. 国家执法和刑事司法系统层面的能力建设至关重要。虽然大多数国家已经开始建立负责调查网络犯罪和涉及电子证据的犯罪的专门机构，但在很多国家，这些机构资金不足，并且缺乏能力。由于电子证据对网络犯罪调查而言至关重要，执法机关可能需要明确区分网络犯罪调查人员和数字司法鉴定实验室的能力，并为其建立明确的工作流程。一线执法人员可能越来越需要掌握和利用一些基本技能，例如使电子存储设备形成完好的取证图像所需的技能。

68. 总而言之，由于新型技术和犯罪的继续快速发展，建设执法部门和刑事司法行为体打击网络犯罪的能力显然将是一个持续不断的进程。

可能的对策

69. 技术援助与合作对能够分享良好的调查做法、经验和传播新技术至关重要。会员国不妨加强分享就调查复杂的互联网金融诈骗、网上贩毒或利用虚拟货币洗钱而采取的新办法，从而使得各个国家的执法机关能够快速获得必要技能以打击新出现的网络犯罪威胁。

70. 执法机构内部专门的反网络犯罪机构或部门能够让各国更容易将有限的资源集中到一处，以形成专门的调查技术，并收集和分析合适的电子证据，包括开展数字法证检验。同时，这些机构或部门可以为当地执法机构提供培训，协调针对网络犯罪的国家对策，促进参与调查的伙伴之间的合作，并瞄准一国可能特别关注的网络犯罪形式。

71. 根据大会第 65/230 号决议及预防犯罪和刑事司法委员会第 22/7 号和第 22/8 号决议，毒品和犯罪问题办公室通过其网络犯罪问题全球方案，受权通过能力建设和技术援助协助会员国打击网络犯罪。根据这一方案，毒品和犯罪问题办公室主要就发展中国家在网络犯罪方面的能力建设、预防和提高意识以及国际合作和分析提供重点技术援助。该方案还根据请求并在其任务授权范围内，向有需要的会员国提供立法援助。

72. 例如，毒品和犯罪问题办公室开发了关于加密货币调查的培训员培训课程，并且一直在不同区域开展加密货币调查培训。该培训的目的是提高执法官员、分析人员、检察官和法官关于加密货币、在金融调查中追踪比特币、定位信息来源和在国际案件中进行合作的能力。

讨论要点

73. 委员会不妨考虑以下要点以供进一步讨论：

(a) 在与网络犯罪有关的措施和战略中，哪些方面是技术援助和能力建设的高度优先事项，特别是考虑到网络犯罪不停演变的性质以及与其相关的新的和新出现的威胁？

(b) 从分享良好的调查做法、经验和传播新技术作为技术援助合作范例中吸取了哪些教训？

(c) 为了向需要援助的会员国提供切实和可持续的能力建设服务，如何在就网络犯罪问题提供技术援助的国际组织之间寻求和促进最佳协同效应和联盟？

四. 解决当前差距和展望未来

74. 为了更好地了解和应对网络犯罪威胁，国际社会仍在继续加大努力。尽管如此，亟需开展更多工作，这是因为在制定和实施针对网络犯罪的全面、协调、可持续和有效的对策方面，仍然存在重大挑战。

75. 通过促进第二十七届会议上的专题讨论，委员会在审议相关议程项目期间将充当一个平台，以供交流相关信息、最佳做法和经验教训，以及制定有关打击网络犯罪的有效对策和促进相关国际书或标准。

76. 在考虑采取进一步行动来应对网络犯罪构成的挑战并进而制定适当对策时，委员会不妨将讨论重点放在当前国家法律和体制框架中被认为带来最大风险的领域，以及会员国面临最大挑战的优先领域。

77. 委员会可以考虑建议会员国进一步加强其能力建设工作和法律框架，特别是在审查现行国家政策、法律和体制框架时，目的是确定可加强其应对现有和新出现的网络犯罪威胁的能力的新的或经修正的立法、体制框架和做法。

78. 委员会可以在相关任务授权基础上确定和优先考虑毒品和犯罪问题办公室可能与其他相关行为体密切合作与协调的技术援助领域，以更好地支持会员国执行国家政策、法律和机构能力，应对当前和新出现的与网络犯罪有关的挑战。

79. 委员会不妨进一步请毒品和犯罪问题办公室协助其与处理网络犯罪和刑事司法对策的其他政府间机构，包括有组织犯罪公约缔约方会议及其国际合作工作组，在其各自的任务授权范围内酌情保持沟通，以预防和打击网络犯罪。