

Distr.: General  
12 April 2019  
Chinese  
Original: English

## 2019年4月27日至29日在维也纳举行的全面研究网络犯罪问题专家组的报告

### 一. 引言

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变化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，该专家组应在委员会第二十届会议之前召开会议，全面研究网络犯罪问题以及会员国、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，以加强现有的并提出新的国家和国际打击网络犯罪的法律对策或其他对策。
2. 全面研究网络犯罪问题专家组第一次会议于 2011 年 1 月 17 日至 21 日在维也纳举行。在这次会议上，专家组审查并通过了一系列专题和研究方法（[E/CN.15/2011/19](#)，附件一和二）。
3. 专家组第二次会议于 2013 年 2 月 25 日至 28 日在维也纳举行。在这次会议上，专家组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）按照大会第 [65/230](#) 号决议所载任务授权在专家组指导下编拟的关于网络犯罪问题以及会员国、国际社会和私营部门对策的全面研究报告，还注意到专家组第一次会议通过的一系列专题和研究方法。会上对研究报告的内容、结论和备选方案表达了不同意见（见 [UNODC/CCPCJ/EG.4/2013/3](#)）。
4. 在第十三届联合国预防犯罪和刑事司法大会通过并经大会第 [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》中，会员国注意到专家组的活动，并请委员会考虑建议该专家组在其工作的基础上继续就国家立法、最佳做法、技术援助和国际合作交流信息，以期审查各种备选方案，以加强现有对策并提出国内和国际打击网络犯罪的新的法律对策或其他对策。
5. 专家组第三次会议于 2017 年 4 月 10 日至 13 日在维也纳举行。在这次会议上，专家组除其他以外审议了以下内容：通过报告员编写的专家组第一和第二次会议审



议情况摘要、网络犯罪问题全面研究报告草稿及相关评论意见，以及今后处理报告草稿的方式。会上还就国家立法、最佳做法、技术援助和国际合作交流了信息。

6. 委员会在 2017 年 5 月第二十六届会议通过的第 26/4 号决议中请专家组跟上网络犯罪不断变化的趋势，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，并发挥进一步讨论网络犯罪相关实质问题的平台的作用。委员会在该决议中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，以加强现有对策并提出国内和国际打击网络犯罪的新的法律对策或其他对策。

7. 专家组第四次会议于 2018 年 4 月 3 日至 5 日在维也纳举行。专家组这次会议重点讨论与网络犯罪有关的立法与框架以及刑事定罪。会上讨论了在国家和国际两级应对网上犯罪问题的立法和政策发展情况，并审议了国家一级将网络犯罪定为刑事犯罪的各种方式。专家组还通过了主席关于专家组 2018-2021 年工作计划的建议（UNODC/CCPCJ/EG.4/2018/CRP.1）。

8. 扩大主席团在 2018 年 11 月 2 日的会议上决定了专家组第五次会议的会期，并商定了临时议程。

## 二. 初步建议和结论清单

9. 按照专家组 2018-2021 年工作计划，报告员将在专家组 2019 年和 2020 年两次会议上，在秘书处协助下，根据专家组的讨论和审议情况，编写会员国提出的初步结论和建议清单，该清单应当准确无误，侧重于加强打击网络犯罪的实际对策。按照工作计划，该清单将以会员国所提建议汇编的形式纳入每次会议的报告中，供不晚于 2021 年举行的评估会议进一步讨论。按照工作计划，专家组将在评估会议上审议初步结论和建议，将其并入一份已通过结论和建议清单，以提交委员会。在评估会议之前，将把会员国提出的初步结论和建议分发给所有会员国、观察员和其他利益攸关方征求意见，随后在评估会议前将这些意见发布在网上，供各代表团审议。

### A. 执法和调查

10. 按照工作计划，本段载列会员国在会议上在题为“执法和调查”的议程项目 2 下提出的建议汇编。这些初步建议和结论是会员国提交的，列于此处并不表示已得到专家组核可，其编排也并非依重要性顺序：

(a) 一些会员国指出，由于网络犯罪在不断演变，具有复杂性和跨国性，谈论国际合作的共同标准为时尚早。因此，会员国应采取新的国际对策打击网络犯罪，即考虑在联合国框架内谈判一项关于网络犯罪的新的全球法律文书。考虑该文书时除其他外要考虑到所有会员国的关切和利益，以及 2017 年 10 月 11 日向秘书长提交的拟议的联合国合作打击网络犯罪公约草案（A/C.3/72/12，附件）；

(b) 然而，另一些会员国指出，审议一项新的全球法律文书既不必要，也不适当，因为通过能力建设、执法机构之间的积极对话与合作以及使用《欧洲委员会网络犯罪公约》（《布达佩斯公约》）等现有工具，可以很好地应对网络犯罪造成的挑战并处理为调查人员、检察官和法官提供充分培训一事。根据这一建议，会员国应继续使用和（或）加入现有的关于网络犯罪的多边法律文书，如《布达佩斯公约》，

许多国家认为该《公约》是制定关于网络犯罪的适当国内立法——不管是实体立法还是程序立法——和促进旨在打击这类犯罪的国际合作的最有意义的指南；

(c) 鉴于网络犯罪具有跨国性以及全球网络犯罪绝大多数由有组织集团实施这一事实，会员国还应更多地利用《联合国打击跨国组织犯罪公约》促进为网络犯罪相关刑事调查交流信息和证据；

(d) 会员国应促进和参与旨在打击网络犯罪的国际合作，利用现有文书，在互惠原则的基础上缔结双边协定，并与毒品和犯罪问题办公室协作，支持司法和执法当局之间定期联网和分享信息；

(e) 各国应通过向警官提供培训，发展他们在调查网络犯罪方面的专门知识，许多国家以及毒品和犯罪问题办公室及其他伙伴均提供此类培训，目的是加强侦查、调查和打击网络犯罪的能力。这一领域的能力建设应特别顾及发展中国家的需要，注重每个国家的薄弱之处，以便为了受益方的最大利益因地制宜地提供技术援助，促进交流最新知识；

(f) 鼓励各国继续向毒品和犯罪问题办公室提供必要的任务授权和财政支持，以期这一领域的能力建设项目取得切实成果；

(g) 各国应投入资源，发展调查网络犯罪的专门知识，并建立伙伴关系，以利用合作机制取得重要证据；

(h) 会员国应继续努力发展和支持执法、检察和司法当局内专门的网络犯罪单位、机构或部门，以便他们拥有必要的专门知识和设备，以应对网络犯罪带来的挑战，并为刑事诉讼收集、分享和使用电子证据；

(i) 鉴于打击网络犯罪需要中期和长期执法战略，包括与国际伙伴合作，以瓦解网络犯罪市场，这些战略应当积极主动，最好将目标对准可能在多个国家拥有成员的有组织网络犯罪集团；

(j) 各国应继续以技术中性的语言颁布实体立法，处理网络空间中新的和正在出现的犯罪形式，以确保与信息和技术领域未来的发展保持一致；

(k) 国内程序法必须跟上技术进步的步伐，并确保执法当局有足够的力量打击网络犯罪。在起草相关法律时，应考虑到适用的技术概念以及网络犯罪调查人员的实际需要，同时符合正当程序保障、隐私利益、公民自由和人权，以及相称性和辅助性原则及确保司法监督的保障措施。此外，会员国应拨出资源颁布国内立法，授权：

- (一) 要求计算机数据控制者-即互联网和通信服务提供商-快速保全数据，以便在一段特定时期内保持数据和维持数据的完整性，因为此种数据有可能发生变动；
- (二) 搜索和扣押数字设备上存储的数据，这些数据往往是电子犯罪最重要的证据；
- (三) 下令提供隐私保护程度较低的计算机数据，例如流量数据和订户数据；
- (四) 在适当情况下实时收集流量数据和内容；
- (五) 国内执法当局开展国际合作；

(l) 由于网络犯罪调查需要创造性、技术敏锐性以及检察官和警察之间的共同努力，各国应鼓励检察官和警察在调查早期密切合作，以形成足够的证据，对所确定的主体提出指控；

(m) 在对网络犯罪案件进行调查时，执法人员应听从调查人员指导，以确保遵守正当程序标准；

(n) 国内执法机构应与国内互联网服务提供商和其他私营行业团体进行接触与合作。这种外联活动会增进利益攸关方之间的信任与合作，从而有助于执法调查；

(o) 各国在网络犯罪领域应灵活处理适用的管辖权依据，包括更多以信息和通信技术服务提供地为准，而不是以数据所在地为准；

(p) 各国应投资于提高公众和私营企业对网络犯罪的认识，以解决与其他类型犯罪相比网络犯罪报案率较低的问题；

(q) 会员国应促进公私伙伴关系以打击网络犯罪，包括为此颁布立法和建立对话渠道，以促进执法当局、通信服务提供商和学术界之间的合作，以期增进相关知识并加强打击网络犯罪对策的有效性；

(r) 各国应采取措施鼓励互联网服务提供商在预防网络犯罪及支持执法和调查活动方面发挥作用，包括在国内立法中就这些服务提供商的义务作出相关规定，并明确界定此类义务的范围和界限，以保护服务提供商的合法权益；

(s) 各国应加强与协助、教唆和筹备网络犯罪行为有关的调查和执法活动，以期有效应对整个网络犯罪链条；

(t) 各国应继续加强能力建设，提高司法和执法当局调查和起诉网络犯罪的能力。应在能力建设活动中强调云计算、暗网和其他新兴技术带来的日益严峻的挑战。此外，鼓励各国向发展中国家提供能力建设援助。

## B. 电子证据和刑事司法

11. 按照工作计划，本段载列会员国在会议上在题为“电子证据和刑事司法”的议程项目 3 下提出的建议汇编。这些初步建议和结论是会员国提交的，列于此处并不表示已得到专家组核可，其编排也并非依重要性顺序：

(a) 会员国应制定和实施法定权力、管辖规则和其他程序性条款，确保在国家一级对网络犯罪和利用技术实施的犯罪进行有效调查，并在跨国案件中实现有效合作，同时考虑到有效执法、国家主权以及保护隐私和其他人权的必要性。这可能包括：

- (一) 调整证据规则，确保电子证据得以收集、保全、认证并在刑事诉讼中使用；
- (二) 通过关于国家和国际追查通信的规定；
- (三) 通过关于进行国内和跨境搜索的规定；
- (四) 通过关于拦截经由计算机网络和类似媒体传输的通信的规定；
- (五) 颁布在技术上中立的实体法和程序法，使各国能够应对新的和正在出现的网络犯罪形式；

(六) 统一国家立法；

(七) 颁布新的或加强现有的立法，以便有可能承认电子证据的可采性，并界定和确定电子证据的范围；

(b) 会员国应推动努力建设执法人员的能力，包括在专门执法机构工作的人员、检察官和司法人员的能力，使这些人员至少具备电子证据方面的基本技术知识，能够对追查通信方面的援助请求作出有效和迅速的反应，并为调查网络犯罪采取其他必要措施；

(c) 会员国应促进能力建设，以改进调查工作，增进对网络犯罪以及可用于打击网络犯罪的设备和技术的了解，并使检察官、法官和国家中央当局能够对这类犯罪进行适当的起诉和判决；

(d) 会员国应推动努力建设参与司法协助相关要求和程序国际合作的中央当局的能力，包括提供关于起草附有充分信息的综合请求书以求获得电子证据的培训；

(e) 会员国应考虑采用“起诉小组”办法，将各机构的技能和资源加以汇总，将检察官、调查人员和法证分析人员汇集在一起进行调查。这种做法使检察官能够处理和提出电子证据；

(f) 电子证据的可采性不应取决于证据是否从一国管辖范围以外收集，条件是证据的可靠性未受到损害，而且证据是合法收集的，例如，是根据司法协助条约或多边协定或与拥有管辖权的国家合作收集的；

(g) 会员国应采取必要措施，颁布确保电子证据可采性的立法，同时铭记包括电子证据在内的证据的可采性是每个国家应根据其国内法处理的一个问题；

(h) 会员国应加强执法机构、检察官、司法当局和互联网服务提供商之间的国际合作，以弥合网络犯罪分子的作案速度与执法对策的快捷性之间的差距。为此，会员国应利用现有框架，例如 24/7 网络和通过国际刑事警察组织（刑警组织）开展的合作，以及司法协助条约，以促进涉及电子证据的国际合作。会员国应进一步协调和理顺与司法协助有关的程序，并制定一个共同模板，以加快此类程序，以便及时收集和移交跨境电子证据；

(i) 鼓励会员国更多地交流经验和信息，包括国家立法、国家程序、跨境网络犯罪调查最佳做法、关于有组织犯罪集团的信息以及这些集团使用的技术和方法；

(j) 会员国应在执法机构、司法当局和检察官之间建立一个协调人网络；

(k) 会员国应评估授权专家组或毒品和犯罪问题办公室专家在会员国协助下对网络犯罪趋势和新威胁进行年度评估并予以公布的可能性；

(l) 毒品和犯罪问题办公室应支持扩大研究活动，以查明新的犯罪形式和模式、犯罪在关键领域的影响以及电信环境的发展，包括物联网的扩展、区块链技术和加密货币的采用以及人工智能与机器学习的结合使用；

(m) 毒品和犯罪问题办公室应当在有资源的前提下，通过网络犯罪问题全球方案，酌情促进、支持和实施技术合作和援助项目。此类项目将使预防犯罪、计算机

安全、立法、起诉、调查技术和有关问题方面的专家与寻求这些方面信息或协助的国家汇合在一起；

(n) 毒品和犯罪问题办公室应为会员国的司法和检察当局制定一项教育方案，重点是提高关于打击网络犯罪措施的知识 and 认识，特别是电子证据收集领域的措施；

(o) 会员国应采取行动，加强在收集电子证据方面的合作，其中包括：

(一) 分享关于网络犯罪威胁的信息；

(二) 分享关于有组织网络犯罪集团的信息，包括其使用的技术和方法；

(三) 促进增强执法机构、检察官和司法当局之间的合作与协调；

(四) 分享打击网络犯罪的国家战略和举措，包括将网络犯罪分子绳之以法的国家立法和程序；

(五) 分享与跨境调查网络犯罪有关的最佳做法和经验；

(六) 建立执法当局、司法当局和检察官之间的协调人网络；

(七) 协调和理顺与司法协助有关的程序，并制定一个共同模板，以加快程序，及时收集和移交跨境电子证据；

(八) 举办讲习班和研讨会，以加强执法当局和司法当局在司法协助条约范围内起草请求书的能力，以收集与网络犯罪有关事项的证据；

(九) 制定与收集和移交数字证据有关的程序方面的标准和统一做法；

(十) 制定在网络犯罪调查和证据收集方面与服务提供商分享信息安排的共同办法；

(十一) 通过公私伙伴关系与服务提供商接触，以建立执法、网络犯罪调查和证据收集方面的合作模式；

(十二) 制定服务提供商协助执法机构调查网络犯罪的准则，包括保存数字证据和信息的格式和期限方面；

(十三) 通过能力建设和技能发展方案，加强执法机构、法官和检察官的技术和法律能力；

(十四) 向发展中国家提供援助，协助其加强网络取证能力，包括建立网络取证实验室；

(十五) 举办讲习班和研讨会，以提高对应对网络犯罪最佳做法的认识；

(十六) 设立一个国际机构，以验证和认证数字取证工具，编写手册并加强应对网络犯罪的执法和司法对策的能力；

(p) 各国应投资于建立和加强数字取证能力，包括培训和安全认证，以及信息安全管理系统，通过检查电子设备以便以可靠的方式收集证据，为成功地起诉网络犯罪提供支持；

(q) 在采用审问模式的法律制度中，司法人员也是调查人员，司法人员应接受关于网络犯罪的专门培训；

(r) 一些法官不熟悉数字证据，因此，这类证据在认证和可采性方面往往须服从更高的标准。但是，应当考虑到这样一个事实，即没有实际理由对数字证据的完整性规定比传统证据更高的标准。数字证据被篡改或伪造的可能性不大于传统证据。事实上，可以说篡改或伪造数字证据更难，因为有各种数学算法，如“散列值”，可用来验证或提供篡改的证据；

(s) 各国应提高国内机构间相互协调和协同的效力，包括与私营部门、民间社会组织和其他利益攸关方分享可信的信息和情报，以促进有效的国际合作与协作；

(t) 各国应颁布新的或加强现有的立法，以便有可能承认电子证据的可采性，并界定和确定电子证据的范围；

(u) 各国可考虑在国内立法中将下列数据作为电子证据：流量数据，例如日志文件；内容数据，如电子邮件；用户数据，如用户注册信息；以及以数字格式储存、处理和传送的其他数据，这些数据是在犯罪过程中产生的，因此可用来证明该犯罪的事实；

(v) 鼓励各国加强收集电子证据的能力建设，建立具备法律和技术专门知识的专业团队，并加强这方面的经验分享和培训合作。鼓励毒品和犯罪问题办公室在这些努力中发挥作用；

(w) 鼓励各国在国内立法中确立收集电子证据的相关方法，例如扣押和保全原始存储介质、现场收集、远程收集与核实。鼓励会员国冻结电子证据，以防止通过计算电子证据的校验和、锁定网络应用程序账户和采用写保护等措施来增加、删除或修改电子证据；

(x) 鼓励各国制定收集电子证据的技术规范和标准；

(y) 各国应确保电子证据的收集符合正当程序；

(z) 各国应在国内立法中制定评估电子证据的真实性、完整性、合法性和相关性的规则，并在适用关于原始证据、传闻证据和排除非法证据的规则时考虑到电子证据的独特性；

(aa) 在国外收集电子证据时，各国应尊重数据所在国的主权，遵守正当程序，并尊重相关个人和实体的合法权利。在这方面，各国还应避免单方面使用侵入性或破坏性技术调查措施；

(bb) 鼓励各国与其他国家协商，通过优化相关程序和方法，进一步改进国际司法协助和执法合作，为调查网络犯罪和收集电子证据提供便利；

(cc) 各国应考虑通过与收集电子证据有关的调查权的国际示范条文，并探讨是否可能在联合国框架内谈判一项关于打击网络犯罪的有约束力的全球文书。该文书可包括关于跨境收集电子证据的普遍接受的规定。

### 三. 审议情况概要

#### A. 执法和调查

12. 在 2019 年 3 月 27 日和 28 日举行的第 1、第 2 和第 3 场会议上，专家组审议了题为“执法和调查”的议程项目 2。

13. 讨论由以下专题主讲人主持：Shenkuo Wu 先生（中国）；Ioana Albani 女士（罗马尼亚）；Martin Gershanik 先生（阿根廷）；Pedro Verdelho 先生（葡萄牙）；Anton Kurdyukov 先生（俄罗斯联邦）。

14. 在随后的辩论中，专家组审议了据称在数字环境中进行的犯罪活动实例，刑事司法从业人员和调查人员对这些活动启动或进行调查及随后进行起诉都遇到了很大困难。这些实例包括网上欺诈、将互联网用于恐怖主义目的、利用暗网实施非法活动，以及通过滥用信息和通信技术对儿童进行性虐待和性剥削。此外还向专家组通报了网络犯罪与网络安全在概念上的相互依存关系和区别，以及与网络犯罪有关的趋势和挑战，包括勒索软件攻击；用于实施欺诈的社交工程策略（网络钓鱼、鱼叉式网络钓鱼、语音钓鱼、短信欺诈）；利用 Colbalt Strike 平台攻击银行系统；物联网；加密电子货币挖掘和密码劫持；以及盗读银行卡和相关犯罪。

15. 会上再次讨论了是否需要一项关于网络犯罪的综合性全球法律文书，还是各国应侧重于有效执行包括《布达佩斯公约》在内的现有文书等议题。一些发言者认为不需要新的网络犯罪法律文书，因为《布达佩斯公约》提供了适当框架，足以制定适当的国内和国际对策打击网络犯罪。有与会者指出，已有 63 个缔约国加入《布达佩斯公约》，这表明该《公约》开放供非欧洲委员会成员加入。还有人指出，一些非《公约》缔约国的国家从中获得启发，统一国内实质性和程序性的立法标准。还有与会者指出，“统一国家标准”的概念不仅包括趋同和通用定义的情况，还包括国际规范有助于制定国家规章的情况。会上提到《布达佩斯公约》与其他区域文书互为补充，例如 2014 年通过的《非洲联盟网络安全和个人数据保护公约》和上海合作组织（上合组织）发布的《信息安全国际行为准则》。

16. 但其他发言者认为，需要在联合国框架内制定一项关于网络犯罪的全球法律文书，以应对互联网技术的快速发展所带来的、现有机制并未涵盖的挑战，而且也并非全世界所有国家都加入了现有机制。据强调，这样一项文书被设想为联合国所主导进程的一部分，在这一进程中，所有会员国都可在评估或借鉴《布达佩斯公约》和上述《非洲联盟公约》等现有文书的基础上，对高效地努力达成打击网络犯罪全球对策确立自主权并承担责任。在这方面，提到了大会 2018 年 12 月 17 日关于打击为犯罪目的使用信息和通信技术行为的第 73/187 号决议，该决议授权秘书长征求会员国关于本国在打击为犯罪目的使用信息和通信技术行为方面所遇挑战的意见，并根据这些意见提交一份报告供大会第七十四届会议审议。另有与会者认为，《布达佩斯公约》不够透明和包容，没有回应所有会员国的关切，其中规定的案文修正程序既复杂又不透明，考虑到网络犯罪不断演变的特性，这可能是一个不利因素。

17. 会上提到正在为通过《布达佩斯公约》第二项附加议定书进行谈判，该议定书旨在就下列部分或全部问题提供明确的规则和更有效的程序：有关更高效快速地开展国际合作的条款；允许针对索要用户信息的请求、保全请求和紧急请求与位于其



他管辖区的服务提供商直接合作的条款；为跨境获取数据的做法提供框架和有力保障，包括数据保护要求。

18. 还有与会者强调，《有组织犯罪公约》可用作应对网络犯罪挑战的有用工具，特别是考虑到这些挑战的跨国性质。会上建议考虑谈判制定一项专门处理网络犯罪问题的《有组织犯罪公约》附加议定书。

19. 各代表团和专题主讲人向专家组介绍了各国成功实施法律措施和程序措施打击网络犯罪的情况。一些发言者认为，《布达佩斯公约》和相应的能力建设项目是该领域的基本构成部分。会上深入审议了国家一级的立法改革问题，包括此类改革的范围。有与会者提请注意，为确保考虑到不同利益攸关方的意见，需要具有包容性和参与性的进程。有与会者提到，有必要在“法无明文不为罪”原则的基础上确保法律的确性和明确性，还有必要在新的立法中使用技术中性的语言，以便与信息通信技术领域的迅速发展保持一致。

20. 会上还围绕属地管辖权冲突产生的挑战展开了讨论，其中特别讨论了下述情况，例如，服务提供商的总部设在一个管辖区，而数据控制人位于另一个国家，或者数据存储于另一个管辖区或多个管辖区。据指出，云计算的出现为刑事调查带来了更多的实际挑战和法律挑战。另有与会者指出，似宜采用灵活的办法在网络犯罪领域适用管辖权依据，其中包括更多地以信息通信技术服务提供地为准则，而不以数据所在地为准则。

21. 专家组还强调，需要有适当的程序性权力来获取电子证据，包括调查网络犯罪和其他形式犯罪所需的数据和元数据。这种电子证据可包括用户信息、内容数据或流量数据等。据指出，在对涉及电子证据的犯罪开展调查时，匿名软件、高级加密和虚拟货币等新的技术发展造成了难题，调查人员可能需要采取新的战略，并考虑如何利用特殊侦查手段和远程数字取证来收集此类电子证据，同时确保此类证据在法庭上的可采性和使用。会上认为需要优先加强总检察长或特别检察官办公室等国家主管当局的协调作用。

22. 会上还着重讨论了如何在有必要采取有效执法对策打击网络犯罪与保护基本人权，特别是隐私权之间取得平衡。数据保留条例可能是一种务实的办法，可确保通信服务提供商能够更好地配合执法，从而在应对网络犯罪方面发挥更大的作用，但条件是执行这些法律需要配以适当的程序保障措施和隐私保护措施。会上提到联合国人权事务高级专员办事处关于数字时代的隐私权的报告（[A/HRC/27/37](#)），该报告已按照大会第 [68/167](#) 号决议提交人权理事会。

23. 专家组重申有必要在跨国界调查和起诉网络犯罪方面开展国际合作。一些发言者指出，为获取或保全电子证据而提出的司法协助请求数量正在迅速增加，传统的合作模式，特别是被一些人视为冗长的司法协助程序，无法为快速获取数据提供便利。其他人指出，司法协助仍是跨境共享数据的重要工具。一些发言者还指出，关于司法协助相关要求的能力建设和培训，包括起草附有充分信息的综合请求书以求获得电子证据，对确保及时获取数据来说是必不可少的。此外，一些国家建议使用 [24/7](#) 网络来请求迅速保全数据，因为此类证据不是固定不变的，只需点击鼠标即可转移或删除。

24. 会上列举了促进电子证据相关国际合作的多种做法，特别是业务上的做法，其中包括：合作国主管当局之间直接传递司法协助请求；更经常地使用因地制宜的国

际合作工具，以保障电子证据的完整性，例如快速保全计算机数据；联合调查；使用电子手段传递司法协助请求，特别提到刑警组织以电子方式安全传输司法协助交流信息的举措可发挥的潜在效用；24/7 网络联络点之间的信息共享；以及更频繁地利用警方之间的合作，包括借助国际刑警组织的援助，以便进行情报收集工作。会上还提到了欧洲打击网络犯罪中心，该中心是欧洲联盟执法合作署在 2013 年设立的，目的是加强欧盟内部打击网络犯罪的执法对策。

25. 专家组还简短讨论了跨境获取数据的问题。据指出，总体而言，各国所采用的做法和程序，以及这些做法和程序相关的条件和保障均大不相同。有与会者对跨境获取数据的某些做法可能引发的法律问题表示关切。此外，还强调了嫌疑人的程序性权利、隐私考虑和个人数据保护、访问存储在另一管辖区的数据的方法和合法性以及对国家主权原则的尊重。

26. 专家组强调，必须进行可持续的能力建设，提高所有行为方在业务层面的效力和技能，以应对网络犯罪带来的挑战。在这方面，发言者提到，国内外从业人员之间交流良好做法和经验是有益的。一些发言者提到在检察机关和执法当局内加强培训和能力建设，同时建立专门的打击网络犯罪机构或单位。在这方面强调指出，随着电子证据在其他形式犯罪调查中也越来越普遍，非常有必要建立专门机构，利用特定专长、知识和业务技能调查这些犯罪。

27. 专家组进一步讨论了必须促进和加强国家当局与私营部门，特别是通信服务提供商和互联网服务提供商之间的合作，以便加强对数据的保全和获取。在国内开展这种合作日益重要，特别是在涉及严重犯罪的紧急情况下，更是如此，但同时也承认需要做出更多努力，以确保在跨国案件中进行类似程度的合作。在这方面，会上提到了通信服务提供商和互联网服务提供商需要遵守的规定可能相互抵触的问题，换言之即这些提供商应如何根据所涉国家的法律要求平衡其对策。

28. 许多发言者报告了在以下各方面采取的国家措施：制定和执行网络安全战略和政策；颁布和（或）改进关于网络犯罪的立法；采用新的调查工具，以收集电子证据，并为在刑事诉讼中用作证据而确立其真实性，同时考虑到人权保障措施；实施旨在确保更有效地利用资源打击网络犯罪的体制安排；以及促进打击网络犯罪的国际合作。一名发言者表示，网络安全与网络犯罪之间的区别是在制定国内对策和界定有关这些事项的机构权限时主要考虑的一项因素。

29. 许多发言者支持专家组的工作，认为它是唯一一个全面的、最适当的全球论坛，可促进会员国之间就国家立法、最佳做法、技术援助和国际合作进行讨论和交换意见，以期探讨各种可选办法，用以加强各国和国际打击网络犯罪的法律对策和其他对策。会上还提到了委员会在这方面增添的价值。有与会者表示，专家组负有作为这一议题讨论平台的独特任务；但不一定因此排除旨在发展打击网络犯罪综合全球治理的其他举措。

30. 有与会者表示支持毒品和犯罪问题办公室在技术援助和能力建设领域开展工作，以形成有凝聚力的网络犯罪对策。

31. 此外，一些发言者还对《跨境索取电子证据实用指南》的发布表示赞赏。该《指南》由毒品和犯罪问题办公室、反恐怖主义委员会执行局和国际检察官协会共同起草和发布，并通过毒品和犯罪问题办公室的打击犯罪信息与法律网络共享平台门户网站提供给会员国及其刑事司法官员。该《指南》是与会员国、国际和区域组织以

及脸书、谷歌、微软、优步等通信服务提供商合作拟订的，其中所载信息介绍了在国家一级为收集、保存和共享电子证据可采取的步骤，其总体目标是确保司法协助工作的效率。

## B. 电子证据和刑事司法

32. 在3月28日和29日举行的第4和第5场会议上，专家组审议了题为“电子证据和刑事司法”的议程项目3。

33. 讨论由以下专题主讲人主持：Xiaofei Zhai 先生（中国）；Markko Kunnapu 先生（爱沙尼亚）；Camila Bosch 女士（智利）；Giuseppe Corasaniti 先生（意大利）；Vadim Smekhnov 先生（俄罗斯联邦）；Briony Daley Whitworth 女士（澳大利亚）。

34. 在随后的辩论中，与会者指出了电子证据的双重作用。一方面，会上承认技术和数字基础设施的应用使犯罪者有更多机会依赖网络和借助网络实施严重的、有组织的罪行，扩大了其非法活动的范围，使更多受害者沦为目标，并且增加了犯罪者的得益。另一方面，会上也强调，电子证据在侦查、调查和起诉所有类型的犯罪方面变得越来越重要。

35. 很多发言者提到电子证据在刑事诉讼中日益重要，并介绍了各国在界定此类证据的范围方面的不同做法。一些发言者指出，电子证据在国际一级尚无公认的定义，而在国家一级制定有关此类证据及其可采性的规则是会员国的特权。发言者提请注意有必要制定程序性立法，授权主管执法当局有效收集电子证据，同时规定须遵守保密、隐私、人权、正当程序和其他法律保障。会上指出，调查权力可以是传统的程序性权力和一般性调查权力，也可以是各类特定的数字调查手段。

36. 与会者一致认为，网络犯罪和数字调查的关键步骤之一是维护电子证据的完整性，并确保其真实性和在相关刑事诉讼中作为证据的可采性。在这方面，会上提到了处理电子证据的国家标准、程序和要求。专家组再次强调，有必要建设主管当局的能力和技术知识，以切实有效地应对相关挑战。

37. 专家组审议了评估电子证据可采性的相关因素，并强调了在网络犯罪调查中使用特殊侦查手段必须遵守相称原则，包括动用卧底特工和远程取证，特别是利用暗网使用上述手段时，均须遵守该原则。据指出，在许多国内法律制度中，主要由监督调查的司法当局以及酌情由法院检验该原则的遵守情况。可以根据以下因素来确定相关性：所涉罪行的严重程度或隐私受到所用特殊侦查手段侵犯的人数；所涉电脑数据的类型；是否存在限制性较小的替代措施；是否在决策过程中采取了确保程序公正的措施；以及受影响者是否有充分的机会可获得法律补救。

38. 有与会者提请注意软件和应用程序中内置加密技术的兴起，这使得在没有适当解密密钥的情况下获取用作电子证据的数据既困难又耗时。与会者就如何克服这一问题提出了切实可行的建议，包括与其他可能具备获取加密信息能力的国家合作、利用欧洲打击网络犯罪中心以及与相关行业进行合作，这些做法可建立能够及时获取加密数据的机制。

39. 会上还提到了人工智能在调查中的应用，其中特别提到了面部识别和鉴定侵犯版权行为。总体来说，人工智能可提供解决方案，使人们在海量数据中筛寻重要电子证据时，能够更有效地利用时间和资源。

40. 与会者讨论了用户信息，认为这是刑事司法当局在对网络犯罪和其他涉及电子证据的案件进行刑事调查时最常寻求的数据类型。在这方面，许多发言者提到了在获取相关用户信息方面的挑战，这些用户信息涉及在刑事犯罪中用到的具体互联网协议地址。会上指出，虽然静态互联网协议地址是稳定的，并在服务安排期间分配给某一特定用户，并且服务提供商可在用户数据库中查找此类信息，但服务提供商可能会将一个互联网协议地址分配给多个用户。因此，有必要确定某一互联网协议地址在特定时段分配给了哪个用户。还有人指出，之所以动态分配互联网协议地址，是因为根据互联网协议第四版，可用的地址数量有限。一旦向互联网协议第六版的过渡完成或升级后，这个问题就会得到解决。

41. 与会者还讨论了区分所索要数据的不同类型，及其对获取电子证据国际合作机制的有效性和及时性产生的影响。会上审查的解决方案主要涉及加强执法合作、继续推进关于跨国获取计算机数据的多边对话以及根据《布达佩斯公约》第 18 条第 3 款中的定义，单独建立一个用户信息获取制度。

42. 很多发言者提到了电子货币给网络犯罪调查工作带来的挑战。向专家组通报了毒品和犯罪问题办公室开设的电子货币调查培训师培训课程。该培训旨在提高执法官员、分析人员、检察官和法官应对电子货币的能力，包括在金融调查中追踪比特币、定位信息来源和合作开展国际个案工作等能力。

43. 在议程项目 3 下，一些发言者讨论了管辖权问题，其中特别提到了国家判例最近的一些动态，涉及当计算机数据存储于位于其他管辖区的云服务器时对属地原则的解释问题。

44. 发言者一致认为，国际合作对在跨境调查中收集和共享电子证据来说至关重要。会上强调，各国应充分利用《有组织犯罪公约》和打击网络犯罪的相关多边、区域和双边条约和安排，以便在相关案件中促进司法协助和执法方面的国际合作，同时遵守主权、平等和互惠原则。会上强调了促进联网交流经验和专门知识具有重要意义，特别是有助于应对各国对此类证据的可采性、作为证据应具备的完整性和真实性的要求各不相同所带来的挑战。

45. 许多发言者认为，第一要务是需要国家执法和刑事司法系统内进行可持续能力建设，包括针对参与国际合作的中央当局从业人员进行能力建设。有人指出，无论是在人力资源、基础设施和设备方面，还是为了弥合发展中国家与发达国家之间的数字鸿沟，这种能力建设都是必不可少的，特别是对发展中国家来说，更是如此。会上一致认为，总而言之，随着技术和犯罪手法继续快速更新，对执法和刑事司法行为方进行打击网络犯罪能力建设将是一个持续不断的进程。因此，绝大多数发言者都提到技术援助与合作是加强国内能力、促进共享良好调查做法和经验以及传播新技术的重要先决条件。

46. 在这方面，一些发言者提到法证领域资源有限，缺乏通常耗资不菲的法证工具和设备，而且收集到的供分析的数据体量庞大，这些问题造成了诸多挑战。还有人报告了在征聘技术足够娴熟的人员方面遇到了挑战。

### C. 其他事项

47. 在 2019 年 3 月 29 日举行的第 6 场会议上，专家组审议了题为“其他事项”的议程项目 4。

48. 一位发言者要求提供资料，介绍关于打击为犯罪目的使用信息和通信技术行为的报告，该报告将根据大会第 73/187 号决议提交大会第七十四届会议。对此，秘书处的一位代表提及该决议所载任务授权，强调已于 2019 年 2 月 13 日向会员国发出普通照会，请会员国提供资料，说明本国在打击为犯罪目的使用信息和通信技术行为方面所遇到的挑战，并且通报会员国这些资料将被用来编写上述报告。提交国家反馈意见的截止日期定为 2019 年 4 月 12 日星期五。秘书处将在截止日期之后汇编收到的反馈意见，以期在 2019 年 5 月完成报告。

## 四. 会议安排

### A. 会议开幕

49. 专家组副主席 André Rypl（巴西）以专家组第五次会议主席的身份宣布会议开幕。

### B. 发言情况

50. 以下会员国的专家作了发言：阿尔及利亚、阿根廷、亚美尼亚、澳大利亚、白俄罗斯、巴西、布基纳法索、加拿大、智利、中国、哥伦比亚、哥斯达黎加、多米尼加共和国、厄瓜多尔、爱沙尼亚、法国、格鲁吉亚、德国、印度、印度尼西亚、伊朗伊斯兰共和国、意大利、日本、约旦、科威特、马来西亚、毛里塔尼亚、墨西哥、摩洛哥、荷兰、尼日尔、尼日利亚、挪威、巴拉圭、秘鲁、菲律宾、俄罗斯联邦、塞尔维亚、斯洛伐克、南非、西班牙、斯里兰卡、泰国、阿拉伯联合酋长国、大不列颠及北爱尔兰联合王国、美利坚合众国和越南。

51. 来自以下两个政府间组织的代表也作了发言：欧洲委员会和欧洲联盟。

### C. 通过议程和其他组织事项

52. 在 2019 年 3 月 27 日第 1 场会议上，专家组通过了以下临时议程：

1. 组织事项：
  - (a) 会议开幕；
  - (b) 通过议程。
2. 执法和调查。
3. 电子证据和刑事司法。
4. 其他事项。
5. 通过报告。

#### D. 出席情况

53. 来自 105 个会员国、联合国预防犯罪和刑事司法方案网的一家研究所、毒品和犯罪问题办公室、政府间组织和私营部门的代表出席了会议。

54. 与会者名单载于 [UNODC/CCPCJ/EG.4/2019/INF/1/Rev.1](#) 号文件。

#### E. 文件

55. 除了关于网络犯罪问题及会员国、国际社会和私营部门就此问题所采取对策的全面研究报告草稿外，专家组还收到下列文件：

(a) 临时议程说明 ([UNODC/CCPCJ/EG.4/2019/1](#))；

(b) 主席根据预防犯罪和刑事司法委员会第 26/4 号决议提出的专家组 2018-2021 年工作计划建议 ([UNODC/CCPCJ/EG.4/2018/CRP.1](#))。

### 五. 通过报告

56. 专家组在 2019 年 3 月 29 日第 6 场会议上通过了报告 ([UNODC/CCPCJ/EG.4/2019/2](#))。