联合国 A/74/130

大会

Distr.: General
30 July 2019
Chinese
Original: English

第七十四届会议
临时议程*项目 109
打击为犯罪目的使用信息和通信技术行为

打击为犯罪目的使用信息和通信技术行为

秘书长的报告

摘要

本报告系根据大会题为“打击为犯罪目的使用信息和通信技术行为”的第73/187号决议编写。在该决议中，大会请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。

本报告载有会员国根据上述决议提交的意见资料。

* A/74/150。

目录

一. 导言

1. 大会在其题为“打击为犯罪目的使用信息和通信技术行为”的第 73/187 号决议中，请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。

2. 根据这一要求，秘书处分别在联合国毒品和犯罪问题办公室（毒品和犯罪问题办公室）于 2019 年 2 月 13 日和 2019 年 3 月 19 日签发的 CU 2019/55/DTA/OCB/CMLS 号和 CU 2019/90/DTA/OCB/CSS 号普通照会中请会员国提交资料，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面临的挑战。秘书处告知会员国，这些资料将用于编写关于第 73/187 号决议执行情况的报告，以提交大会第七十四届会议审议。秘书处指出，各国为本报告提交的材料不应超过 1,000 个英文单词，但会员国可能提交的任何法律案文或立法文本除外。提供提交材料所附的法律案文和（或）立法文本将在打击犯罪信息与法律网络共享平台（夏洛克数据库）知识管理门户网站上发布，作为补充信息资源。

3. 以下会员国应邀提供了意见：阿根廷、亚美尼亚、澳大利亚、奥地利、白俄罗斯、多民族玻利维亚国、博茨瓦纳、巴西、加拿大、中国、哥伦比亚、哥斯达黎加、捷克、朝鲜民主主义人民共和国、萨尔瓦多、爱沙尼亚、法国、格鲁吉亚、德国、加纳、匈牙利、印度、伊朗伊斯兰共和国、伊拉克、爱尔兰、以色列、意大利、日本、约旦、黎巴嫩、列支敦士登、马来西亚、蒙古、摩洛哥、缅甸、荷兰、新西兰、尼加拉瓜、挪威、秘鲁、菲律宾、葡萄牙、卡塔尔、罗马尼亚、俄罗斯联邦、沙特阿拉伯、塞尔维亚、新加坡、斯洛伐克、斯洛文尼亚、南非、西班牙、斯里兰卡、瑞士、阿拉伯叙利亚共和国、塔吉克斯坦、泰国、土耳其、大不列颠及北爱尔兰联合王国、美利坚合众国和委内瑞拉玻利瓦尔共和国。

4. 这些意见体现在秘书处编写的下文所载概要中。提交的材料涵盖国家和国际一级面临的挑战，也涵盖为解决这些挑战所采取的行动，包括在现行专门机制的框架内。会员国提供了关于技术性挑战和技术相关挑战的资料，并分享了应对这些挑战的经验。它们还强调了在打击为犯罪目的使用信息和通信技术方面开展国际合作的重要性。

二. 从各国政府收到的答复

阿根廷

5. 阿根廷指出，各国在打击为犯罪目的使用信息和通信技术行为方面面临的最大挑战包括：

(a) 国际文书的范围。除了《欧洲委员会网络犯罪公约》之外，尚未通过有关这一主题的其他国际协定。阿根廷正在为欧洲委员会网络犯罪公约委员会的活动做出积极贡献，并建议尚未加入该《公约》的国家考虑加入，以加强实施该《公约》和促进非欧洲委员会成员国的国家遵守该《公约》。然而，考虑到网络犯罪现象的全球性以及建立全球应对机制的必要性，阿根廷支持《欧洲委员会公约》框架内的各项进程和力求在联合国框架内推进就该事项谈判一个普遍法律框架的讨论；

(b) 在跨境获取数字证据方面面临的困难。在大多数案件中遇到的主要困难

是，构成证据的数据所在管辖区域与进行刑事诉讼的管辖区域不同，而且几乎在所有案件中，这些数据都为私人公司所有。迄今为止，为这些问题提出的解决方案均未充分涉及到解决第三国的需求问题，例如，美国的《澄清海外合法使用数据法》（已生效）和欧洲联盟的电子证据倡议（正在进行中）；

(c) 衡量在交流信息和良好做法方面所取得成果的能力不足。在很多情况下，难以衡量在按照协议规定交流良好做法和信息方面的成果；

(d) 在更新与技术进步有关的监管框架方面存在困难。不断更新刑事监管框架，包括在实质和程序两个方面，都会带来许多困难，而这些困难在拥有成文法体系的国家更为严重；

(e) 民众和组织的认识水平低。打击犯罪的一个重要方面与预防有关。在网络犯罪中，预防与提高人们和组织对使用信息和通信技术所带来的风险和威胁的认识直接相关。有必要制定国家认识计划，确保在该计划下制定的私营和公共部门的努力与举措具有一致性，并能优化资源使用。

(f) 私营部门的责任。私营部门在应对网络犯罪构成的挑战方面发挥着十分重要的作用。企业责任涉及平台和设备数据脆弱性的控制和管理以及为犯罪目的使用社交网络等方面。除了私营部门的自愿合作之外，还有必要分析强制性合规规则的必要性；

(g) 风险不断增加。成本较低且能够在没有最低安全级别的情况下访问互联网的“智能”设备的大量使用增加了潜在攻击的土壤和网络犯罪的范围。为应对这一挑战，国家政策和企业责任战略需要互为补充。由国家驱动并且旨在建立设备和（或）应用程序的信息解密机制以及后门机制的项目必然存在风险。各司法机构提出的信息渗透和信息提取或监测工具也需要评价。

6. 阿根廷确定其在调查和起诉利用信息和通信技术实施的犯罪方面面临以下主要挑战：

(a) 培训整个刑事司法系统的行为体；

(b) 需要为司法机关和执法人员配备适当的计算和调查取证工具；

(c) 缺少犯罪行为的法律定义或没有将犯罪行为确立为刑事犯罪；

(d) 考虑到数字证据特殊性的程序规则；

(e) 完善国际合作机制；

(f) 加强私营部门公司（互联网服务提供商）的合作。

7. 阿根廷还表示，在网络犯罪领域以及在收集数字证据方面开展培训是确保有效刑事起诉面临的最大挑战。应集中努力拓宽系统操作人员的知识，从而更好地适用现行法律和国际文书。这不仅将确保有效应对这些犯罪，还将确保尊重诉讼当事方的基本权利。

8. 阿根廷重视联合国（通过毒品和犯罪问题办公室）、美洲国家组织、欧洲联盟和欧洲委员会等国际和区域组织在分享最佳做法和经验方面的贡献。目前，司法部正在努力制定获取数字证据的示范程序规则，作为联邦立法和省立法的依据。

9. 阿根廷是一个联邦国家，而这意味着联邦司法系统与 24 个省级司法系统并存。这导致它难以应对网络犯罪和数字证据等复杂的国际现象。设立专门的财政单位是一项非常有用的做法。正在做出努力以确保国内不同司法管辖区都采用这一模式并加快调查和信息交流。

10. 阿根廷还介绍了其面临的另一项挑战，即缺少实行司法机关和安全部队内部所需转型的财政资源，其中包括在国家政策层面作出可持续的努力。

亚美尼亚

11. 亚美尼亚表示，相关国家机构和政府机构稳步采取措施，以应对使用信息和通信技术实施犯罪行为所产生的不断变化的风险，并为此改进部门立法，包括为此与联合国专门实体、欧洲安全与合作组织、欧洲联盟和欧洲委员会进行持续对话，以及在独立国家联合体反恐怖主义中心、集体安全条约组织和国际刑事警察组织（国际刑警组织）框架内加强合作与信息交流。

12. 亚美尼亚报告称，它设想在 2019 年至 2020 年期间设立一个机构间工作组，以期在信息和网络安全领域制定概念、国家战略和行动计划。工作组将酌情由政府官员和专家、科研机构、基金会以及民间社会和私营部门组织组成。

13. 亚美尼亚还报告称，已经起草关于修订《刑法》和《刑事诉讼法》的法律草案，预计这两部法律草案将在不久的将来获得通过。这些法案规定了对有关使用计算机系统实施犯罪的条文的修正和补充。在起草《刑事诉讼法》草案的过程中，与欧洲委员会的警方专家代表举行了一系列会议。

14. 亚美尼亚定期评估本国内洗钱和资助恐怖主义的风险。最新一次的即对 2014-2017 年期间的评估于 2017 年进行。对《2014 年洗钱和资助恐怖主义风险国家评估报告》[1]进行了分析和更新，揭示了与使用信息和通信技术有关的某些洗钱风险。分析结论表明，新产品和货币交付机制（如在线销售点终端、电子银行、手机银行和数字钱包）被越来越多地用于建立业务关系或进行复杂且异常庞大的交易。

15. 亚美尼亚指出，与使用销售点终端和电子银行系统有关的产品和服务在查明业务关系中可能出现的风险方面存在不足。特别是，一旦与客户建立了业务关系并采取了必要的初始客户尽职调查措施，客户的后续业务活动将在在线环境中进行，不涉及与相关银行员工（前台）的面对面接触。在这种关系中，查明可疑活动的机会较少。此外，从外国银行发行的银行卡中窃取的数据可用于注册数字钱包账户，并通过输入一组有效的银行卡标识符（卡号、到期日、银行卡验证码）来激活数字钱包账户。因此，犯罪人能够在不经过强制性客户尽职调查程序的情况下获得金融服务。注册的数字钱包随后可用于进行多笔电汇，以期掩盖犯罪所得的来源，并且随后转移账户上的可用余额。

16. 考虑到已确定的风险动因和因素，亚美尼亚中央银行金融监测中心一直在采取相关预防和威慑措施，包括向特定金融机构下达相关任务和指示。

[1] 洗钱和资助恐怖主义风险国家评估是要对一些出现重大动态的部门所面临的威胁和脆弱性进行评估，并由专家就此提出建议，作为欧洲委员会评价反洗钱措施和打击资助恐怖主义行为专家委员会对亚美尼亚打击洗钱和资助恐怖主义行为的制度进行相互评价的一部分。执行摘要可查阅：www.cba.am/Storage/EN/FDK/risk_assesment/NRA_Update_Executive_Summary(Public)_eng.pd。

17. 警方打击有组织犯罪总局打击高科技犯罪司在 2018 年期间启动 79 项刑事案件调查。其中 70 起与高科技犯罪有关，另外 9 起是依据其他条款立案的，与信息和通信技术的使用密切相关。

18. 警方开展的一项研究表明，根据亚美尼亚《刑法》第 181 条（通过计算机实施的盗窃）和第254条（非法挪用计算机数据）提起的刑事诉讼有所增加。研究表明，第181条所涵盖行为的受害者既有个人，也有法律实体，而第254条所涵盖犯罪的受害者大多是社交网络或电子邮件服务的用户。这些罪行的披露主要与其在国外实施或犯罪痕迹隐藏在几个国家的服务器系统上有关。因此，在这种情况下，调查工作因不同国家的立法不同而变得复杂。因此，提出请求的执法机构一般无法获得请求提供的信息。

19. 根据《欧洲委员会网络犯罪公约》的相关规定，警方内部的国家联络点已为发现和揭露非俄语社交网络的用户采取措施。与行动或刑事案件有关的查询可通过“每周 7 天，每天 24 小时”联络点网络进行。正如亚美尼亚所报告的，在接到请求（口头或书面）后，有专门的分部[2]向地区警察分部提供有关部门问题的专业援助和咨询意见。此外，还对各地区警察部门的负责人进行了一次培训，对计算机犯罪的特点和收集证据的过程进行了详细说明。

20. 来自专门警察分部的官员访问了相关国际组织，并参加了为其量身定制的讲习班和研讨会，以研究打击网络犯罪的最佳做法。[3]在集体安全条约组织行动代理框架内，亚美尼亚作出了适当的组织安排，旨在打击使用信息和通信技术实施犯罪。警察部队一直在开展活动，旨在提高对与信息和通信技术有关的各类问题的认识。[4]

21. 专门警察分部对亚美尼亚域名区和大众社交网络的亚美尼亚部分进行监测，以便进行犯罪侦查。监测不仅限于发现网络犯罪（例如勒索软件），还涉及只利用互联网作为犯罪实施手段而不是直接工具的犯罪行为（如敲诈、勒索和强迫自杀）。

22. 亚美尼亚还指出，在信息安全方面，煽动基于认同的不容忍、暴力、仇恨、仇外心理及极端主义和恐怖主义做法，以及通过使用互联网尤其是在国家一级鼓励和策划时美化种族灭绝行为实施者的行为令人严重关切，这些行为会带来社会激进化的风险，导致外国恐怖主义作战人员的出现。同时，亚美尼亚强调，应该在线上和线下平等和无差别地保障包括集体权利在内的人权和基本自由，不分国界[5]和领土的法律地位。

[2] 在接到刑事案件调查任务之后，专门的分部根据有关法律开展实际查找活动，并处理公民提出的申请。

[3] 特别是在欧洲联盟和欧洲委员会联合举办的一次活动中，在东部伙伴关系基金项目 2（加强司法改革）和项目 3（打击严重形式网络犯罪的支助措施）的框架内采用了先进的打击网络犯罪的方法。此外，还讨论了《刑事诉讼法》草案、立法改革的前景以及与私营部门合作的法律依据。

[4] 这些活动包括接受各种媒体机构的采访、参加新闻发布会、印发各种新闻材料以及参与各种电视节目。

[5] 见《公民权利和政治权利国际公约》第十九条做出的规定和默示。

澳大利亚

23. 澳大利亚指出，它认为网络犯罪包括以计算机为目标的犯罪以及利用计算机实施的较为传统的犯罪。澳大利亚还强调，需要将讨论重点放在技术专门知识上。网络犯罪的挑战复杂且不断变化。应对这些挑战需要持续关注，需要网络犯罪问题技术专家的指导和建议。在这方面，澳大利亚高度重视根据大会第 65/230 号决议设立的全面研究网络犯罪问题专家组的工作。澳大利亚认为，专家组拥有联合国关于交流网络犯罪问题的相关任务授权，应继续作为讨论网络犯罪问题的主要论坛。更广泛地说，毒品和犯罪问题办公室拥有联合国关于打击跨国犯罪和毒品的相关任务授权。由于网络犯罪是一种跨国犯罪，因此，有关网络犯罪的讨论宜继续在毒品和犯罪问题办公室的主持下在维也纳集中进行。澳大利亚期待专家组 2021 年的报告，包括其关于国家立法、最佳做法、技术援助和国际合作的结论和建议。

24. 在境外数据方面，与所有会员国一样，澳大利亚报告称，其国内执法机构在访问和获取数据以有效开展网络犯罪调查和起诉方面面临挑战。数据曾经通常存储在境外，并且可在获得国内调查授权时获取。现在，由于全球互连互通和对云计算的依赖程度不断提高，数据分布于不同服务、提供商、地点和司法管辖区域。这些数据可能很难定位，只能通过复杂而缓慢的国际法律合作进程获得。对越顶通信服务的使用越来越多，这意味着有关获取电信运营商和运营服务提供商数据的传统授权无法覆盖网络犯罪调查所需的数据宽度。

25. 澳大利亚强调，《欧洲委员会网络犯罪公约》等条约办法为允许执法部门在得到拥有数据合法披露权的人员同意或在可公开获取信息的情况下获取位于他国境内的数据提供了确定的依据。除此以外的限制（包括要求国家主管机关的同意）对调查和起诉网络犯罪构成了重大挑战。

26. 司法协助等传统国际法律合作机制难以满足需求，导致网络犯罪调查出现延误。国家主管机关、执法机关以及在适当时根据国内法与通信服务提供商之间的替代性国际合作框架可以迅速提供实用的解决办法。

27. 澳大利亚报告称，除其双边和国内安排外，它还成功地利用《联合国打击跨国有组织犯罪公约》和《欧洲委员会网络犯罪公约》等多边条约作为国际法律合作的基础。关于跨境获取数据的新机制可应对不断变化的网络犯罪，比如，正在谈判的《欧洲委员会网络犯罪公约附加议定书》所设想的新机制，并将大大提高执法机构获取数据以便进行网络犯罪调查的能力。通过更高效地获取数据，可适当兼顾执法目标和数据保护目标。

28. 在保障措施和警察权方面，澳大利亚指出，有必要建立适当的监督机制，以便在保障人权和基本自由与执法实体行使调查权以打击网络犯罪的合法需要之间取得平衡。在澳大利亚，执法权受到实质性监督，特别是在行使更具侵犯性的权力时，例如获取存储的通信内容和实时窃听。这些保障措施包括对司法机关行使权力的要求、议会报告要求、被告人质疑证据可采性的权利、复审权以及对所有通讯的监督都需要得到英联邦监察员的授权。要确保在执行警察权时适当兼顾保障措施就需要不断评估和持续审查，而这在某些司法管辖区可能是一项挑战。

29. 关于法律和业务框架的适应性问题，澳大利亚强调，它致力于维持能够适应要求的国内立法框架，以期与技术和行为的快速发展保持同步。澳大利亚承认，在起草法律方面面临的挑战是，法律要涵盖各种实质性网络犯罪、网络犯罪调查的程序权和电子证据的可采纳性，但仍然适用于不断发展的技术和行为。为应对这一挑战，澳大利亚不仅在国内推动技术中立的立法，而且将其作为能力建设努力的一部分，并且在立法中考虑到未来的网络犯罪行为和技术。

30. 澳大利亚报告称，其立法和条例以《欧洲委员会网络犯罪公约》为蓝本，该公约是关于网络犯罪的主要国际文书，为开展打击网络犯罪的国际合作提供了坚实的法律和业务基础。《公约》有 63 个缔约方，其中超过一半的缔约方不是欧洲联盟成员。澳大利亚报告称，根据其经验，该《公约》是一项现代进步公约，并有意保持技术中立，这使其能够随着新技术的出现而不断发展并保持相关性。它还为全世界各区域包括目前尚未加入《公约》的国家采取国内立法办法提供了依据。

31. 澳大利亚还认为，除了将网络犯罪定为刑事犯罪的全面框架外，还需要对一线执法人员进行可持续的连续培训。培训应涉及借助技术的犯罪以及数字证据的收集和使用问题。澳大利亚认为，有必要通过能力建设方案向澳大利亚执法实体以及国际合作伙伴提供并维持可持续的最新培训。

32. 网络犯罪的性质要求与其他国家密切合作。澳大利亚发现，如果在网络犯罪问题上必须与之合作的国家能力有限，或者没有全面的国内法律框架应对网络犯罪问题，则在开展合作方面面临挑战。应对这一挑战需要各国注重加强和建设打击网络犯罪的能力，包括通过专门的网络犯罪培训。澳大利亚强调，为立法改革提供援助对发展中国家也很重要。澳大利亚向各国提供能力建设和技术援助，以协助建设其技术能力。澳大利亚还支持毒品和犯罪问题办公室网络犯罪问题全球方案所做的重要工作。

奥地利

33. 奥地利在报告打击网络犯罪方面的全球挑战时指出，网络犯罪是一个不断变化的挑战，影响到每个国家，需要一种高效率和有效力的办法来：

(a) 最大限度地增加拥有适当、相互兼容且支持国际合作的网络犯罪相关国内立法的国家数量；

(b) 建立合作机制、信任和技能，共享数据以调查、起诉和减少网络犯罪。

这包括但不限于，确保不存在网络罪犯的安全避护所，提高执法机关和司法机关对网络罪犯进行有效调查、起诉和定罪的能力。

34. 为确保整个欧洲联盟制定全面的网络相关立法，包括奥地利在内的欧洲联盟成员国同意制定一套对犯罪行为作出共同定义的文书：关于攻击信息系统行为的指令、关于打击对儿童性虐待和性剥削及儿童色情制品的指令，以及 2001 年 5 月

28 日关于打击欺诈和伪造非现金支付手段的框架决定[6]。此外，欧盟委员会还在 2018 年 4 月 17 日提出了改善刑事调查中跨境获取电子证据的立法建议。

35. 然而，获取电子证据只能被视为第一步，因为在欧洲层面缺乏共同的数据保留计划来保障电子证据的可得性。因此，欧洲联盟各成员国在电子证据的时限和数量方面差别很大，甚至可能取决于各组织的善意。在这方面，WHOIS 现状存在问题，而且仍然没有有效的解决办法，但具有相关性。《欧洲委员会网络犯罪公约》的第二项议定书将述及更好地获取电子证据的必要性。

36. 奥地利指出，2013 年，欧洲联盟执法合作署（欧警署）设立了欧洲打击网络犯罪中心，该中心为欧洲联盟成员国利用灵活的打击犯罪模式努力打击网络犯罪作出了重大贡献。奥地利表示，有必要让检察官尽早介入网络犯罪案件，并认为建立欧洲打击网络犯罪司法网等专门网络有好处。

37. 关于旨在加强现有对策和提出新的国内和国际法律对策或其他对策以应对网络犯罪的备选方案，奥地利指出，网络犯罪是一个全球性问题；每个国家都需要其他国家的协助来打击网络犯罪。奥地利认为，《欧洲委员会网络犯罪公约》是国家立法的典范和国际合作的宝贵框架，并认为它甚至为不是欧洲委员会成员的缔约方提供了可供选择的灵活文书。因此，奥地利不支持有关制定一项关于网络犯罪的新国际文书的呼吁。

38. 奥地利表示，全面研究网络犯罪问题专家组现在是而且至少在 2021 年之前应该仍然是联合国一级关于网络犯罪专题的主要进程。专家组取得了若干成果，包括在根据现行国际标准进行立法改革方面，特别是在能力建设方面。应当对 2013 年提出的网络犯罪综合研究草案进行更新，这将需要专家组的专门知识。

39. 奥地利建议毒品和犯罪问题办公室和会员国实现这些目标，还建议会员国支持毒品和犯罪问题办公室将重点放在以下能够对网络犯罪威胁产生实际影响的具体领域：

(a) 通过一般和专门培训提高警察和执法人员技能；

(b) 在发展中国家开展技术援助；

(c) 分析国际合作中的差距以确定优先领域；

(d) 支持公众宣传运动，以加强犯罪预防，并使民间社会和企业与执法实体开展合作；

(e) 加强现行业务机制，例如“每周 7 天，每天 24 小时”网络；

(f) 收集关于网络犯罪威胁的数据；

(g) 充当打击网络犯罪最佳做法和案例研究的储存库。

[6] 该框架决定不再有效。截至 2019 年 5 月 29 日，该决定由欧洲议会和欧洲理事会 2019 年 4 月 17 日关于打击欺诈和伪造非现金支付手段的第 2019/713 号指令（欧盟）所取代（《欧洲联盟公报》，L123 号，2019 年 5 月 10 日），第 18-29 页。

白俄罗斯

40. 考虑到现代毒品犯罪的现代化以及利用暗网和加密货币进行毒品贩运，白俄罗斯认为，会员国的优先事项之一应是确保在超国家一级交流信息，了解犯罪手段和在暗网上侦查犯罪活动的方法；收集和获取电子证据；以及开发和使用具体技术调查在虚拟空间中实施的犯罪。向执法人员提供关于暗网和加密产业如何运作的培训可作为打击为犯罪目的使用信息和通信技术行为的手段之一。白俄罗斯强调，有必要制定一项国际法律机制（建议），制定在法院作出裁决之前扣押非法加密资产和储存这些资产的程序。

41. 白俄罗斯指出，白俄罗斯已于 2019 年 3 月 18 日通过《信息安全概念》，对信息安全和打击网络犯罪领域的战略任务和优先事项做出了规定。《概念》系基于白俄罗斯的地缘政治利益和关于在确保国际信息安全领域开展合作的国际协定，同时考虑到大会各项决议的主要规定以及欧洲安全与合作组织的建议。

42. 白俄罗斯认为，在联合国框架内制定和通过一项具有普遍性的国际文书，将有助于会员国的主管机构在打击为犯罪目的使用信息和通信技术行为方面开展合作。

多民族玻利维亚国

43. 多民族玻利维亚国指出，技术进步对本国和世界各地人类活动的各个方面都产生了影响，也对与使用新技术有关的安全产生了影响。通过使用软件、应用程序和通信网络，信息和通信技术使传统犯罪发生变化和传播成为可能。金融机构对数字系统的依赖为欺诈等犯罪的实施提供了便利。同样，在没有登记个人资料的情况下便可轻易获取手机使匿名实施犯罪成为可能。

44. 对于多民族玻利维亚国的警察来说，预防犯罪和确保通信安全是主要优先事项。在打击犯罪特别部队内设立了一个网络犯罪司，这是一个专门侦查信息和通信技术犯罪的单位。国家执法机构有专门的单位来监测新闻和社交网络。对社交媒体进行监测的目的是防止“信息泡沫”（限制信息以便对公众舆论产生负面影响），并防止敲诈勒索、威胁、贩运人口、欺诈、网络欺凌、歧视和其他威胁国家安全的犯罪。

45. 多民族玻利维亚国报告称，儿童，特别是 12 岁至 18 岁青少年面临与使用信息和通信技术有关的风险，因为他们从小就接触到这些新技术，并经常将其用于娱乐、通信和信息。然而，儿童并不总是能从这些技术中获得教学或教育方面的好处。

46. 多民族玻利维亚国提供了以下有关滥用信息和通信技术和计算机犯罪的类型的非详尽清单，具体如下：

(a) 通过社交网络、电子邮件、甚至报纸观点版面中的评论空间进行骚扰、侮辱、诽谤和社会排斥。在学校等看似无害的环境中，通过“脸书”等发起针对某些儿童的匿名活动；通过指控卖淫等方式诽谤大学生；以及试图根据不实信息诋毁公司；

(b) 诈骗和欺诈，例如“网络钓鱼”，犯罪组织通过这种手段获得机密信息，从而进入银行账户并转走其资金。另一个例子是在线招聘工作人员，以掩护

从事贩运人口和儿童色情制品的网络。一般而言，欺诈与获取机密信息以及更改机密信息的可能性有关；

(c) 垃圾邮件。尽管垃圾邮件不一定构成违法，却是许多公司向潜在用户扩展其营销活动而将数据库不当用于商业目的的结果。它可能包含卖淫活动和其他非法活动；

(d) 儿童性虐待材料是犯罪集团在互联网上以视频和照片的形式出售的。这违反了《儿童权利公约》和《刑法》；

(e) 知识产权。人民和创新型组织的权利受到多种形式的侵犯，包括取用受保护文本的照片（版权）；

(f) 网上销售，包括所谓的彩票中介和竞赛。

47. 多民族玻利维亚国表示，随着计算机技术的发展，犯罪分子找到了能够比刑法反应速度更快地实施欺诈和其他犯罪的创新方法。面对这种与日俱增的现象，预防和保护应被视为国家、企业、组织和公民中每个人的责任。从这个意义上讲，技术创新对负责解决这些问题的机构构成了多重挑战，包括：

(a) 公众缺乏对使用信息和通信技术的认识和了解。缺乏这种认识和了解使人们更容易受到不同犯罪的影响。一个相关的挑战是如何制定适当的政策来加强对恰当使用这些技术的了解；

(b) 由于无知或现行立法不适用于涉及信息和通信技术的新型犯罪而存在法律真空。因此，有必要审查和更新立法；

(c) 鉴于涉及信息和通信技术的犯罪不断变化，需要使用新方法来修改传统的调查战略和打击犯罪对策；

(d) 需要加入关于在网络犯罪领域研究、保障和获取证据的国际合作协定。在拉丁美洲，已有几个国家成为这方面公约的缔约国，并在发展其预防和调查通过信息和通信技术所实施犯罪的技术能力方面取得了较大进展。

48. 多民族玻利维亚国回顾指出，政府机构采用新技术影响到组织文化，修改了程序并吸收了新知识。安全机构开发和实施的许多技术都需要专门知识，这可能导致这些机构向大学、技术研究所、研究中心和软件提供商等不一定属于安全领域的人员或组织开放。目前，警察部队和公民都有各种技术工具来处理安全问题和犯罪行为，在某些情况下可用于预防犯罪，在另一些情况下可帮助调查刑事案件。这些工具中有一些在公民和警察当中非常普遍，而另一些则比较昂贵，一般公众很难获得。

49. 多民族玻利维亚国总结指出，技术进步带来了新的犯罪动态，迫使机构适应并纳入创新战略，从而使它们能够领先犯罪行为体一步，通过预防和调查犯罪来保卫社会和维护公共秩序。因此，难以想象负责安全的机构会考虑在不使用技术工具的情况下面对犯罪现象。负责安全事务的机构不仅可能在内部利用各种技术工具，还可能利用它们让公民参与预防犯罪。

博茨瓦纳

50. 博茨瓦纳指出在打击犯罪方面遇到以下挑战，特别是利用信息和通信技术协助打击犯罪的挑战：

(a) 各国和管辖区域的网络犯罪和数据保护立法不统一，使得对网络空间犯罪活动的调查变得非常困难；

(b) 事实证明，不同国家的不同机构之间缺乏交换网络安全信息的国际框架致使多个管辖区域在开展网络保护和犯罪活动调查方面遇到挑战；

(c) 人工智能和物联网等新出现的技术创新具有应用于农业、医疗和气候数据分析等领域的潜力，但这些创新也提供了一个潜在的平台，网络攻击可能由此产生或通过这个平台发起；

(d) 另一个障碍或主要挑战是执法机构、服务提供者、政策制定者和监管者这些各种参与者中进行能力建设，以解决网络安全问题；

(e) 在与脸书、WhatsApp、谷歌、微软和奈飞等没有获得许可但仍在国内市场提供服务的跨国公司打交道时遇到困难。难以获得与通过其网络实施的犯罪有关的信息或证据；

(f) 博茨瓦纳和许多其他国家不是关于信息和通信技术和网络安全的现有公约（例如《非洲联盟网络安全和个人数据保护公约》和《欧洲委员会网络犯罪公约》）的缔约国，因此，很难利用这些公约寻求追诉权。《欧洲委员会网络犯罪公约》为网络犯罪和电子证据方面的国际合作提供了法律框架，应鼓励各国加入该公约；

(g) 司法协助过程缓慢而繁琐，导致博茨瓦纳和其他国家的司法效率低下；

(h) 在许多管辖区域，自愿披露网络犯罪仍然是一个障碍。获取信息的过程漫长，在某些情况下是不可能的；部分原因是各国之间没有统一获取用户信息的规则。博茨瓦纳可能解释为或认为属于犯罪的行为在另一国家可能不是犯罪。

51. 博茨瓦纳提出以下建议：

(a) 需要毒品和犯罪问题办公室、国际电信联盟和国际刑警组织等机构之间进行合作与协作，共同应对犯罪分子利用信息和通信技术网络实施犯罪的挑战。需要澄清各机构在处理网络安全问题方面的作用；

(b) 应为联合国会员国制定交换网络安全信息的国际框架；

(c) 需要制定一个国际政策和监管框架，以处理妥善利用包括人工智能和物联网在内的新技术的问题；

(d) 应为会员国制定能力建设方案；

(e) 应为跨国公司向会员国提供信息和证据并协助调查在公司网络内实施的犯罪制定一个框架；

(f) 应鼓励联合国对各国在批准关于信息和通信技术和网络安全的区域公约方面采取似乎不情愿的立场的理由进行调查；

(g) 应为建立一个更简单的司法协助框架制定一项标准，供会员国通过；

(h) 最后，需要一项国际条约来解决信息和通信技术网络中的犯罪问题。这项条约应对普遍立法、信息共享原则、最低信息安全标准和执法事项（调查、引渡和起诉）方面的援助进行统一，并提供简明指导。

巴西

52. 巴西报告称，自互联网出现以来，巴西当局一直在处理网络犯罪，而且这种犯罪的数量和复杂性都在增加。将不同罪行转移到数字平台需要做大量的工作，需要根据新威胁对立法和司法对策做出适当的更新。这些罪行的地理范围也对巴西提供和接受国际法律合作的传统机制构成挑战。挑战是巨大的：互联网服务提供商持有调查网络犯罪和收集电子证据所需的信息，经常将实体总部设在一个国家，在不同大陆提供服务，并将其信息存储在地球上任何其他地方的服务器上。在这种情况下，执法人员努力确定并及时联络对数据拥有管辖权并可直接获取这些数据的人员。国际合作请求通常是通过司法协助条约提出的，处理起来非常缓慢，而且有时因数字处理的速度太快而变得不适用。

53. 巴西还报告称，只要调查和管辖区域涉及国际内容，案件的法律进展往往会因对隐私保护的含义存在分歧而减慢，这体现在各国对数据披露有不同的要求。国际法律合作面临的另一项挑战是数字证据的极端不稳定性，因为在全球范围内传播的大量信息和存储相关成本使企业保留数据的时间不会超过其业务严格需要的时间。

54. 在巴西执法人员起诉的数字媒体众多犯罪中，儿童色情制品是最常见的一种。巴西为处理这一问题投入的精力最大，无论是通过国际刑警组织还是直接处理（例如，已经收到来自美国的 200 万份报告）。网站入侵和网络钓鱼也是经常发生的犯罪。二者都是以银行欺诈为目的，巴西金融部门采取了积极而有条理的应对措施，对银行欺诈行为进行了打击。盗窃比特币和劫持密码（如 2017 年通过 WannaCry 病毒）成为最新趋势；它们也给犯罪分类带来困难。

55. 巴西对数字证据和网络犯罪的特殊性质非常敏感。《互联网民事框架》第 11 条规定，计算机终端位于巴西境内的，在收集、存储和处理数据时必须适用巴西法律。因此，在巴西设有分支机构或向巴西用户提供服务并收集、存储、维护或处理从这些用户获得的数据的外国公司必须遵守巴西法律。这一框架使当局能够直接获取从该国提供的服务中收集的电子证据和数据。巴西的管辖权立足于在其国家境内提供服务的概念。

56. 巴西认为，虽然互联网是一个没有边界的虚拟空间，但它与现实世界的连接点存在于国家现有既定领土内。协调一致的国际管辖区域分配是在起诉网络犯罪方面向前迈出的一步。2014 年，巴西法律吸纳了针对特定目标的检验标准（类似于欧洲联盟的电子证据倡议[7]）。即使在就这一事项展开全球条约谈判之前，巴西就已经预计到未来将运用针对特定目标的检验标准的法律机制来统一国内立法问题，而不考虑服务器所在位置和保管公司的国籍。

[7] 欧洲联盟理事会 2008 年 12 月 18 日关于为获得物品、文件和数据用于刑事事项诉讼的欧洲证据令的第 2008/978/JHA 号框架决定（《欧洲联盟公报》，L 350 号，2008 年 12 月 30 日）。

57. 巴西表示，需要进行更多和更好的合作，可以采用先进方式执行现行司法协助条约，也可借助关于网络犯罪的补充条约，这将有助于加快（本质上短暂的）数字证据的国际交流。显示有网络犯罪特点的众多平台、系统和战略也要求增加技术合作。有关专家、警官、检察官和法官应该有更多机会学习经国外同行已被证明获得成功的经验和方法。

58. 巴西还表示，在联合国主持下就一项国际文书进行多边谈判可能是在现有国际和区域文书的基础上为交换信息和证据以打击网络犯罪制定共同最低标准的一种方式。这类讨论应在毒品和犯罪问题办公室的支持下在维也纳举行，毒品和犯罪问题办公室已经具备打击网络犯罪的专门知识，而且全面研究网络犯罪问题专家组已在讨论这一问题。召集一个不限成员名额专家组以开始起草一份案文可以作为制定一项网络犯罪公约的第一步。

加拿大

59. 加拿大报告说，尽管最近对本国法律进行了修订，以便能够在二十一世纪更好地打击犯罪，但这些法律仍然面临挑战。加拿大强调国际社会已采取两种方式来努力应对这些挑战的基本情况。

60. 首先，在程序方面，加拿大强调了全面研究网络犯罪问题专家组所做的重要工作。该专家组的任务是全面研究网络犯罪问题和针对此问题的对策，以期审查各种备选方案，加强针对网络犯罪的现行国内和国际法律对策或其他对策，并提出新的此类对策。这项工作正在进行，并以确保该专家组在 2021 年完成其工作的工作计划为指引。加拿大认为，该专家组的工作对联合国今后讨论应对网络犯罪的可能办法至关重要，为专家参与讨论包括网络犯罪问题国际合作和能力建设层面在内的高度技术性的网络犯罪问题提供了一个论坛。

61. 第二，从实质角度看，加拿大完全支持《欧洲委员会网络犯罪公约》，认为它是打击网络犯罪的最佳国际工具。通过目前 63 个缔约国在打击网络犯罪方面开展国际合作，包括大量和越来越多的非欧洲国家，《公约》正在有效应对全球性滥用信息和通信技术实施犯罪问题。《公约》可以适应新出现的挑战，发布指导说明以帮助缔约方将现有条款适用于网络犯罪的新现象，并辅之以“每周 7 天，每天 24 小时”网络服务和强有力的能力建设方案。《公约》缔约国也在努力加强国际合作机制，因为刑事调查越来越需要获得存储在其他管辖区域的信息。加拿大支持《公约》，并坚信它无论是作为对愿意且能够加入《公约》的国家具有法律约束力的框架，还是作为未加入《公约》的国家制定国内立法的模式，都是现有最佳选择。

62. 就新技术进步带来的挑战而言，加拿大回顾说，通信无处不在：它可以随时随地存在，也可以通过任何提供商或任何设备提供。这影响到执法问题。调查人员通常必须考虑伙伴关系安排的性质、资产所有权和实体在全球化背景下所处位置。对最终用户来说，似乎是一项服务，而这样的项目几乎总是由多种服务、多种技术、多种所有权组成，而且分布在多个司法管辖区域。

63. 此外，加拿大还指出，与信息和通信技术相关的犯罪行为仍在不断变化和调整。它变得越来越受到利润驱动，具有跨国性质，而且往往是有组织和专业化行为。犯罪活动分成较小的行为，通常由不同的罪犯实施，每个人在犯罪团伙中扮

演一个角色。这种专业化不仅增加了犯罪行为的复杂性，而且还可能提供更多的保护，因为某些构成要件在某些管辖区域可能不构成刑事犯罪。此外，犯罪要件可能分散在多个管辖区域。利用分布式网络技术的网络不仅可以利用国内司法系统的弱点，还可以使国家本身受到其属地性和主权影响。

64. 加拿大重点介绍了在国内法适用领土范围有限的情况下适用国内法面临的挑战，该国报告称，法律通常限于特定领土，这就带来了重大挑战，因为在日益数字化的世界中，边界往往无关紧要。信息和通信技术继续以令人眼花缭乱的速度发展和演变，而（涉及滥用或利用信息和通信技术的）网络犯罪也随之扩散和演变。数字证据的短暂性增加了问题的复杂性。它可以被快速删除或从一个管辖区域一键转移到另一个管辖区域。此外，令问题更难办的因素还源于重要隐私和人权关切，以及如何在数字环境中顾及这些问题。虽然传统法律规定的一些调查权在打击网络犯罪方面仍然有用，但也需要有新的或更先进的法律工具，以确保调查能力能够应对犯罪分子对此类技术的利用。

65. 加拿大指出，从实际角度来看，与从其他国家获取必要信息相关的挑战包括了解数据所在地、是否有可用数据以及数据是否全面。在某种程度上，这取决于它们是什么类型的计算机数据。某些类型的数据可以存储起来以供长期可用，而通信量数据等其他类型的数据可能比较短暂。虽然电信公司的覆盖范围是全球性的，但它们通常受国家或地区法律的约束：如何获取或保留数据，因国家而异。加拿大对一些数据保留制度感到关切，因为这些制度对隐私影响相当大，并且缺乏公众支持。加拿大认为，《欧洲委员会网络犯罪公约》提出的调查保存制度提供了一个谨慎的替代办法。此外，关于《公约》第二附加议定书的谈判也将会增进国际合作和对云数据中证据的获取。

66. 关于当前国际合作框架面临的挑战，加拿大认为，在国内和国际获取数字证据是成功调查和起诉网络犯罪和其他类型严重犯罪的关键。然而，无论数字证据多么重要，单方面越境获取数字证据的后果都会给国际关系带来压力，破坏这种证据搜集工作的有效性。

67. 加拿大指出，司法协助条约的主要目的在于获取此类信息。然而，加拿大还指出，目前的程序并非总是足够及时地满足对涉及电子证据的调查的迫切需要，也不适合因许多留下数字证据足迹的不同犯罪而产生的大量请求。加拿大认为，《欧洲委员会网络犯罪公约》中规定的互助机制是目前众多缔约国之间开展国际合作的最佳手段。另外，关于《公约》第二附加议定书的谈判也将会增进国际合作，并为从云数据中获取证据提供条约依据。

中国

68. 中国欢迎大会通过题为“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，注意到大会在几项关于预防犯罪和刑事司法的决议中强调加强打击网络犯罪的国际合作。中国建议大会在每届会议上都讨论网络犯罪这一议题，包括考虑授权建立相关的特别政府间机制。与此同时，中国表示支持在预防犯罪和刑事司法委员会框架内继续讨论网络犯罪问题。中国还支持全面研究网络犯罪问题专家组开展的工作，支持它根据其 2018-2021 年工作计划深入讨论打击网络犯

罪的实质性问题，并向预防犯罪和刑事司法委员会提出建议和结论。中国还鼓励不同的区域或国际组织积极讨论网络犯罪问题，并共同制定应对措施。

69. 在国际立法方面，中国认为，《打击有组织犯罪公约》无法有效满足对国际合作应对网络犯罪的新要求。在打击网络犯罪领域已有一些区域公约，例如，欧洲委员会、上海合作组织、阿拉伯国家联盟和非洲联盟制定的公约。由于这些公约的成员国范围和内容不同，致使打击网络犯罪的国际立法零散不全。因此，中国表示，国际社会迫切需要建立打击网络犯罪的全球法律框架，并共同努力应对日益严重的犯罪形势，特别是云计算、人工智能、物联网和加密货币等新技术带来的新挑战。中国支持所有国家在联合国主持下，借鉴现有区域公约的经验，谈判并制定一项向所有国家开放的全球打击网络犯罪公约。

70. 中国认为，该全球公约应有效协调打击网络犯罪的国家法律和实践，及时应对技术发展带来的新问题，并为全球网络犯罪治理提供普遍接受的解决方案。在适用范围方面，除了针对计算机系统的犯罪之外，该公约还应适用于主要通过使用互联网和信息技术实施的犯罪，以及协助和准备实施此类犯罪的活动。在执法和调查方面，公约应规定有针对性的执法和调查措施，并对公私伙伴关系问题做出安排，明确规定网络服务提供商和运营商在预防网络犯罪、协助执法和调查方面的配合义务。在国际合作方面，公约应规范电子证据的跨境取证做法，在尊重国家主权和保障法人和个人权利的基础上，设计更有效的取证机制，并就符合网络犯罪特点的管辖权制度做出规定。此外，公约还应就能力建设、技术援助和预防犯罪机制做出规定。

71. 在国际合作方面，中国指出，在全球公约出台之前，鼓励各国根据《打击有组织犯罪公约》、区域公约和双边条约，在相互尊重、平等互利的基础上开展打击网络犯罪的务实合作。中国还指出，一些国家通过了国内立法，绕过司法协助和执法合作渠道，单方面从国外获取电子数据，这反过来对主权和保护个人及法人权利等国际法基本原则产生负面影响。中国继续在尊重国家主权、保护法人和个人权利以及便利调查之间寻求平衡，并通过优化司法协助和执法合作程序以及创新合作模式来提高取证效率。

72. 在国内措施方面，中国坚持认为各国应在国内采取相应措施，有效打击网络犯罪，特别是：

(a) 将为恐怖主义目的使用互联网以及协助和准备实施网络犯罪的活动定为刑事罪；

(b) 规定互联网服务提供商和运营商有义务配合预防网络犯罪，协助执法和调查，同时明确上述义务的界限，保障相关企业和个人的合法权利；

(c) 提升执法和司法机关调查网络犯罪，特别是更好地应对新技术所带来挑战的必要能力；

(d) 承认电子数据的证据效力，规定电子证据的定义和范围；

(e) 澄清电子证据的取证和采信规则，并在国内立法中规定扣押和封存原始存储介质、现场收集、远程检查和冻结等手段；

(f) 在适用传统证据规则时考虑电子证据的特殊性；

(g) 加强电子证据取证人员的能力建设，培养具有法律知识和技术能力的专业团队，并制定电子证据的取证技术标准。

哥伦比亚

73. 哥伦比亚同意有必要向发展中国家提供技术援助以完善他们的国内立法，并加强其国家主管机关预防、侦查、调查和起诉此类犯罪活动的能力，从而加强各国在打击为犯罪目的使用信息和通信技术方面的协调与合作。然而，哥伦比亚认为，必须区分与网络犯罪有关的问题与对信息和通信技术的可能广泛监管会超越对非法行为的刑事监管范围问题。因此，非常重要的是，要明确对为犯罪目的使用信息技术和通信进行监管的概念，以及在国际安全背景下的信息和电信安全。哥伦比亚赞成自由、开放和安全的互联网，并认为各国必须拥有工具，使它们能够合作打击网络犯罪，加强国家能力，巩固国家间的相互信任措施。

74. 哥伦比亚指出，网络犯罪领域存在着巨大挑战，例如：数字身份；与互联网服务提供商的合作；与数字证据、获取数字证据的技术、存储、保管链、认证和有效性有关的事项；以及数据保护、隐私和尊重个人权利和自由。此外，网络犯罪还与其他跨境犯罪密切相关。因此，哥伦比亚认为，必须更深入地了解犯罪、犯罪作案手法等。基于这一原因，各国必须分享经验和良好做法，以加强应对此类犯罪的国内和国际对策。数字鸿沟使一些国家更加脆弱，合作并非无效。必须调整国际司法合作，以便更快地开展工作（例如，司法协助、司法协助请求和司法协助条约）。为此，哥伦比亚提议设计有助于各国理解并在调查和司法程序框架内有效的规程和模板。

75. 不过，哥伦比亚还认为，预防犯罪和刑事司法委员会应通过全面研究网络犯罪问题专家组，从技术和政治角度继续讨论与网络犯罪有关的问题。应将该专家组作为主要论坛，不应产生限制各国参与的新的替代专家组。专家组已就一项工作计划达成一致，预计将在 2021 年提出一份报告，其中将载有关于加强现有应对措施和提出新的法律和（或）其他应对措施的备选方案。

76. 最后，哥伦比亚认为没有必要从头开始谈判一项新的网络犯罪协定。对哥伦比亚来说，至关重要的是在《打击有组织犯罪公约》和《欧洲委员会网络犯罪公约》等现有条约的基础上，优先开展能力建设和合作。

哥斯达黎加

77. 哥斯达黎加谈到其承认、尊重和保护人权的悠久历史。因此，该国签署和批准的国际文书不妨碍其国家主权。

78. 哥斯达黎加认为，在网络犯罪案件中，检察官和调查人员在为受害者提供援助时必须兼顾个人隐私权和公共安全；在收集证据时必须保证尊重这些权利，为此，应向法官提交申请，以发布搜查、解除银行保密或解除税务保密等命令。所有这些都是在调查中取得成功和确保法庭采信证据所必需的。

79. 哥斯达黎加是《欧洲委员会网络犯罪公约》的缔约国，可获得对法律从业人员的广泛培训，并可获得“每周 7 天，每天 24 小时”网络服务以及与其他区域的其他官员进行交流的机会，以便获取和交流与实时调查和获取数字证据有关的信

息。此外，由于哥斯达黎加是《欧洲委员会网络犯罪公约》的缔约国，它参与了欧洲委员会和欧洲联盟题为“全球打击网络犯罪扩大行动”的项目，在该项目中，哥斯达黎加参与了以下活动：

(a) 2018 年 5 月 21 日至 24 日在圣何塞举办的“全球打击网络犯罪扩大行动”项目初步评估团；

(b) 网络犯罪和电子证据立法问题协商团和网络犯罪问题国家政策和战略协商团。2018 年 10 月 8 日至 11 日在圣何塞举行的网络犯罪和数字证据问题立法框架的制定和修订以及关于网络犯罪问题国家政策的制定和修订；

(c) 2019 年 2 月 11 日至 15 日在圣何塞为法官、检察官和律师举办了关于网络犯罪和电子证据的司法培训员培训；

(d) 为法官、检察官和其他司法官员举办网络犯罪和电子证据司法培训高级课程（2019 年 5 月 13 日至 16 日），以及网络犯罪和电子证据程序立法问题咨询团（2019 年 5 月 16 日和 17 日）。

80. 此外，“全球打击网络犯罪扩大行动”项目还支持哥斯达黎加在国外参与了以下活动：

(a) 2017 年 12 月 12 日至 14 日在菲律宾宿务举行的网络犯罪和电子证据司法培训战略国际讲习班；

(b) 2018 年 3 月 7 日和 8 日在荷兰海牙举行的欧洲委员会和欧洲司法组织关于网络犯罪领域司法合作的国际联席会议；

(c) 2018 年 4 月 3 日至 5 日在维也纳举行的全面研究网络犯罪问题专家组第四次会议；

(d) 2018 年 5 月 14 日至 18 日在维也纳举行的预防犯罪和刑事司法委员会第二十七届会议和“全球打击网络犯罪扩大行动”指导委员会会议；

(e) 2018 年 7 月 9 日至 13 日在法国斯特拉斯堡举行的网络犯罪公约委员会会议、网络犯罪公约委员会第十九次全体会议、第二议定书起草全体会议、合作打击网络犯罪问题八方会议和“每周 7 天，每天 24 小时”网络研讨会；

(f) 2018 年 8 月 27 日至 31 日在新加坡为网络犯罪调查单位和中央主管机关举办的国际联合讲习班；

(g) 2018 年 9 月 4 日至 6 日在巴西里约热内卢举行的单位负责人网络犯罪问题工作组第四次会议；

(h) 2018 年 9 月 4 日至 7 日在法国斯特拉斯堡举行的地下经济和网络犯罪问题会议；

(i) 2018 年 9 月 18 日至 20 日在新加坡举行的第六次国际刑警组织-欧警署网络犯罪问题会议；

(j) 2018 年 11 月 27 日至 30 日在法国斯特拉斯堡举行的网络犯罪公约委员会第二十次全体会议、议定书起草第三次全体会议、全球打击网络犯罪扩大行动委员会会议；

(k) 2019 年 2 月 25 日至 27 日在布加勒斯特举行的网络空间刑事司法会议；

(l) 2019 年 2 月 25 日至 3 月 1 日在波哥大举行的国际刑警组织教员培养课程；

(m) 2019 年 3 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第五次会议。

81. 目前，《欧洲委员会网络犯罪公约》已经得到（来自欧洲大陆和其他区域的）63 个国家批准，这就是为什么对哥斯达黎加来说，它是一项有执行记录的国际文书。

捷克

82. 捷克报告称，它已于 2013 年批准了《欧洲委员会网络犯罪公约》。2014 年，它批准了《公约附加议定书》，重点是将通过计算机系统实施的种族主义和仇外性质的行为定为刑事罪，扩大了《公约》及其实质性、程序性和国际合作条款的范围。《公约》及其《附加议定书》向所有国家开放，而不仅仅是对欧洲委员会成员国开放。

83. 捷克坚信，在应对世界各地网络犯罪现象带来的所有挑战方面，《欧洲委员会网络犯罪公约》是最有效和最新的文书。因此，捷克欢迎近期有越来越多的非欧洲委员会成员加入或考虑加入《公约》，从而奠定了其跨区域性及其加入程序的包容性和透明度的基础。因此，与其制定一项新的文书，不如把重点放在有效执行以《欧洲委员会网络犯罪公约》为代表的现有法律文书上，同时考虑到它对协调国家立法标准的积极贡献，因为通过和批准联合国公约过程漫长，制订新文书会产生相反的效果。

84. 捷克支持并赞扬毒品和犯罪问题办公室保证的专门知识及其《跨境请求电子证据实用指南》等具体成果。仍应重点关注由设在维也纳的全面研究网络犯罪问题专家组在审议时提出的这一问题所涉专家方面，而该专家组在联合国一级具有独特的价值。

85. 捷克指出，加强程序规则以打击网络犯罪至关重要；人权和包括个人数据保护在内的法治保障也同样重要。

86. 捷克意识到与网络犯罪有关的威胁越来越多，而且网络犯罪越来越具有跨国性质，因此，捷克报告称，它重点关注提高对网络威胁的认识和培训，包括开展能力建设和招聘具备必要专门知识的新的执法人员。在这方面，在区域层面开展工作并专门处理网络犯罪问题的国家检察官网络以及设立专门的网络犯罪警察单位在惩治网络犯罪方面得到了非常积极的评价。除此之外，捷克还报告称，电子证据受到重视，刑事诉讼中电子证据的数量大幅增加。捷克通过了一项新的法规于 2019 年 2 月 1 日生效，该法规对国内和跨国案件中加速保存计算机存储数据的规则做出了明确规定。

87. 司法数字化是捷克司法部的工作重点之一。政府通过了《打击网络犯罪国家概念战略》（定期更新由内政部发布的《打击有组织犯罪国家概念战略》就是对这一问题的反映），并确定了在此领域即将采取的明确目标和措施。

88. 在司法协助方面，捷克报告称，协助请求和相关行动越来越多地以电子方式处理。相关程序已经简化，以实现提高效率和快速合作的目标，包括在国家间交流信息方面（例如，通过在《欧洲委员会网络犯罪公约》“每周 7 天，每天 24 小时”网络内设立非正式沟通渠道或联络点）。

89. 捷克提到了与其他国家同样的潜在挑战：用户匿名性的增加（将加密作为一项标准）、恶意软件和付费非法服务（将犯罪作为一项服务内容）的提供、以虚拟货币隐藏犯罪利润的可能性及其匿名性。最后但同样重要的是，捷克强调，上述国际司法协助制度不足以解决网络问题，特别是因为其速度缓慢。（欧洲委员会成员国）处理涉及网络问题的司法协助请求的平均时间为 21 个月。因此，宜开始讨论网络空间管辖权的定义和直接获取境外（或未知地方）服务器上的电子证据问题。在与外国服务提供商开展直接合作问题上也有开展辩论的余地。捷克作为欧洲联盟和欧洲委员会的成员国，一直参与这方面的诸多讨论，特别是关于欧洲出示令和保存令以及《欧洲委员会网络犯罪公约》第二附加议定书的讨论。

朝鲜民主主义人民共和国

90. 朝鲜民主主义人民共和国政府认为，信息和通信技术不应该用于犯罪活动，不得威胁或破坏各国政治、经济和社会稳定。它认为，为了预防将信息和通信技术用于犯罪目的，各国之间开展合作与协调至关重要。

91. 鉴于世界范围内旨在预防和打击为犯罪目的使用信息和通信技术的法律文书不够充分，朝鲜民主主义人民共和国认为有必要根据各国利益，起草一份关于合作预防为犯罪目的使用信息和通信技术的联合国决议。

92. 朝鲜民主主义人民共和国政府强调，应在所有相关国家都出席的相关不限成员名额专家组会议上讨论犯罪活动中使用信息和通信技术问题。

萨尔瓦多

93. 萨尔瓦多政府认为，缺少立法是打击为犯罪目的使用信息和通信技术问题面临的主要挑战，在这方面，萨尔瓦多指出了以下需要考虑的因素：

(a) 缺少对所有普通民众移动电话分配和互联网使用进行管制的措施或立法，特别是很容易获得预付费电话并可用于任何目的；

(b) 没有立法允许在线和实时获取关于国内不同运营商公共和私人 IP 地址的使用日志和分配的信息；

(c) 缺少对使用无人机、信号屏蔽器、拦截器、病毒感染设备和其他允许实施网络犯罪行为的设备等技术设备的监管；

(d) 缺少迫使公共、私人或非营利机构网络管理员有义务建立、维护和保护其内部客户连接日志的法规。没有这种法规可能被用于实施传统犯罪和网络犯罪。

爱沙尼亚

94. 爱沙尼亚指出，网络犯罪和为犯罪目的使用信息和通信技术的现象日益增多，给世界各地的执法实体带来了挑战。

95. 爱沙尼亚指出，由于大多数网络犯罪具有跨境性质，因此，国际合作至关重要。通常情况下，与犯罪有关的电子证据存储在刑事调查所在国之外。然而，国际合作并非总是有效，各国往往没有必要的实体法和程序法，或者执法实体和司法机构也没有足够的能力。

96. 爱沙尼亚指出，目前，《欧洲委员会网络犯罪公约》是在打击具有全球影响力的网络犯罪方面唯一具有法律约束力的文书。该《公约》关于实体法和程序法以及国际合作的条款一直被世界上许多尚未加入《公约》的国家作为范例。由于这些标准已被许多国家所接受，并且已经存在一定程度的统一，因此，有必要也有可能进一步合作。因此，《公约》作为一项已经存在且具有法律约束力的国际文书，为那些尚未没有制定必要法律框架的国家提供了也应遵循的标准。

97. 爱沙尼亚认为，《欧洲委员会网络犯罪公约》是收集和交流电子证据的得力工具。由于《公约》的程序法条款和措施也可用于涉及计算机数据或电子证据的其他刑事犯罪，因此，《公约》不仅仅是一项关于网络犯罪的文书。此外，由于《公约》的条款可以用来处理与任何刑事犯罪有关的电子证据，因此，对各国来说，它变得更加有用，更有价值。电子证据和获取电子证据已成为执法当局在进行刑事调查时面临的最大挑战之一。由于电子证据通常储存在其他国家，因此，需要利用国际合作措施和渠道。尽管基于《欧洲委员会网络犯罪公约》和《打击有组织犯罪公约》等其他文书的国际合作具有成效，但仍有必要加以改进并使其更加有效。

98. 爱沙尼亚指出，几年来，一直在讨论《欧洲委员会网络犯罪公约》的第二附加议定书。最近已开始就此进行谈判。《附加议定书》将对《公约》缔约国开放，将为执法机关和司法机构提供额外的工具，以加强国际合作，并提供更明确的规则和保障。因此，爱沙尼亚表示，《公约》及其全球重要性和覆盖面将来会扩大，更多国家可以利用这一点。

99. 爱沙尼亚强调了在毒品和犯罪问题办公室层面就打击网络犯罪和进行能力建设问题展开的讨论。自 2011 年以来，全面研究网络犯罪问题专家组一直在讨论应对网络犯罪的可能对策，包括如何确保更好地执行现有国际文书。该专家组已成为各国讨论网络犯罪相关问题和挑战以及交流最佳做法的一个有益和有效的平台。虽然迄今为止在许多问题上没有达成共识，但能力建设得到了大力支持。专家组目前正在根据商定的工作计划继续开展工作，预计将在 2021 年前提出结论和建议。

100. 爱沙尼亚认为，在联合国一级开始平行讨论和编写平行报告的时机尚不成熟。因为资源有限，所以应该以最有效的方式加以使用；因此，现有专家组应继续并完成其任务和工作计划范围内的工作。然而，正如目前的讨论已经表明的那样，与网络犯罪、在线调查和电子证据有关的新的分专题和主题已经出现，可能会使专家组在 2021 年后继续存在。

法国

101. 法国报告说，它已与 60 多个其他国家和数百个国际组织、民间社会和私营部门代表一道，在《网络空间信任与安全巴黎呼吁》中申明，支持一个开放、安全、稳定、可访问、和平且可适用包括人权在内的国际法的网络空间。打击为犯罪目的使用数字手段是实现这一目标的条件之一。

102. 在这一领域，法国报告说，就现有法律和预防措施而言，法国在打击网络犯罪领域有一个强大的国家体系，并为调查人员和法官有效打击这一现象提供了专用资源。从一定程度上讲，该机制源于《欧洲委员会网络犯罪公约》条款的转换，通过加强国内立法体系，也通过为国际合作铺平道路，为解决网络犯罪现象提供了一个适当而灵活的国际法律框架。这些条款是对《打击有组织犯罪公约》中关于所有形式跨国有组织犯罪的条款的补充。

103. 尽管通过了这个国际法律框架，而且有强有力的国内体系，但法国报告说，它在打击网络犯罪方面仍然面临某些困难。全面研究网络犯罪问题专家组会议对这些困难进行了探讨，具体如下：

(a) 很多国家缺少打击网络犯罪的国内法律和专门手段，特别是一些国家缺少适应网络犯罪问题的国内立法（实体法和程序法），调查人员和负责刑事案件的人员也缺少有效打击网络犯罪的培训和适应的资源。为了帮助加强这一领域的机制，法国不仅积极参与了若干双边能力建设方案，而且也参与了欧洲联盟和欧洲委员会一级的能力建设方案；

(b) 私营部门和一些外国管辖区域缺少在数据传输方面的合作，甚至在保护调查和法院诉讼程序中的冻结令方面。现阶段，服务提供商的合作仍然是局部合作（平均为 60%，但各合作伙伴合作程度各不相同）。后者必须满足各国主管机关在调查和刑事诉讼中发出的请求，而不以 IP 地址所在国国籍为响应条件。为了增加获取电子证据的机会，法国正在积极参与欧洲联盟内部关于欧洲联盟委员会 2018 年 4 月 27 日提出的两项立法提案的谈判，一项是对获取电子证据的条款和条件做出规定的法规草案，另一项是要求服务提供商指定一名授权法律代表负责接收和回应各种禁令的指令草案。法国还参加了负责起草《欧洲委员会网络犯罪公约》的一项附加议定书的工作组，该议定书也涉及这一问题；

(c) 适应新技术的持续挑战（特别是只受到部分监管的加密货币）导致资金流、暗网、加密和物联网面临重大的匿名化风险。关于更好地理解这些现象的良好做法的讨论和交流是在全面研究网络犯罪问题专家组的框架内进行的，更广泛地说，也是在毒品和犯罪问题办公室框架内进行的，法国希望强调这些讨论和交流的业务价值。

格鲁吉亚

104. 格鲁吉亚报告称，为了有效打击网络犯罪，该国从 2008 年起对其实质性和程序性立法及政策文书进行了本质性修订。所有重大修订都与格鲁吉亚于 2012 年加入的《欧洲委员会网络犯罪公约》保持一致。

105. 格鲁吉亚认为难以获取跨境数据是打击网络犯罪面临的一大挑战。面对不断发展的云计算，传统的司法协助机制已基本上过时。格鲁吉亚认为，放松管制或以其他方式放宽对跨境数据的获取将是一项不可避免的改革，以提高网络犯罪调查和起诉的成效。然而，这些改革必须由各国通过多边文书进行，跨管辖区域程序权力必须伴有强有力的保障措施。格鲁吉亚认为起草《欧洲委员会网络犯罪公约》第二附加议定书就是这方面的一个重要机会。

106. 格鲁吉亚报告说，近年来，它参加了欧洲委员会（东部伙伴关系项目）、欧洲联盟和美国政府实施和（或）支持的各种能力建设项目。作为这些项目的一部分，数百名执法和司法专业人员接受了培训，政府通过的各种政策文件吸收了网络犯罪、电子证据和网络安全领域的多国专家意见。

107. 就实体法而言，格鲁吉亚报告说，依照《欧洲委员会网络犯罪公约》第 2 至 6 条，根据 1999 年《刑法典》第 284 至 286 条，将非法获取和拦截、数据和系统干扰以及滥用设备定为刑事罪。所有与网络相关的犯罪都被作为常规犯罪起诉，没有遇到重大挑战。例如，网络欺诈是近期一直在不断增长的一种犯罪，格鲁吉亚法院认为适用传统欺诈立法办理此类案件没有困难。

108. 关于程序法，格鲁吉亚报告说，自 2010 年以来，格鲁吉亚在其立法中实施了《欧洲委员会网络犯罪公约》规定的所有程序权力，包括：出示令、实时收集通信量数据、拦截内容，而另外几项权力在其立法中已经存在。与此同时，格鲁吉亚采取了强有力的程序性保障措施，包括对所有侵犯隐私的程序性权力的司法授权、相称性要求、使用某些程序性权力的限制（仅在严重犯罪案件中使用）以及要求使用现有程序性权力中侵入性最小的选项。

109. 关于外国互联网服务提供商的合作，据称，格鲁吉亚执法机构一直从各种全球互联网公司（脸书、苹果、微软等）寻求与在格鲁吉亚境内提供的服务有关的订户信息，都很成功。例如，在披露率方面，格鲁吉亚是世界上披露率最高的十个国家之一，在 2017 至 2018 年期间，脸书对格鲁吉亚所提法律程序请求的披露率为 94%。2018 年，格鲁吉亚出台了一项国际出示令，授权格鲁吉亚法官在累计满足以下条件的情况下，对格鲁吉亚领土管辖范围以外的个人或实体发布出示令：接受命令的主体同意自愿披露电子数据；外国实体所在国通过其法律或行政政策允许此类披露。这种命令必须由检察官从法院获得，并且必须通过总检察长授权的官员传达。不遵守此类命令不会导致任何法律责任。根据《欧洲委员会网络犯罪公约》第 18 条，格鲁吉亚已针对脸书和其他国际服务提供商在格鲁吉亚境内提供的服务使用过国际出示令。

德国

110. 德国提到技术发展致使社会在不断变化。技术发展创造了新的机会，每个人都能从中受益，整个社会也能从中受益。另一方面，技术进步也带来新的挑战。在全球范围内快速沟通和行动的技术可能性也被用于非法目的。因此，德国认为，勇于正视挑战和打击犯罪行为非常重要。这需要一个得到充分发展的国家法律框架，但也需要顺利运作的跨境合作。

111. 对德国来说，国际一级的任何解决方案都应根据信息和通信技术带来的具体挑战进行量身定做，并应解决在信息系统保密性、完整性和访问方面面临的问题

（所谓的核心网络犯罪）。试图制定适用于使用计算机或通过互联网实施的所有罪行的条款既不可行，也不可取。关于核心网络犯罪的条款需要足够灵活，以跟上技术发展。另一方面，需要有跨境数据交换机制来调查、起诉和惩罚网络犯罪。

112. 德国强调，《欧洲委员会网络犯罪公约》非常适合有效应对打击网络犯罪的现有挑战。在这方面，事实证明，《公约》是打击网络犯罪的适当工具，它也向第三国开放。德国指出，《公约》被许多国家广泛接受，成为打击网络犯罪的主要国际文书，并被德国当局用作国内立法的指南。《公约》对各种犯罪的定义具有技术中性，并且仍然是最新定义。德国认为，总体而言，正是这种对侵犯信息系统的保密性、完整性和可访问性的犯罪的普遍关注促成了全球高度接受《公约》。因此，德国认为有必要保持对提及一套核心网络犯罪概念的理解。相比之下，在将“网络犯罪”的范围扩大到仅以计算机设备为手段实施一般犯罪的各种行为时，应谨慎行事。几乎任何犯罪都可以使用计算机设备实施，但这并不意味着它们就是“网络犯罪”。

113. 德国指出，对最新情况的适应应当以《欧洲委员会网络犯罪公约》为基础，目前在获取电子证据领域展开的关于第二附加议定书的谈判就是如此。第二附加议定书将旨在改善各方在网络犯罪追踪领域和获取电子证据领域的合作。因此，德国不支持关于制定一项新的网络犯罪问题国际文书的呼吁。

114. 此外，全面研究网络犯罪问题专家组正在全面研究打击网络犯罪的各种挑战。自 2011 年以来，专家组已就网络犯罪的挑战进行了实质性讨论。德国认为，专家组现在是而且应该继续是联合国一级关于网络犯罪专题的主要进程。应尽可能避免与大会决议相关的平行进程以及可能发生的工作重复。

115. 德国强调，应特别关注网络犯罪立法的实施，并切实取得有效进展，包括通过提供技术援助。不缺适当的国际标准，会员国也为执行现有标准制定了关于网络犯罪的实质性刑事立法。全面研究网络犯罪问题专家组现在应该应对的挑战是如何为执法实体提供健全的法律框架和必要的资源，以获取电子证据，同时通过基于法治和保护基本权利和自由的条件和保障来界定执法权力。

加纳

116. 加纳报告说，它目前有两项关于网络和电子证据的主要立法：2008 年《电子通信法》（第 775 号法）和 2008 年《电子交易法》（第 772 号法）。

117. 在加纳，虽然总检察长是所有刑事犯罪的主要检察官，但警方等其他机构也可依据总检察长的授权起诉犯罪。不过，警方移交的案件由总检察长办公厅负责起诉。警方向总检察长办公厅移交的网络犯罪或计算机赋能犯罪案件较少，因此，注意到在起诉此类案件方面遇到一些问题和挫折。

118. 加纳报告说，警方作为主要调查机构，缺乏必要的工具，因为打击网络犯罪法证实验室工具已全部过期。因此，调查工作被外包给私营法证实验室，由此产生的费用往往转嫁给投诉人。不支付检查费用通常会对审判产生负面影响。即使最终支付，警方也要花很长时间才能筹集到所涉金额。延迟付款往往会影响报告的及时发布，从而延误审判。网络犯罪实验室是唯一服务于全国的实验室。然而，它缺乏必要的称职工作人员。缺乏称职的工作人员也严重影响了其产出。

119. 加纳报告说，目前加纳高等法院在访问电子设备内容方面有两项不同的判决。根据其中一项判决，执法机构不需要法院令状就可以访问可疑设备的内容；而在另一项判决中，强调在获取内容之前须获得令状。为使两项对立的判决和谐、明确，已将案件移交加纳最高法院裁决。

120. 从性质上讲，网络犯罪可能跨越几个国际边界。因此，成功起诉一个案件所需的关键信息可能在另一个司法管辖区内。加纳强调，获取此类信息往往是不可能的，或者极其缓慢。在当事国之间没有司法协助条约的情况下，可能无法获得信息。如果存在司法协助条约，转发信息的过程往往是缓慢而官僚主义的，导致调查和随后的案件审判工作延迟。

匈牙利

121. 匈牙利报告称，国内和国际滥用信息和通信技术行为的受害人数均有增加。一般而言，与基于全球移动通信系统的技术相比，犯罪分子更喜欢利用基于互联网的应用程序（例如 Viber、Snapchat、Messenger、WhatsApp 和 iMessage），而且不需要特殊专业知识。匈牙利认为这对警察和其他执法机构构成了挑战。

122. 匈牙利还指出，现代信息和通信技术被用作实施网上诈骗、网上传播儿童色情制品和网上贩运合成毒品等犯罪的一种手段。社交媒体也以图片或视频形式被轻易地用于影响儿童和实施性剥削。此外，暗网也被用于非法和匿名购买武器、毒品和伪造的证件。比特币被用于支付非法和危险产品的货款。此外，在考虑生产武器或零部件时，3D 打印技术也有可能成为一种新出现的威胁。

123. 匈牙利进一步强调，大多数与信息和通信技术有关的犯罪具有国际特征，经常有两个以上国家牵涉其中。如果那些国家之间交换信息需要有调查委托书，这给主管部门造成困难。例如，主管部门在调查相关犯罪时可能遇到困难，因为使用虚拟专用网络服务使主管部门更难识别用户的有效个人数据。因此，在预防领域需要做出更多的努力。

124. 匈牙利指出，国家互联网服务提供商必须与包括警方在内的公共部门密切合作。由于互联网服务提供商的义务没有国际标准，国家主管机关应该协调此类提供商在与通信有关的信息记录、存储和共享（数据留存）方面的义务，包括数据类型、数据保存的最短和最长期限以及通信的详细内容。警方向互联网服务提供商发出请求的最低要求也应该标准化，因为提供商期望用于处理一项请求的信息通常比主管部门拥有的信息要多。

125. 匈牙利建议将各成员国在《欧洲委员会网络犯罪公约》框架内指定的“每周 7 天，每天 24 小时”联络点视为一种良好做法。它还提议利用国际刑警组织的通信渠道来交换信息。

126. 匈牙利报告称，对个人技术手段进行加密有助于预防网络犯罪，但犯罪分子为了隐瞒自己的身份和下落会滥用加密。解锁加密是警察要应对的另一个挑战。需要提高公共和私营部门对网络安全的认识。此外，要想提高国家能力，有必要使各机构的信息技术基础设施升级，并对公共和私营部门工作人员进行培训。

127. 匈牙利强调，不同国家之间开展良好合作对于成功解决案件必不可少。在欧洲，欧警署在合作领域发挥决定性作用。《欧洲委员会网络犯罪公约》可作为从其他国家的服务提供商那里获取电子证据的一种良好做法。

128. 由于网络犯罪是一种不断变化的挑战，影响到每一个国家，匈牙利认为以下要求对有效打击网络犯罪是必要的：

(a) 最大限度地增加拥有足够的、兼容的、支持国际合作的网络犯罪相关国内立法的国家数量；

(b) 建立共享数据的合作机制、信任和技能，以调查、起诉和减少网络犯罪；

(c) 保证犯罪分子没有安全避难所，并提高执法和司法机关的能力，特别是获取电子证据的能力。

129. 在技术援助方面，匈牙利回顾了网络犯罪问题全面研究报告草案，并指出各方达成了广泛的共识，即努力建设打击网络犯罪的能力至关重要。毒品和犯罪问题办公室《网络犯罪问题全球方案》已经开始实施，所有会员国的参与非常重要。匈牙利还支持其他一些能力建设方案，例如，欧洲委员会和欧洲联盟实施的方案。对匈牙利而言，需要确保所有能力建设项目都具有有效的针对性，都要进行协调，以避免重复，并且进行适当设计和排序，以满足国际合作的需要和确保取得可持续成果，同时进行有效评价以评估其影响。

130. 关于加强应对网络犯罪的现有国家和国际对策及提出新对策的备选方案，匈牙利认为，《欧洲委员会网络犯罪公约》是国家立法的有效模式，也是国际合作的宝贵框架。《公约》向欧洲委员会成员国以外的国家开放，以供其加入，并为此提供了一个灵活机制（制定国家措施和促进国际合作）。匈牙利不支持有关就网络犯罪问题制定一项新的国际文书的呼吁。

131. 匈牙利认为，全面研究网络犯罪问题专家组现在是而且应该继续是联合国一级打击网络犯罪的主要进程，至少在 2021 年前应如此。该专家组已经取得成果，包括根据现行国际标准进行立法改革，以及在能力建设方面。在过去六年里，各国尤其在利用现行国际标准进行立法改革方面取得了良好进展。许多组织制定了能力建设方案。这些努力需要继续下去并进一步扩大。

132. 匈牙利建议会员国支持毒品和犯罪问题办公室采取以下行动应对网络犯罪威胁：

(a) 通过一般和专门培训，提高警察和执法的技能；

(b) 为发展中国家提供技术援助；

(c) 分析国际合作差距，确定优先领域；

(d) 支持开展宣传运动，以加强预防犯罪，并与执法实体开展民间社会和商务合作；

(e) 加强“每周 7 天，每天 24 小时”网络等现有业务机制；

(f) 收集网络犯罪威胁方面的数据；

(g) 作为打击网络犯罪最佳做法和案例研究信息库。

印度

133. 印度提到网络犯罪在稳步增长，给执法部门提出了新问题和新挑战。网络犯罪在性质、范围、手段、证据和活动方面与传统犯罪大不相同；因此，实时或接近实时交换信息对于收集证据以将网络犯罪分子绳之以法至关重要。与网络犯罪有关的罪行在技术和法律方面都很复杂。网络空间和网络犯罪没有实体边界，因此，国际合作对于开展调查、收集数据和证据以及进行处罚等极为关键。

134. 印度报告称，根据其国家犯罪记录局的数据，2014 年记录了 9,622 起与网络犯罪有关的犯罪行为，2015 年记录了 11,592 起，2016 年记录了 12,317 起。在 2016 年报告的网络犯罪案件中，有 48.6%是为获得非法收益（12,317 起案件中有 5,987 起），其次是报复（占 8.6%，1,056 起案件）和侮辱妇女的端庄（占 5.6%，686 起案件）。

135. 印度还提到打击网络犯罪国家法律和体制框架，指出 2008 年修订的 2000 年《信息技术法》和《印度刑法典》为处理电子商务、网络安全、网络犯罪和网络恐怖主义问题提供了法律框架。国家法律涉及范围广泛，涵盖了大多数与网络犯罪有关的问题。

136. 印度还指出，以“核心”网络犯罪以及以信息和通信技术辅助网络犯罪形式出现的各类滥用信息和通信技术行为构成了不同挑战，需要加以应对。滥用信息和通信技术行为包括入侵和破坏网站、病毒或恶意代码、拒绝服务攻击和分布式拒绝服务攻击、黑客、网络钓鱼、网络恐怖主义、传播儿童色情制品、“性索贿”、盗用身份、网络盯梢和骚扰、假新闻和宣传、非法赌博、销售假药和毒品、网络间谍活动等。

137. 印度指出，网络犯罪是使用恶意软件、僵尸网络、洋葱路由技术甚至是普通移动电话等现代信息和通信技术工具实施的。

138. 在打击为犯罪目的使用信息和通信技术行为方面，印度提到以下挑战：

(a) 使用多种形式恶意软件和僵尸网络，使犯罪分子能够避开杀毒软件和互联网过滤器等技术控制，并且避免被执法实体侦破；

(b) 使用具有模糊性、匿名性、计算能力和拒绝追溯犯罪来源或犯罪实施者的技术；

(c) 虚拟专用网络服务能够通过互联网提供匿名通信的事实；

(d) 有多种工具使犯罪分子能够在网上保持匿名或无法追踪。在这些工具中，僵尸网络构成的挑战最大，原因有很多；

(e) 处理网络犯罪需要专门的法律知识、成套调查技能、法证工具和分析敏锐性；

(f) 在法律挑战方面，网络犯罪具有跨国性的事实致使管辖权错综复杂，从而使调查和起诉变得困难。各国立法不统一，给调查和起诉网络恐怖主义犯罪带来困难。

139. 印度重点介绍了在国际一级妨碍打击非法滥用信息和通信技术的合作方面的挑战，并提到以下问题：

(a) 在网络犯罪调查中时间至关重要，因此，需要为国家间多边合作规定提供数字证据的时限；

(b) 司法协助条约主要侧重于犯罪后的情况，然而，与传统犯罪不同，迅速交换信息对于预防网络犯罪至关重要。预防网络犯罪领域也需要开展国际合作；

(c) 司法协助条约中没有满足对应急要求的需求的条款，满足这种需求是应对网络犯罪的关键。这方面需要讨论；

(d) 考虑到犯罪分子普遍使用控制与指挥、僵尸网络和深网技术，网络犯罪安全方面的国际合作必不可少；

(e) 隐私法阻碍了信息共享。

伊朗伊斯兰共和国

140. 关于在打击为犯罪目的使用信息和通信技术行为方面面临的挑战，伊朗伊斯兰共和国报告称，首要问题是外国互联网和社交网络服务提供商不遵守规定。互联网和社交媒体为改善人们生活作出了巨大贡献。然而，通过互联网和社交媒体随时随地进行无缝通信及其可以转移性致使犯罪分子特别是有组织犯罪集团越来越多地为犯罪目的使用这种技术。互联网和社交网络服务提供商在防止和打击为犯罪目的使用信息和通信技术行为方面，特别是在电子证据收集和保存领域以及执法领域发挥着不可或缺的作用。

141. 对于伊朗伊斯兰共和国来说，公平和具有复原力的对策在很大程度上依赖于对社交媒体上的活动进行监管。在伊朗私营部门拥有的社交媒体上，由国家主管部门根据《计算机犯罪程序法》对各种活动进行妥善监管。执法部门可以侦测网络空间的犯罪活动，收集和保存电子证据，并有效调查和起诉为犯罪目的使用信息和通信技术行为。然而，鉴于网络犯罪具有域外性，主管部门在起诉使用外国公共或私营部门所有并设在其他国家的服务器实施的犯罪行为时面临重大挑战。外国社交网络服务机构大多在刑事事项上不配合。这些实体不满足各国的合作要求，对有效预防和打击犯罪构成挑战，并在国家和国际两级使法治陷入险境。

142. 关于单方面胁迫措施，伊朗伊斯兰共和国报告称，它位于有组织犯罪肆虐的区域，在刑事事项上，特别是在开展国际合作打击为犯罪目的使用信息和通信技术行为方面遇到国际障碍。单方面胁迫措施不利于集体应对此类犯罪，影响各国与伊朗执法部门合作调查和起诉犯罪行为，特别是通过使用信息和通信技术实施的犯罪行为，还影响它们在转让保存电子证据和开展数字法证鉴定所需技术工具方面开展合作。单方面胁迫措施严重违反了《联合国宪章》规定的国际法基本原则，不仅妨碍了在打击为犯罪目的使用信息和通信技术行为方面开展有效合作，还削弱了法治，使犯罪分子更有胆量从事非法活动。清除国际障碍仍然至关重要，不仅可以有效打击为犯罪目的使用信息和通信技术行为，还可以确保各国的集体安全。伊朗伊斯兰共和国致力于打击有组织犯罪，支持毒品和犯罪问题办公室推动的打击网络犯罪国际合作，并强调需要加强这一领域的技术援助。

143. 关于缺乏包容性国际框架问题，伊朗伊斯兰共和国强调需要一个关于网络犯罪问题的国际法律框架。目前，缺乏健全和包容各方的关于网络犯罪问题的国际框架仍是打击为犯罪目的使用信息和通信技术行为面临的一项挑战。网络犯罪的

性质必然要求制定一项国际文书，采取有针对性且具有适应能力的集体对策，并要考虑到需要跟上技术发展和有组织犯罪集团新的作案手法。已经制定网络犯罪文书的国家数量有限，现有网络犯罪文书中缺乏采取这种对策的必要条件，而这又使这些文书无法在国际上适用。

144. 伊朗伊斯兰共和国赞扬并感谢毒品和犯罪问题办公室，特别是全面研究网络犯罪问题专家组所做的各种宝贵工作。该国表示继续支持毒品和犯罪问题办公室在此方面做出的努力，并认为在联合国主持下通过一项关于网络犯罪问题的普遍公约符合各国的最大利益，并将减轻在打击为犯罪目的使用信息和通信技术行为方面面临的挑战。

145. 关于网络犯罪问题法律框架，《伊斯兰刑法典》规定，在伊朗伊斯兰共和国境内通过使用网络空间促使或促成的传统犯罪应受到处罚。不过，伊斯兰协商大会（议会）已制定并批准了针对网络犯罪的立法，以便通过高效且具有适应能力的方式预防和打击为犯罪目的使用信息和通信技术行为，尤其是网络犯罪。这项立法还涵盖电子证据，因为电子证据在起诉网络犯罪方面起到不可或缺的作用。

146. 伊朗伊斯兰共和国从实体刑法角度提到了 2004 年《电子商务法》。该法规定，承认电子合同和设备对商业秘密的保护措施，并将滥用个人数据、侵犯消费者权利和披露电子交易中的保密商业信息以及计算机欺诈和造假行为定为刑事犯罪。该国报告称，2009 年《计算机犯罪法》包含关于刑事定罪和法人赔偿责任的条款。该法规定，除其他外，未经授权获取数据和访问计算机系统、播放淫秽内容、侵害数据完整性和保密性以及与计算机有关的盗窃和欺诈行为均被定为刑事犯罪。犯罪行为可被处以罚款和 15 年以下监禁。第 26 条将有组织、大规模或针对公共服务计算机系统实施网络犯罪行为定为加重处罚情节。目前，该国正在对该法进行审查，以便适应犯罪分子新的作案手法，并为执法部门提供一个具有适应能力的法律框架。

147. 伊朗伊斯兰共和国从程序法角度提到了计算机犯罪程序法，该程序法先前是 2009 年《计算机犯罪法》的一部分，经少量修改后，被纳入《刑事诉讼法》。这项立法涵盖管辖权、专门的调查部门、起诉网络犯罪以及搜查和扣押电子证据、数据和计算机系统的条件和程序等问题。该法确保采用正当程序和保护隐私。第 671 条和第 672 条允许法院只有在有确凿且合理理由的情况下发布搜查和扣押数据的命令，且该命令应在合法所有人在场的情况下执行。根据第 679 条的规定，凡导致财产损害或导致公共服务中断的扣押都是被禁止的。

伊拉克

148. 伊拉克指出，使用互联网是现代文明的一个特征，也是发展、融入人类文明和与其他国家相互交流的一种手段。因此，科学和文化交流的方法发生了革命性变化。互联网已成为获取知识的一个主要渠道，有助于社会和个人超越地理界限、政治和社会决定因素以及知识理论建立联系和形成凝聚力，有助于不同文明的融合以及不同民族、语言和宗教之间的思想交流。这促使人们思考哪些价值观和原则应该主导互联网的内容：这仍然是一个存有争议的重要议题。虽然发展中国家在世界互联网用户中所占比例很小，但内容问题对其及其重要，因为内容对其社会产生影响。虽然平等和自由是互联网的价值观之一，但发展中国家社会的

隐私问题要求其政府要特别考虑到这一点，并尽力保护它们不受多重取向和文化的影响。

149. 伊拉克强调指出，各国人民的趋同性也对犯罪和犯罪行为全球化产生影响，包括产生了影响到发展中国家保守社会的犯罪。因此，有必要制定与每个社区的具体情况相适应的互联网道德规范。因此，根据适当的道德标准制定章程将确定适用于每个国家或地区的互联网内容，但未必适用于所有国家和地区。

150. 伊拉克强调指出，在过去十年里，在线应用程序的使用呈指数级快速传播。因此，有必要对其进行组织和监管。最近的一些应用程序（娱乐或游戏程序）要求用户允许获取其一系列的个人信息。由于网上可用信息的获取水平决定了同一网络上用户的隐私程度，伊拉克鼓励应用程序的设计者和推销者制定标准，要求他们对获取信息或访问设备目的的证据进行说明。另一种办法是让志愿者根据商定标准评价应用程序，以提高对适当应用程序的信心，降低对恶意应用程序的信任。

151. 伊拉克报告称，众所周知，新闻在互联网上迅速向可能无法或不在乎核实新闻来源的广大受众传播。应该鼓励企业准确、客观地处理新闻，不要发布加剧不同社区间仇恨的假新闻或假视频。特别是在当前，可能还需要减少仇恨视频、音频和文字媒体的来源。这也有助于加强新闻和社交媒体赞助方与分析新闻和探索新闻可信度的自愿新闻评估小组之间的合作。

152. 关于儿童的网上风险，伊拉克指出，信息社会提供了只用点击鼠标便可即时进入的数字世界。通过连接了互联网的计算机或移动设备，可以获得的服务和信息达到前所未有的水平。设备成本和接入互联网等障碍正在迅速减少。这些发展成果为儿童和青少年提供了无与伦比的机会，他们可以成为一个没有边界或国界的网络世界的“数字公民”。与儿童和青少年使用互联网有关的网上风险和脆弱性包括以下方面：

(a) 接触非法和有害内容，如色情、赌博、自残网站、暴力场景、恐怖主义和其他少儿不宜的内容，并与其他用户进行联系。在多数情况下，包含此类内容的网站的运营商都没有采取有效措施限制儿童访问；

(b) 通过垃圾邮件和广告有针对性地推销针对特定年龄和兴趣的产品；

(c) 强制和过度使用互联网和网上游戏；

(d) 恐吓、骚扰、威胁和勒索；

(e) 接触激进行为和种族主义以及其他歧视性言论和图像；

(f) 谎报个人年龄；

(g) 通过剽窃和未经许可上传内容（特别是媒体），包括不恰当的照片，滥用个人数据和披露个人信息，造成人身伤害以及本人或他人权利受到侵犯的风险。

153. 伊拉克将重点放在公共安全问题上，强调大型互联网公司为社会和经济发展提供了极好的服务和机会。只有用户能够真正代表自己，网上平台才能适合促进社会经济发展，然而，当用户使用匿名或假名时（这在社交媒体中很常见），他们可能会滥用这些服务并进行犯罪活动，如散布仇恨言论、恐怖主义意识形态、威胁和勒索信息。对发展中国家政府而言，这是一个难以应对的公共安全挑战，特

别是当他们缺乏高水平技术并试图寻求互联网公司的配合时。这些公司可以收集其客户的一般信息和个人信息，作为其账户管理流程的一部分，通过这些信息，它们可以监测客户的地理位置、电话号码和其他有用信息，并且可以预防犯罪和拯救生命。这要求利益攸关方在密切协作的前提下负起应尽的责任，以应对这些挑战，并确保更安全的持续服务，以实现可持续发展目标。

154. 伊拉克还提到在打击为犯罪目的使用信息和通信技术行为方面面临的其他挑战，其中包括：没有一项关于网络犯罪问题的全球公约；数字证据或部分数字证据难以理解，并且很容易被销毁或消失；网络犯罪超出了地理界限，加之犯罪分子与受害者之间有一定的地理距离；主管部门在打击网络犯罪方面缺少足够的培训和能力建设；有时，非政府组织和其他政府实体在调查网络犯罪方面的经验和专门知识没有得到充分利用；没有为打击网络犯罪提供充足的电子基础设施；难以限制或压制实施网络犯罪的方式。

155. 伊拉克的结论是，利益攸关方之间越来越迫切需要加强合作，以确保拥有一个安全的数字未来。

爱尔兰

156. 爱尔兰提到网络犯罪问题全面研究报告草稿至关重要，其中指出各方就必须努力建设打击网络犯罪的能力达成了广泛共识。事实上，最近举行的全面研究网络犯罪问题专家组第五次会议达成了广泛的一致意见，即当前能力不足会给有效应对网络犯罪带来最严峻的挑战。

157. 爱尔兰强调指出，任何犯罪行为都可能涉及网络要素，特别是在电子证据方面，因而在能力建设方面产生了重大挑战。因此，至关重要的是，所有调查人员、检察官和法官都要拥有网络领域的相关专门知识。酌情对专业从业者进行培养也很重要。网络犯罪具有国际性，意味着一个国家缺乏充足的能力不仅会对本国也会对任何国家打击犯罪的能力产生不利影响，这一事实凸显了这一挑战。

158. 爱尔兰指出，为了应对这些挑战，必须继续实施并扩大国家和国际两级的能力建设方案。必须切实瞄准和协调这些能力建设项目，以避免重复并确保其可持续性。它们还应根据各国不同法律制度的具体要求和国际合作需要进行适当的设计。最后，应该对这些项目进行有力的评价，以便为今后项目的发展提供参考。

159. 爱尔兰承认全面研究网络犯罪问题专家组提供的论坛对于交流与网络犯罪带来的挑战有关的知识和经验的价值。爱尔兰特别指出，专家组作为专家论坛而不是政治论坛的性质是其取得成功的关键。因此，爱尔兰认为，专家组应继续作为联合国一级处理网络犯罪问题的主要进程。

160. 爱尔兰还指出，在网络犯罪方面遇到的主要挑战与该领域的国际法律框架无关。因此，爱尔兰确认，它不支持有关制定一项新的关于网络犯罪问题的国际文书的提议。作为打击网络犯罪方面第一项具有约束力的国际文书，《欧洲委员会网络犯罪公约》证明它对不断变化的技术环境和全球范围都具有灵活性。来自联合国所有五个区域组的 63 个缔约国加入了《公约》，而且相当多的不是《公约》缔约国的国家执行了以《公约》为蓝本的打击网络犯罪法律，这证明了《公约》具

有全球性。在这方面，《公约》的实质条款已在很大程度上在爱尔兰法律中得到实施，爱尔兰也致力于尽早批准《公约》。

161. 爱尔兰表示完全支持正在为谈判《欧洲委员会网络犯罪公约》关于加强国际合作的第二附加议定书而开展的工作，该议定书将进一步完善《公约》，并有助于确保该《公约》仍然是关于网络犯罪问题的最重要国际文书。

以色列

162. 以色列强调指出，鉴于信息技术公司的私有平台也可能被用于犯罪活动，各国如今面临的最严峻挑战之一是国家与私营公司之间的互动。在这方面，有必要考虑制定一个适当的均衡框架，一方面便于各公司向其客户提供可靠的服务，同时保护其隐私和言论自由及促进创新，另一方面，找到一个适当的框架，与执法机关合作处理犯罪活动案件。

意大利

163. 意大利报告称，意大利国家警察局通过邮政和通信警察署负责预防和打击网络犯罪。在邮政和通信警察署内设立了“每周 7 天，每天 24 小时”国家信息技术犯罪和保护关键基础设施中心，专门负责预防和打击针对关键基础设施实施的（具有共同、有组织或恐怖主义性质的）信息技术犯罪。该中心通过对互联网进行持续监测，成功地执行了这项任务。“每周 7 天，每天 24 小时”国家信息技术犯罪和保护关键基础设施中心根据公共安全局与管理关键基础设施的实体签订的协议（公私伙伴关系）提供网络保护服务。负责与跨国犯罪事件有关的意大利技术和业务紧急情况联络点也是该中心一部分。

164. 关于网络恐怖主义，意大利报告称，邮政和通信警察署负责预防和打击网上煽动圣战恐怖主义，特别是在语言和文化调解人的支持和中央预防警察总局及警方一般调查和特别行动司的配合下对互联网进行监测。此外，尽管国家警察局、宪兵队和金融调查机构负有对恐怖主义和颠覆方面进行调查活动的权限，但邮政和通信警察署还是在持续更新用于恐怖主义目的的网站清单。此外，金融调查机构也通过特别技术欺诈股侦测、预防和打击利用网络工具实施逃税的犯罪、各种海关犯罪、与欧洲联盟资源有关的欺诈、货币犯罪和伪造犯罪。

165. 在欧洲一级，邮政和通信警察署作为欧警署互联网查询小组的国家联络点，负责接收成员国关于网上圣战恐怖主义宣传内容的报告。

166. 就银行部门而言，根据内政部长的一项指令，邮政和通信警察署已被赋予一项预防和打击利用网上钓鱼、黑客或软件或硬件技术等特定手段以欺诈性地窃取、复制和使用数字身份、供使用网上银行服务的代码和电子交易中的支付卡等网络犯罪。

167. 关于加密货币，意大利指出，加密货币经常被用作购买货物和服务的付款手段。这些交易的特点是发起人和实际收货人都是匿名，这助长了他们对加密货币的非法使用（例如，在网上钓鱼和勒索软件类加密病毒框架中）。

168. 意大利指出，在邮政和通信警察署内设立了打击网上儿童色情制品国家中心。该中心不断更新黑名单，将其发送给互联网服务提供商，以便它们能够阻止意大利的互联网用户访问含有来自其他国家网上儿童性虐待材料的虚拟空间。该中心还依赖参与未成年人教育和保护的所有机构和社会行为者之间开展合作，以便针对这些现象采取共同战略，为支持调查开展研究和开发新技术。邮政和通信警察署采用的创新调查方法是以最先进的秘密手段为基础，旨在阻止匿名化系统，便于识别参与虐待行为的主体和遭受虐待的未成年人。调查还面向存在各种形式的新诱惑和网络欺凌事件以及网上诽谤罪行（主要针对负有机构责任的人）、盯梢、骚扰、威胁和煽动仇恨的社交网络。

日本

169. 日本首先着力应对因网络犯罪性质而产生的一个确切挑战。网络犯罪行为高度匿名化，几乎没有留下什么痕迹。此外，网络犯罪也没有任何地域或时间限制，可能会立即给无数受害者造成损害。因此，犯罪分子能够利用没有有效反制措施的脆弱国家并将这些国家作为基地，对世界各地的受害者进行网络犯罪活动，轻而易举地实施网络犯罪。因此，国际社会面临的一项共同挑战是缩小这一能力差距，以便每个国家都能采取充分和适当的网络犯罪反制措施，不让犯罪分子有操作空间。

170. 日本认为，有两个方面进一步加剧了上述挑战：一是缺乏法律框架，二是缺乏能力建设。一些会员国在实体法和程序法方面缺乏健全的法律框架来处理网络犯罪是一个重大挑战。例如，有些国家没有充足的立法将开发计算机病毒行为定为刑事犯罪，有些国家没有能够保存互联网数据的立法，这些都为打击网络犯罪带来了严峻挑战。为了应对这一挑战，国际社会应协助会员国制定能够应对不断出现的新型网络犯罪并经得起时间考验的新立法。

171. 日本认为，实现这一目标最全面和最具成本效益的方法将是利用现有国际法律框架。这不仅将避免工作重复，而且还将使会员国颁布的立法能够达到已被广泛接受的标准。这将缩小会员国之间的差距，而且有利于开展国际合作（例如，具有类似法律框架的会员国之间将更好地执行双重犯罪原则）。在这方面，《欧洲委员会网络犯罪公约》已被国际社会广泛接受，并提供了一个共同起点。事实证明，依据该《公约》颁布的法律在日本是有效的。例如，根据《公约》，日本在2011年颁布了“创建无授权命令的电磁记录”罪（《刑法典》第168-2条），并已顺利适用于制作勒索软件等不断出现的新型网络犯罪，而这些犯罪在该法颁布时没有预料到。

172. 日本强调，即使制定了健全的法律框架，执法机构和司法机构缺乏利用这些框架的能力也将严重阻碍一切打击网络犯罪的努力。在这方面，执法实体侦测、调查和收集电子证据的能力不可或缺。司法机构还必须了解网络犯罪的作案手法并正确理解电子证据，以期适当地决定这些证据的可采性和可信性。日本认为，国际社会仍然缺少向有需要的会员国提供能力建设和技术援助。

173. 日本报告称，除其他外，它还通过为特定国家提供培训方案的方式，向有需要的国家提供能力建设方案，包括一些由日本国际协力事业团、亚洲和远东预防犯罪和罪犯待遇研究所以及日本-东南亚国家联盟（东盟）网络犯罪对话实施的培

训方案。这些方案面临的一个共同挑战是让受援国能够自主且可持续地继续努力开展本国的能力建设。在这方面，日本政府自 2006 年以来一直与国际刑警组织全球创新中心合作，为各国提供必要援助，以鼓励其努力开展本国的能力建设。

174. 日本强调需要继续开展专家讨论，并强调，为了确定与立法和缺乏提供技术援助以打击网络犯罪的能力有关的挑战，最有效的方法是听取专家的意见和经验。专家们可以介绍网络犯罪问题的最新情况，并考虑到网络犯罪具有不断演变的性质以及不断出现的新型挑战。专家之间的讨论将使人们能够更好地了解这个问题的整体严重性，以期确定国际社会应该把工作重点放在哪里。

175. 日本提到设在维也纳的全面研究网络犯罪问题专家组由来自世界各地的相关专家组成，并为讨论和确定最新趋势、挑战和前进方向提供了理想场所。目前，该专家组正在按照所有会员国以协商一致方式通过的多年期工作计划，每年对相关议题进行讨论。预计该专家组将继续开展工作并在 2021 年进行一次回顾。回顾活动将使国际社会能够确定众多挑战及将要采取的步骤。关于网络犯罪的一切讨论都必须以专家提出的具体循证意见为基础。因此，专家组的成果应被视为今后讨论的基础。日本政府坚信，关于网络犯罪的讨论应该由专家组在维也纳进行。换言之，任何阻碍专家组工作的行动，例如将有关网络犯罪的讨论从维也纳转移到一个少数专家参与的论坛，都将严重削弱国际社会打击网络犯罪的能力。

约旦

176. 约旦列出如下与打击为非法或犯罪目的使用信息和通信技术行为有关的主要挑战：

(a) 存在隐瞒用户身份并使其难以被跟踪和被侦测的免费软件和程序；

(b) 可从大量免费公开网站轻易获得信息以及能够获得有关使用犯罪工具的知识和专门知识；

(c) 暗网为非法活动提供了滋生土壤，其中包括雇凶杀人、贩毒、贩运人口和剥削儿童，使监测和监视这类网站和用户成为一项棘手的任务，因为暗网使用加密技术防止用户身份被侦测；

(d) 在若干管辖区域出现网络犯罪案件程序和信息共享缓慢的情况，特别是考虑到网络犯罪需要快速程序和处理；

(e) 一些社交媒体平台在与执法机关交换信息方面不予回应和配合；

(f) 需要通过国际培训方案和与发达国家交流网络犯罪事项方面的经验开展能力建设。

黎巴嫩

177. 黎巴嫩报告称，2018 年是在行政部门、议会和司法部门一级忙于打击为犯罪目的使用信息技术行为的一年。在国际电信联盟（国际电联）全球网络安全指数（2018 年）中，黎巴嫩排在全球第 124 位，而其互联网使用指数率为 65（国际电联信通技术发展指数（2017 年））。

178. 黎巴嫩政府高度重视网络安全问题。一份部长级声明明确提到，在开展题为“数字政府”的电子政务项目的同时，黎巴嫩政府采取了有关加强用以保护黎巴嫩网络空间和信息基础设施以及个人和机构的个人数据的程序和措施。新政府新设了一个部（国家技术事务部）。

179. 此外，总理还于 2018 年底作出一项决定，组建国家网络安全小组，由各部委和相关部门的代表参与。该小组的任务是制定黎巴嫩国家网络安全战略，并建立处理这个问题的国家管理机构。正在制定的国家战略包括五个关键问题。在准备期结束后，与该计划有关的工作已于 2018 年 11 月 15 日开始，并计划在接下来的两个月内结束。

180. 黎巴嫩还报告称，包括信息技术委员会及信息和通信委员会在内的各议会委员会举行了若干次议会会议，以评估现状并提出建议。

181. 在立法层面，关于电子交易和保护个人数据的《第 81/2018 号法律》于 2018 年 10 月 10 日发布，并于 2019 年 1 月 17 日生效。该法律涉及多种同类问题，包括保护个人数据和与信息系统和数据有关的犯罪。该法律对《刑法典》中与网络犯罪有关的一些条款进行了修订。另外，该法律还涉及与电子证据有关的问题，规定互联网服务提供商应将客户的日志文件储存三年。

182. 黎巴嫩还报告称，利用欧洲委员会和欧洲联盟在“南方网络”项目内提供的支持，对司法部的 20 名法官进行了关于处理电子证据的培训。在提交国家答复时，司法部正在为实施《第 81/2018 号法》起草立法法令。

183. 黎巴嫩提到特别是司法部以及一般而言整个国家遇到以下挑战：

(a) 未发布启动《第 81/2019 号法律》所需的必要法令；

(b) 《第 81/2018 号法律》所载的一些法律条款既不明确，也不充分，特别是在保护个人数据和指定专门管辖权以便在未规定设立机构负责核实电子商务从业人员提供强制性数据的情况下加快处理紧急事项（第 31 条）方面，或在防止促销广告（第 32 条）方面；

(c) 所有负责处理电子犯罪或电子证据的法官都缺乏专门知识，需要培养法官和安全部门的能力，并向他们提供必要的培训和设备，使他们能够具有应对犯罪分子的实力和技术能力；

(d) 法院未实行数字化及以此将其与所有部委以及与其打交道的机构联系起来；

(e) 需要在国家一级通过国家网络安全战略和政策，并设立执行这些政策和战略的国家机构；

(f) 在适用《欧洲联盟一般数据保护条例》程序方面遇到困难，这妨碍司法警察直接访问以前可用的 IP 地址；

(g) 通信部使用的网络地址转换 IP 地址联网系统等服务提供商使用的标准系统存在薄弱之处；

(h) 犯罪分子通过使用特殊软件（VPN、TOR 等）具有隐瞒其真实身份的能力，难以知道其实际所在位置，以及犯罪分子使用加密技术隐瞒交易。所有这些

都妨碍了主管安全部门解密和破获犯罪分子的信息和数据及其在实际和计划犯罪中使用的信息和数据；

(i) 多个设备直接与信息技术和互联网连接，几乎每个设备（冰箱、汽车等）都可以通过物联网与网络连接，没有在这些设备投放市场之前考虑所需的保护系统；

(j) 黎巴嫩缺乏数字转型战略计划及其执行计划；

(k) 各部门和公共机构未采用信息安全标准和公认的政策；

(l) 未能在社会成员中传播提高对网络安全及如何保护个人信息和数据以及对黑客和盗窃风险及如何采用最佳做法和保护这些信息和数据的认识的文化；

(m) 暗网现象使犯罪分子能够非法买卖货物和药物、秘密从事犯罪活动，特别是毒品贸易、销售武器和交换儿童色情制品、恶意程序和个人资料；

(n) 虚拟和数字货币现象使个人和恐怖主义团体能够秘密买卖犯罪物质，且无法追查这种资金的来源或向其转移这些物质的实体；

(o) 国家之间在交换与数字证据和打击网络犯罪有关的信息方面缺乏国际合作框架（公约、条约）；

(p) 不同安全机构与公共和私营部门机构之间需要进行信息交流和做出协调一致的努力；

(q) 与本地和国际服务提供商沟通缓慢；

(r) 未报告所有网络犯罪，特别是那些与性骚扰和性敲诈有关的犯罪等引起某种尴尬的网络犯罪；

(s) 犯罪分子使用“分布式攻击”等复杂技术，从世界各地的多个服务器发起攻击，或使用一些以前被黑客侵入的“智能”设备，作为向其他目标发动攻击的平台。

列支敦士登

184. 列支敦士登指出，网络犯罪数量正在上升，国际社会面临各种各样的挑战，包括在调查和起诉此类犯罪活动方面。对于列支敦士登而言，网络钓鱼、“CEO 诈骗”、劫持邮箱和非法截取数据是目前面临的最大挑战。这些挑战要求在国家层面采取坚定的执法和立法对策以及在国际层面加强合作。然而，列支敦士登对出现以侵犯包括隐私权在内的人权和基本自由的方式对网络空间进行监管以及对网络犯罪进行刑事定罪、调查和起诉的趋势感到担忧。列支敦士登指出，各国在任何时候都必须遵守其根据国际法特别是人权法承担的义务，包括在对网络空间进行监管以及在对网络犯罪进行刑事定罪、调查和起诉时。

185. 列支敦士登报告称，其关于网络犯罪的国家立法是以《欧洲委员会网络犯罪公约》为基础。在 2009 年和 2011 年对其《刑法》进行的最近几次重大修订期间，该《公约》成为引进新的网络相关条款的主要国际参考框架。列支敦士登于 2016 年批准该《公约》，并将其继续作为日后修改立法的框架。

186. 列支敦士登表示，它支持在透明、包容和合作原则的基础上，并完全按照现有人权标准，加强旨在规范网络空间活动的国际法。《欧洲委员会网络犯罪公约》已得到来自所有区域的国家的批准，通过统一法律、制定程序和确定联络点的方式，极大地促进了国家之间的合作。列支敦士登表示，它支持以该《公约》为基础加强国际合作，并反对在网络犯罪领域制定平行或相违背的规范标准，列支敦士登已在对大会第 73/187 号决议投反对票时表达了这一立场及其他关切。

马来西亚

187. 马来西亚指出，由于物联网、云计算、人工智能等技术以及洋葱路由器和暗网等服务的发展，网络犯罪变得更加复杂。这些技术是一把双刃剑：它们一方面为国家和政府带来好处，但另一方面也被某些犯罪的行为人所利用。因此，马来西亚政府在打击为犯罪目的使用信息和通信技术行为方面面临更多挑战。

188.马来西亚指出，由于假名和匿名因素，网络环境为犯罪行为人提供了温床，并给执法机构发现犯罪并将其与具体个人联系起来带来了挑战。加密技术的广泛使用在确保机密性和完整性方面带来了巨大好处，但也给执法机构在收集网络犯罪证据方面带来挑战。这些技术也为犯罪分子从事犯罪活动提供了便利。此外，互联网上还有包括反法证工具在内的很多应用程序和工具，不仅容易下载，还可能为犯罪目的所滥用。

189. 此外，马来西亚还指出，云计算等技术的出现为犯罪分子提供了在云环境中存储信息的机会。云计算本身所具有的性质给执法机构发现和获取数字证据带来了新的挑战。从提供商控制的远程云平台发现和获取数字证据与从现场或本地发现证据有很大不同。因此，从云环境中获取数据需要使用不同的工具、技术和方法。

190.马来西亚认为，有必要解决负责处理数字证据的人员所面临的挑战以及与维护保管链和确保有全面的程序和适当基础设施有关的挑战，以提高证据在法庭上的可采性。负责处理数字证据的人员的技术能力对于避免损害和污染证据至关重要。例如，执法机构和检察官不仅在留住现有专家方面面临挑战，而且在获取新资源以处理网络犯罪调查方面也面临挑战。此外，还需要提高法官和检察官的技能和能力，加强他们对信息和通信技术及网络安全基础知识的了解，包括与计算机和网络系统有关的术语。因此，需要为法官和检察官提供网络安全、网络犯罪和互联网技术方面的专门培训。

191. 马来西亚认为，电子证据非常不稳定，修改或删除起来非常简单。因此，时间在取证过程中至关重要。马来西亚还报告称，执法机构的人力资源不足是国家当局面临的另一个挑战。一些执法机构甚至没有一个专门致力于网络犯罪调查的团队。电子证据通常存储在私营部门（即电信公司和互联网服务提供商）的基础设施中，而这些公司在保留和保存数字证据方面的能力存在差别。

192. 正如马来西亚所强调的，在网络犯罪调查方面，执法机构需要通过司法协助官方渠道来获取跨境数字证据，以便证据能够被法庭采信。通过这种援助收到答复可能需要很长时间，这可能会延长法庭的审理程序。此外，请求管辖区域外提供证据仍然需要考虑双重犯罪问题。

193. 马来西亚还提到政府在打击犯罪分子滥用信息和通信技术方面遇到的另一个问题：在让法律能够恰当应对当前高科技网络犯罪技术方面带来的挑战。此外，马来西亚还强调，马来西亚国内立法要求文件出具者须在法庭上核实其来源或对证据进行认证。不过，全球服务提供商等一些证人出于对文件或信息来源的真实性的考虑而不愿出庭作证，从而导致无法起诉。

蒙古

194. 蒙古强调，在过去十年中，由于互联网的质量、速度和范围进一步改善，互联网的使用迅速增加。因此，与互联网有关的犯罪和侵权行为数量也每日增加。外国犯罪集团经常通过互联网平台对个人和商业实体进行攻击。

195. 蒙古提到打击网络犯罪的三个核心要素：互联网追踪和数字追踪；分析；以及国际合作。有必要提高打击网络犯罪的能力，并在打击此类犯罪方面达到国际标准。

196. 蒙古表示，必须特别关注网络犯罪，因为此类犯罪涉及各类网络攻击、金字塔式传销计划、网上钓鱼、网上贩运、网上威胁、信用卡诈骗、网上诈骗、儿童色情制品和基于互联网的知识产权犯罪。

197. 正如蒙古所报告的，其他国家的打击网络犯罪的单位的结构和组织分为三类：(a)打击针对计算机、网络和系统的网络犯罪；(b)打击利用计算机、网络和系统实施的网络犯罪；以及(c)跟踪、加强和研究数字足迹。然而，在国家一级，蒙古在打击网络犯罪方面的人力资源不足，因为国家不愿意在该领域进行能力和人力资源的建设。例如，俄罗斯联邦有一所专门致力于培养网络安全领域人才的学校，目的是培养打击网络犯罪的未来人才队伍。目前，蒙古还没有设立一个用于培养打击网络犯罪领域未来人才队伍的专门机构。因此，今后，为了能够在引领打击网络犯罪的国家的援助与合作下打击这种犯罪，蒙古强调需要培训和建设未来人才队伍的能力，此外，还需要对现有员工进行定期培训和准备，使他们具备充分的能力来打击网络犯罪。

198. 蒙古还指出，IP 地址在调查网络犯罪和网络侵权行为方面发挥了至关重要的作用。然而，由于金融、技术和软件方面的原因，在蒙古，互联网服务提供商向多个用户提供一个 IP 地址，因此，很难明确犯罪行为的确切时间和日期。因此，很难追踪到实施网络犯罪或网络侵权行为的个人。为了获得通信监管委员会的相关牌照，互联网服务提供商必须具备技术能力，以确保最多 20 人共享一个 IP 地址。不过，蒙古认为该规定的执行既不充分，也没有什么效果。因此，如果不解决与 IP 地址有关的问题，就几乎不可能对网络犯罪启动快速调查。

199. 此外，蒙古还强调，有必要对《刑法》规定的一些条款进行澄清。例如，有必要对蒙古《刑法》第 26 条规定的“电子设备”、“受保护的网络”和“非法攻击”等术语作出进一步澄清；在实践中，对这些术语的使用有困难，因为其他法律和法案中也没有对这些术语进行澄清或作出解释。其他国家在网络犯罪方面的细则和条例非常全面。《刑法》规定的此类犯罪的构成要件很明确；因此，相关条款不存在混淆或误解的可能。

200. 蒙古公民大多使用脸书、推特、Instagram 和雅虎等互联网社交平台，这些社交平台都是根据不同国家的法律和法规注册的。因此，国家当局不可能从在国外注册的实体那里获得调查网络犯罪所需的文件。蒙古和美国就请求取得文件问题签订了一份警方合作文件。然而，根据美国法律规定，要想取得相关文件，必须获得有关取得文件的司法命令，这使合作变得不可行。

201. 蒙古认为，有必要通过一项打击网络犯罪的国家方案。通过这一方案，就有可能分阶段和可持续地实施打击网络犯罪的政策行动。蒙古可改善打击网络犯罪相关法规的现状，并设立一个专门负责打击此类犯罪的单位。

202. 在当今时代，信息技术飞速发展，提高国家网络安全和打击网络犯罪至关重要。蒙古在国际电联全球网络安全指数（2018 年）中排第 84 位。随着信息技术的发展，网络犯罪变得更加复杂，涉及新型犯罪。要清除在互联网上实施的网络犯罪几乎不可能。然而，通过使用相关法律法规，蒙古能够通过预防和打击两种手段应对这种犯罪。

203. 此外，蒙古还表示，公众遭受网络犯罪侵害的主要原因是没有意识到危险的存在，并且缺乏关于网络犯罪的必要的知识、信息和警告。因此，蒙古强调有必要进行建设能力，并在互联网上向公众传播网络犯罪潜在危险的意识。必须执行严格遵守技术要求，监督相关规定的执行情况，解决短期 IP 地址问题和其他困难，并增加互联网服务提供商的责任，以预防、抑制、发现和打击网络犯罪。

204. 蒙古指出，从目前的状况可以明显看出，执法机构应当做好预防和打击此类犯罪的准备。因此，必须对相关人员进行培训和教育，并尽力提高这些机构在打击网络犯罪方面的能力。还需要建立一个负责侦查、加强、研究和分析数字足迹的实验室，并增加打击网络犯罪的单位的数量。

205. 蒙古认为，有必要制定一部用于打击和应对涉及信息和通信技术的犯罪的国际法律文书。

摩洛哥

206. 摩洛哥指出，当今世界正在经历一场信息和通信技术革命，包括由大公司开发的高端计算机和信息处理程序。全球化和便捷的信息传输对这一进程产生影响，使法律和司法系统之间的距离进一步缩小。这些全球化因素导致犯罪和实施犯罪的方法全球化。尽管信息技术具有种种优势，但由于遭到滥用和偏离预期目的，信息技术也带来了一系列严重的负面后果，这主要体现在对个人、机构和国家的基本价值观和利益的攻击。出现了许多通过使用互联网和电子媒体实施的犯罪，这又反过来使实施这些犯罪以及（在确定犯罪者身份和地点方面）逃避司法管辖变得更加容易。

207. 摩洛哥报告称，根据分权司法警察部门在这方面开展的调查，与应对网络犯罪有关的挑战一般涉及以下方面：

(a) 匿名：使用代理服务器和暗网；

(b) 跨国：将证据存放在境外的服务器上；

(c) 频繁使用数据加密；

(d) 非法滥用加密货币；

(e) 不断变更所用操作模式；

(f) 难以获取在国外托管的某些应用程序或网站上的用户迁移数据；

(g) 为参与网络犯罪调查和数字证据的人员安排有关打击网络犯罪的持续培训，以跟上日新月异的技术进步的步伐；

(h) 获取充足、有效的专门硬件和软件，以开展与网络犯罪有关的调查；

(i) 信息和通信技术用户应该参加关于不遵守保护措施所面临风险的提高认识方案；

(j) 启动独立国家联合体的保护机制和应对网络相关威胁；

(k) 在澄清法律问题、执行相关法律、调查机制和有效开展涉及数字证据的调查方面开展国家间合作与协调。

208. 摩洛哥回顾指出，国际社会已通过规范性文书对网络犯罪做出了回应，通过了相关公约，举行了很多会议。因其所处的战略位置，摩洛哥还必须通过立法来处理信息学现象，建立伙伴关系，特别是与欧洲联盟建立伙伴关系，这么做非常有帮助。

209. 根据刑事司法的一般原则，摩洛哥立法者颁布了适合为犯罪目的使用信息和通信技术行为独特性的刑事立法。这些立法包括在 2003 年作为《刑法》的一部分（第 3/607 节至第 11/607 节）通过的关于自动化数据处理系统管制问题的第 03.07 号法律。这部法律是摩洛哥打击网络犯罪的基本框架，其各项条款源自国际公约，特别是《欧洲委员会网络犯罪公约》及其《附加议定书》。该《公约》和《议定书》是以第 1.14.85 号皇家法令形式于 2014 年 5 月 12 日发布的，以期实施关于批准《网络犯罪公约》的第 136.12 号法律。另外，该法律也受到关于打击信息技术犯罪指南的法律草案的启发。

210. 摩洛哥还根据 2013 年 3 月 13 日第 46.13.1 号法令批准了于 2010 年 12 月 21 日在开罗签署的《阿拉伯打击信息技术犯罪公约》，实施了于 2013 年 4 月 4 日在《第 6140 号政府公报》上公布的第 12.17 号法律。

211. 关于军事司法的第 108.13 号法律的第 3 条对与属于军事法庭管辖范围内的犯罪有关的某些要求做出了规定，允许该法庭也可对网络犯罪作出裁决。

212. 关于实施第 53.05 号电子法律数据交换法的 2007 年 11 月 30 日第 1.07.129 号皇家法令和关于实施第 09.08 号个人数据保护法的 2009 年 2 月 18 日第 1.09.15 号皇家法令等一些旨在保护个人数据或电子数据交换的预防性法律使摩洛哥成为信息技术和数字经济领域的投资目的地。

213. 通过 1997 年 8 月 1 日第 1.97.162 号皇家法令发布且经过了修订和补充的第 96-24 号邮件和通信法和 2009 年 5 月 21 日第 444-08-2 号法令设立了国家媒体技术和数字经济委员会，负责协调国家政策并评估其执行情况。

214. 根据第 187 条、第 448/1 条和第 448/2 条制定的有组织信息犯罪法草案也为应对这种犯罪提供了很多工具。

215. 在机制层面，成立了负责打击网络犯罪的司法警察工作队。在摩洛哥国家安全机构中，设立了两个反恐单位，负责在调查和通过互联网追踪犯罪分子的两个层面打击与信息系统有关的犯罪。国防部设立了网络犯罪总局，负责处理网络犯罪，追踪其影响，并通过与多个国家和国际安全部门协调来打击这种犯罪行为。

216. 尽管作出了这些努力，摩洛哥强调，在打击这一罪行方面仍存在许多挑战。在立法方面，很难就网络犯罪的迅速发展提出对策，例如，对于通过社交网络实施的犯罪，缺少这方面的法律框架。大多数现行法律规定都与社交媒体用户有关，但没有纳入确定网络服务提供商责任并迫使他们删除、屏蔽、停止或禁止访问非法电子内容的任何规定。更为严峻的是，这些平台的大多数提供商和管理者都在国家管辖范围以外。

217. 摩洛哥强调，在与其他管辖区域的电信服务提供商进行沟通方面，就打击网络犯罪开展国际合作也构成挑战，这需要通过一项国际文书，以便能够与其他管辖区域的服务提供商进行直接合作，以确保跨境数据的连通性。

218. 另一方面，摩洛哥还强调，在加强执法机构的能力方面，打击网络犯罪构成更大的挑战。互联网相关犯罪、网络攻击、钓鱼攻击、电子钓鱼、互联网接入、虚拟货币、云计算和加密等网络犯罪技术的大规模连续发展要求调查机构改变其在犯罪推理方面的搜索和调查策略，并提供可被司法机构接受且被其视为权威的电子名录。

缅甸

219. 缅甸指出，打击网络犯罪对保护国家网络安全和国家信息基础设施至关重要。迫切需要制定符合国际标准的适当国家法律，以在打击网络犯罪方面取得最大成效。应向执法机构提供开展有效调查和成功起诉所需的法律文书、技术工具和基础设施以及适当的授权。

220. 此外，缅甸强调，找到网络犯罪威胁的应对战略和解决办法是发展中国家面临的一项重大挑战。关于地域差异，非法内容网站的违法者为避免刑事调查会将其活动转移到未将非法内容定为刑事犯罪的国家。将这种非法活动转移到国外是执法机构面临的挑战之一，因为服务器位于本国领土之外。违法者充分利用这种领土差异，不在本地硬盘驱动器上传播、分发、共享和存储非法内容和冒犯性的图片，而是在他们可以通过互联网访问的外部服务器上进行此类活动。因此，国际合作对于查明罪犯和解决领土差异带来的困难至关重要。在通过国家网络安全政策和制定适当的法律框架时，应将符合国家现行法律以及与国际标准保持一致考虑在内。

221. 缅甸报告称，其在起草网络安全政策及后续法律文书方面遇到以下挑战：

(a) 需要就打击网络犯罪问题通过与国际惯例和程序相一致的全面的国家政策框架和适当的立法。该国需要使其关于网络安全和打击网络犯罪的战略与国际标准保持一致；

(b) 对现行国家法律进行全面分析对于确定网络立法与其他成文法之间可能存在的任何差距和重叠至关重要。详细审查相关法律非常费时，还需要适用很高的专业标准，并需要考虑一些基于国际惯例的概念和进行意见交流；

(c) 需要建立一个执法机构，以确保国家安全和法治尊重公民的基本权利。同时，必须建立一个合法的拦截中心，采用基于数据保护和隐私保障国际原则和标准的合法拦截标准操作程序，实行通信监督；

(d) 应建立网络事件和网络攻击应对小组（即计算机应急响应小组、计算机事件应对小组、计算机安全事件应对小组），并使其具备进行网络危机管理以及威胁和脆弱性评估的充分资格。这些小组应就网络事件、网络风险和网络攻击以及此类网络攻击的潜在风险向公众传播安全信息和提供安全建议，并通过必要的技术援助为执法机构提供支持，以便其能够开展有效调查；

(e) 国家应提供资金支持，为创建安全、可靠的互联网以及确保互联网安全和网络保障采取多种技术保护措施，包括提供执行此类保护措施和开展安全活动所需的基础设施、设施和设备；

(f) 在调整国家网络立法框架以规范刑事调查活动的同时，在使用个人数据时必须考虑保障人权；

(g) 需要为参与收集、存储或共享用户数据的私营部门提供明确和精确的数据保护标准和隐私保障；

(h) 互联网用户应当获得关于网络安全、网络犯罪的性质和类型以及网络攻击的综合复杂情况的明确信息。此外，在面向本国用户推出全球联网信息和通信技术本地化服务的地方，应当支持开展有关提高用户意识的运动和培训，提高数字素养。

222. 在缅甸，网上诈骗和网上诽谤案件频繁发生。常见的网上案件涉及利用在线信息和通信煽动种族和宗教骚乱以及对政府工作人员和组织实施威胁的行为。缅甸面临的主要问题是社交媒体被用于恐怖行为，进行宣传和实施人身攻击。在开展刑事调查时，主管机关从互联网服务提供商那里得不到具体信息或配合。

223. 此外，缅甸报告称，在需要向外国社交媒体公司请求关于订购者用户的信息时，这些公司会以这些请求不符合标准程序为由拒绝请求。因此，在调查过程中遇到了困难。

224. 缅甸还提到，由于缺少技术人员资源、缺少对网上用户的了解以及法律和程序的法律约束力弱，在调查中遇到了许多困难。随着技术的发展，人们可以在手机上访问手机银行业务，因此，手机用户现在成为了网络攻击的目标。

225. 缅甸认为，现有法律机制不足以打击通过使用信息和通信技术实施的犯罪。缅甸报告称，政府正在起草关于电子政务、电子商务和网络安全事项的网络法律和相关政策，该项目由交通电信部牵头实施，一家外部咨询公司为其提供咨询意见。

226. 缅甸指出，可制定并通过一项联合国公约来解决这一问题，因为在这方面需要开展国际合作。

227. 缅甸同意，应对为犯罪目的使用信息和通信技术行为需要在所有相关国家参与下开展长期公开讨论。可设立一个不限成员名额的联合国工作组，为这一讨论提供平台，该工作组的任务授权是制定所有相关文件，并以多数票赞成的方式做

出决定。缅甸还同意并赞赏全面研究网络犯罪问题专家组重点讨论与打击信息犯罪有关的问题。

荷兰

228. 荷兰指出，防止互联网成为罪犯分子的安全避风港是国际警务和司法界的共同责任，决不允许犯罪分子有利可图。尊重基本人权的有效法律文书对于打击网络犯罪至关重要。可以确定不同类型的文书：国内、区域和国际文书。首先，许多国家加强了本国打击网络犯罪的能力。然而，由于在刑法、专门知识和设备方面存在国际差距，致使处理和应对这种跨境现象变得困难。这种差距只能通过加强国家内部和国家之间的能力建设的努力来解决。通过让有能力的执法机构建立起广泛的国际网络，可以对有组织网络犯罪予以沉重打击。第二类文书是区域文书。它们之所以被称之为区域文书是因为该区域以外的国家无法利用这类文书。此类举措的例子包括欧洲联盟电子证据倡议以及上海合作组织、非洲政府间组织及阿拉伯国家联盟的框架。第三类是向世界各国开放的国际文书。此类文书的例子包括《欧洲委员会网络犯罪公约》，该《公约》有 63 个缔约方（而且在增加），并且另有大约 70 个国家将其作为一种示范立法，此外，这类例子还包括《打击有组织犯罪公约》及其各项议定书。作为《欧洲委员会公约》的早期签署国和批准国之一，荷兰通过调整国内法以增加与其他缔约国合作的可能性，在刑事调查方面享受到《公约》带来的好处。荷兰还强调了《打击有组织犯罪公约》框架带来的好处。

229. 荷兰表示，在网络空间执法方面最相关且最紧迫的实际需要是，第一，跨境获取电子证据，第二，在刑事调查方面开展国际合作。在迅速发展的跨境犯罪案件中，缺少双边合作与司法协助。鉴于信息和通信技术的使用，特别是社交媒体和网络短信等多项新增功能的使用，当今需要针对各类犯罪提供电子证据，导致数字数据空前增加。只有执法机构具备参与联合调查等活动的能力和实力，才能加强国际合作。出示令或扩大网络搜查等关于跨境获取电子证据的创新方法已在开发和讨论之中。目前就《欧洲委员会网络犯罪公约》的一项附加议定书进行的谈判证明，许多国家都愿意调整现有框架，以便有效加强网络空间领域的刑事司法。

230. 荷兰表示，在打击为犯罪目的使用信息和通信技术行为方面面临的一大挑战是让现有文书能够充分发挥其潜力，而不是将本已稀缺的资源和精力转移到一个长期进程上以寻求新的超国家框架。《欧洲委员会网络犯罪公约》已是一项切实的成果，每天都在体现其附加值。从美国到斯里兰卡和日本再到塞内加尔的执法机构和司法机关都可以利用《公约》提供的不同可能，使刑事调查取得具体的结果。《公约》的附加议定书是目前为及时了解最新情况和提供最先进解决方案所需努力中已在进行的一个步骤。

231. 随着时间的推移，虽然在能力建设方面投入了巨大努力，但仍有许多工作要做，这是第二大挑战。这可以在双边合作的基础上进行，也可以与欧洲委员会网络犯罪方案办公室以及毒品和犯罪问题办公室共同进行。就联合国而言，全面研究网络犯罪问题专家组是搭建交流意见和最佳做法平台的理想之地。荷兰报告称，在去年和今年的深入磋商期间，专家组在执行其 2017 年工作计划方面取得了重大改进。荷兰预计，这一进程将促成在 2021 年对网络空间刑事司法领域面临的挑战进行更新的和更具议题性的概述，并对未来提出指导性建议。

232.荷兰呼吁改进 2017 年成立的全面研究网络犯罪问题专家组的工作，以此为基础做出进一步努力，并期望对技术援助予以最大程度的重视，以促进在全球范围内转让最佳做法和开展能力建设。荷兰呼吁各方参与现有已经证明其价值并取得成果的现有谈判。它将呼吁其他国家不要发起新的倡议，以免分散为这些谈判投入的资源和精力。

新西兰

233. 新西兰指出，地理上的分隔使本国在历史上免遭某些威胁。但网络犯罪的无国界性质意味着距离无法提供保护。新西兰在打击为犯罪目的使用信息和通信技术方面面临的特别挑战包括：

(a) 对新西兰和世界网络犯罪情况没有完全的了解；

(b) 难以计算网络犯罪的成本；

(c) 难以发现、调查和起诉网络犯罪；

(d) 因政府、非政府组织、私营部门和个人之间分担责任产生的问题。

234. 在应对网络犯罪方面，新西兰报告称，适当的立法、联合办法、提高认识与教育以及国际合作是其重点工作领域。为本报告目的提供的信息摘自于《国家打击网络犯罪计划》（2015 年），该计划可在网上查阅。

235. 对网络犯罪的情况没有完全的了解。网络犯罪与“传统犯罪”的区别在于前者具有全球性，这给执法机构带来了挑战。无论是个人还是团体，即使身处国外，凡是在能够接入互联网的地方都可以进行操作。犯罪者绝大多数将国外作为大本营，并且组织严密。在世界范围内，有许多未报告的网络犯罪案例。在某些情况下，受害者甚至不清楚其本人是否已经受到了影响。其他受害者或因过于难为情而不敢举报这种犯罪，或不知道向谁举报，或不相信执法实体能够提供补救措施。即使受害者能够从提供商或金融机构那里获得补救，他们可能也不会报案。最后，因担心声誉受损，企业可能也不愿揭露所遭受的损失或违规行为。

236. 网络犯罪的成本难以计算，网络犯罪的间接成本，包括机会成本，也难以量化。对于许多中小型企业来说，网络犯罪可能会导致“被迫停止营业”：虽然没有任何商品被窃取，但会对它们的交易能力产生冲击。企业和个人还要承担防范网络犯罪和寻求补救（如需要）的成本。网络犯罪还会导致物理犯罪的组织和实施，例如欺诈、敲诈勒索、动乱以及性和其他暴力攻击。网络犯罪可能以制造尴尬和滋扰的方式造成社会危害，在更严重的情况下，可能会导致身体或情感受到伤害。虽然网络犯罪造成的经济损失在个别情况下可能很小，但随着时间的推移，会对公众信任和信心产生破坏性影响。于犯罪分子而言，网络犯罪成本低，风险也相对较小，因此，是一项高回报活动。数以千计的垃圾邮件可能给每个受害者带来的损失并不大，但对整个新西兰带来的损失要大得多。

237. 发现、调查和起诉网络犯罪是一件难事。网络犯罪的全球性因素使得找出犯罪者并获取相关证据困难重重。不同国家之间的信息交流和合作可能不尽如人意，即使存在强有力的合作关系，司法协助条约进程也可能非常缓慢且繁琐。有些案件可能需要开展大量调查工作，从而减少了处理其他需求所需的可用资源。犯罪者所在国可能也不具备开展调查或保存证据的必要能力。

238. 由于互联网上的操作能够以近乎匿名的方式进行，这让调查变得更加复杂。网络事件中的责任追究非常困难，特别是当攻击来自海外时。这使得网络犯罪不仅对调查而且对起诉都带来了挑战。代理服务器以及洋葱路由器和点对点网络等渠道可能被犯罪分子利用，试图通过层层加密隐藏其身份。这些网络经常被用来为犯罪活动提供便利，并对执法机构带来挑战。这类网络和暗网站点也将网络犯罪作为一项服务进行推销，例如雇佣黑客服务或提供简单工具包服务。这些技术发展降低了从事网络犯罪的门槛。因此，一些行为体即使技能不熟练，也会产生相对破坏性的影响。另一方面，随着活动的扩散和技术的日益复杂，犯罪行为体与国家行为体（其中一些人可能也有犯罪意图）之间的界限正在变得模糊。随着技术和侦查策略的发展，这些犯罪行为体也在提高自身能力，这使应对者很难跟上步伐。罪犯并不介意使用匿名技术，包括使用洋葱路由器等软件，试图隐藏提供儿童剥削材料和毒品交易的网站。

239. 在新西兰，应对网络犯罪的责任由政府、非政府组织、私营部门和个人共同承担。在新西兰，有多个政府机构承担与网络犯罪有关的政策和业务责任。这些职责在很大程度上是自然形成的，而不是经设计的。网络犯罪是一个共同问题，非政府组织、民间社会和私营部门都可以在预防和应对网络犯罪方面发挥作用。不过，这种责任分担可能会带来挑战。有些案件要向多个地方报告，受害者可能要奔走于多个机构之间，以努力找到解决问题的最佳地点。各服务提供方制定的对策也可能存在很大差异。随着新西兰计算机应急小组于 2016 年成立，新西兰在这一领域取得了进展。新西兰计算机应急小组是一个机构，负责提供有关在何处举报网络事件的明确信息、向相关机构提供对网络事件的更有效分类以及向机构、企业和个人提供更可具操作性、更及时的建议。很多私营公司还将提供应对网络犯罪的措施作为其核心客户服务的一部分。这为政府改善犯罪受害者的经历并同时更好地认识这一问题和提高认识提供了机会。

尼加拉瓜

240. 尼加拉瓜认为，现行刑罚条款不足以打击利用信息和通信技术实施的犯罪。许多国家都是这类犯罪的受害者。因此，尼加拉瓜深信，这一专题应由联合国来处理，以期制定和批准一项有关该专题的国际合作和监管协定。

241. 同样，尼加拉瓜认为，现在是尽快设立一个不限成员名额工作组的适当时机，以期推动起草一项关于使用信息和通信技术实施犯罪问题的国际监管文书。

挪威

242. 挪威提到其在 2019 年 3 月 4 日就打击网络犯罪的措施和倡议问题向毒品和犯罪问题办公室提交的与全面研究网络犯罪问题专家组工作有关的意见。[8]

243. 挪威于 2005 年批准了《欧洲委员会网络犯罪公约》，并正在密切关注第二附加议定书的制定进程。挪威支持全面研究网络犯罪问题专家组至少到 2021 年一直作为联合国一级关于网络犯罪专题的主要进程。

[8] 可查阅 www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-March-2019/Compilation_12March.pdf。

244. 挪威指出，随着网络安全领域的威胁不断加剧，必须增加应对挑战的措施，因为缺乏有效措施可能会威胁法治。电子证据在犯罪案件中越来越重要。这些数据通常存储在国外，因此，很难定位和获得。国内和国际合作均发挥有益作用。由于执法机构受到国境限制，因此，需要更加有效的国际框架。同时，制定新国际文书的工作中心必须坚持基本权利和具有高度的保障意识。

245. 挪威确认，它将确保有足够的能力、权限和技术能力来应对不断变化的新型犯罪。挪威提到，需要将提高对数字领域面临的威胁的认识作为本国的工作中心。在更为传统的犯罪背景下看待这些新挑战也很重要。网络犯罪不是一种孤立的犯罪类型：它是包括跨国有组织犯罪和恐怖主义在内许多犯罪类型的共有要素。政府和私营部门采取协调一致的行动是解决方案的核心部分。

246. 挪威还强调，挪威主管部门将根据《挪威国际网络战略（2017 年）》，确保在制定关于网络犯罪和处理网络事件的国际网络安全政策与合作领域内代表挪威的各机构之间进行密切协调。在国际社会持续打击网络犯罪的努力中，挪威将支持采取协作方式，在维护民主价值观和保护普世人权的同时，寻求良好解决方案。

秘鲁

247. 秘鲁报告称，2016 年，美洲开发银行与美洲国家组织合作编写了《2016 年拉丁美洲和加勒比网络安全报告》。在对涉及不同领域（政治与战略、文化与社会、教育、法律框架和技术）的 49 项指标进行评估后，确定秘鲁面临以下四项主要挑战：

(a) 强化武装部队的网络保护能力；

(b) 强化高科技犯罪调查司处理电子证据的技术能力；

(c) 提高社会对网络安全的认识；

(d) 提高大学教师的能力，向公司提供培训。

248. 根据《微软安全情报报告（2017 年）》，秘鲁有 16.9%的计算机感染了恶意软件，而世界平均水平为 7.8%。同样，在秘鲁，感染特洛伊木马病毒（8.13%）、计算机蠕虫病毒（5.7%）和其他病毒（0.92%）的比例也高于世界平均水平。

249. 在最近的一项研究中，秘鲁部长理事会主席团数字政府秘书处表示，有 22.6%的公共行政实体没有能力实施其通用数字安全系统。原因如下：

(a) 实施该系统所需的经济资源不足；

(b) 工作人员不足（50.9%）；

(c) 知识不足，无法开始实施（22.6%）；

(d) 不是其部门的优先问题（16%）。

250. 信息安全风险对组织的关键资产造成严重的负面影响，给实体带来了经济损失和被动成本。在一些案例中，当企业为了恢复信息而被敲诈或勒索大量金钱时，其主要业务往往中断或停止。

251. 为应对重点挑战，秘鲁政府认为有必要设立专门的计算机犯罪检察官办公室，就此问题加强对税务工作人员的培训，并设立一个负责预防公民网络犯罪的机构。计算机犯罪，尤其是计算机欺诈犯罪的投诉数量显著增加。必须面对的主要挑战有：

(a) 通过“伪造银行卡”实施计算机欺诈：犯罪组织利用银行卡机密信息，利用境外域名和服务器在网店上进行在线购买。这使得很难通过调整各国法律的方式及时获得各公司必须提供的信息；

(b) 通过社交网络盗用身份信息：这是由于用户可以自由创建账户并进行匿名浏览，甚至可以创建不同用户名用于非法用途；

(c) 诱骗儿童：犯罪组织伪装成儿童，诱骗受害者在笔记本电脑或计算机摄像头前脱衣服。或者，与儿童见面并在此期间获得儿童性虐待材料，通过 WhatsApp 等应用程序，向国内和国际的其他恋童癖者出售或与之交换；

(d) 对以前的伴侣进行敲诈或勒索：威胁将其涉及性爱的视频或照片发布到互联网上。这可能出于不同的目的，如获得经济利益或恢复关系；

(e) 黑客活动分子发起的宣传攻击：其目的是影响机构形象，他们使用洋葱路由等匿名网络，使攻击来自亚洲国家，从而无法识别其身份。同样，出于商业目的攻击机构信息的案件也正在发生，目的在于从一些实体获得广泛的信息以达成犯罪目的。媒体机构也有可能进行网络攻击或从事网络间谍活动，以获取有新闻价值的材料。

菲律宾

252. 菲律宾称网络犯罪是一种严重的社会问题，并指出网络空间是（除水、陆、空以外的）一个新维度，政府必须对其进行监管，执法机构必须扩大其任务授权以便网络空间纳入其工作范围内。为确保人民的安全和保障，政府已认识到需要通过以下立法为执法机构配备能力：2012 年《预防网络犯罪法》（第 10175 号共和国法）、2000 年《电子商务法》（第 8792 号共和国法）、2009 年《反偷拍及偷窥法》（第 9995 号共和国法）、2009 年《禁止儿童色情制品法》（第 9725 号共和国法）、2003 年《反贩运人口法》（第 9208 号共和国法）、1998 年《接入设备监管法》（第 8484 号共和国法）和 2012 年《数据隐私法》（第 10173 号共和国法）。

253. 菲律宾于 2018 年 2 月 20 日加入《欧洲委员会网络犯罪公约》，并考虑到了有关数据保存、提供用户订阅信息、收集计算机和商业数据和查封域名的国际要求。

254. 在此背景下，该国法律认为专业化是成功调查和起诉网络犯罪分子的关键。根据 2012 年《预防网络犯罪法》设立了以下专门机构来处理网络犯罪及相关问题：

(a) 司法部网络犯罪办公室：根据《预防网络犯罪法》设立的中央机关，旨在确保《欧洲委员会网络犯罪公约》的实施，包括负责国际互助和引渡等相关事项；

(b) 网络犯罪调查和协调中心：根据2015年第10844号共和国法设立的一个机构间机构，受信息和通信技术部行政监督，负责相关机构间的政策协调以及国家网络安全计划的制定和执行；

(c) 国家调查局网络犯罪司：根据《网络犯罪法》的规定进行了重组，以有效提高其网络应对、数字法证和网络安全能力。该机构设立了三个网络犯罪地区中心，获得了最新的法证工具和软件，并为其数字审查人员提供了相应的培训；

(d) 国家警察局反网络犯罪小组：与全国九个地区反网络犯罪办公室一并成立。该小组为专门从事网络犯罪工作的警察人员编写了四门反网络犯罪专业课程。

255. 在主管通信、电子和信息系统事务的副参谋长带领下，菲律宾武装部队正在起草一项网络空间战略计划，为到2022年建立具备完全网络空间能力的组织提供路线图。

256. 反洗钱理事会是菲律宾金融情报机构，其任务是实施经第9194、10167、10365和10168号共和国法修订的《反洗钱法》，又称2012年《预防和打击资助恐怖主义法》。

257. 2017年1月，除了被指定为商事法庭外，司法机构还通过指定网络犯罪法庭负责裁定2012年《预防网络犯罪法》所涉案件的方式为打击网络犯罪工作做出了贡献。

258. 菲律宾还报告称，在国家一级建立了以下机构间合作机制：

(a) 国家执法协调委员会网络犯罪小组委员会：通过协助其他国家的反网络犯罪活动，例如，通过促进信息共享和逮捕参与网络犯罪的人员等方式，加强在打击网络犯罪及其他网络犯罪相关活动方面的机构间协调；

(b) 打击贩运活动机构间理事会：为有效实施经第10364号共和国法（即2012年《经扩充的反贩运人口法》）修订的第9208号共和国法（即2003年《反贩运人口法》）颁布细则和条例。该理事会由司法部长领导，这使方案和项目的协调工作得以加快，以有效解决人口贩运相关问题。它建议采取措施，通过双边和（或）多边安排，加强与其他国家之间的相互协助，以预防和打击国际贩运人口行为；

(c) 禁止儿童色情制品机构间理事会：由社会福利与发展部部长领导，由其他相关政府机构和非政府组织组成，负责制定全面和综合性计划和方案，以预防和禁止任何形式的儿童色情制品，对违反2009年《禁止儿童色情制品法》（第9775号共和国法）规定的个人、机关、协会或机构提起诉讼。

259. 关于执法和调查的良好做法，菲律宾认识到在执法和调查中利用专门机构的重要性。对菲律宾而言，机构间合作对于有效执法和案件调查至关重要，而国家执法协调委员会网络犯罪小组委员会、打击贩运活动机构间理事会和反儿童色情制品机构间理事会是牵头机构。

260. 菲律宾还指出，国际刑警组织是执法机构利用的另一种机制，而设在马尼拉的国际刑警组织国家中心局在处理跨国犯罪方面充当国内和国际警务合作的主要

协调机构。与执法机构、其他政府机构和外国执法机构的密切合作对于调查、追踪和起诉网络犯罪实施者至关重要。

261. 菲律宾跨国犯罪中心是设在马尼拉的国际刑警组织国家中心局的秘书处，该中心与反洗钱理事会共同主办了关于孟加拉国银行被盗资金的国际刑警组织业务会议，这是最大的洗钱案件之一。

262. 关于在收集电子证据和刑事实践方面的良好做法，菲律宾报告称，专门机构已使用数字法证对网络犯罪的罪犯进行追踪、调查和起诉。2012 年 9 月 12 日批准的 2012 年《预防网络犯罪法》已于 2014 年 2 月 18 日生效。该法加上对最高法院发布的电子证据规则的采用使网络犯罪法庭对网络犯罪案件的起诉变得更加有效。

263. 网络犯罪调查与协调中心于 2017 年 5 月 2 日启动了《2022 年国家网络安全计划》，认识到保护菲律宾境内每个互联网用户、国家关键信息基础设施、政府网络、中小企业及其他企业和公司的紧迫性。

264. 尽管政府正在与专门机构一道努力打击网络犯罪，颁布了打击网络犯罪的法律、建立了网络犯罪法庭并采用了电子证据规则，但仍需向专业人员和专家提供使用这些工具的培训。应当利用正在进行的能力建设活动，特别是由当地或外国赞助的活动。此外，应定期对网络犯罪和网络安全进行评估和评价，以便明确菲律宾今后要在哪些方面做出努力。

葡萄牙

265. 葡萄牙指出，信息和通信技术为犯罪分子创造了新的机会，导致数字世界中以及通过数字世界实施的犯罪所占比例和多样性增加。由于对充分享有人权和公民自由产生影响，此类犯罪对国家和企业的关键基础设施稳定以及个人福祉的影响与日俱增。在数字时代，各国关心的问题包括利用技术和互联网传播恐怖主义内容，宣扬仇恨言论、极端主义和激进主义，以及实施性虐待儿童、贩运人口和洗钱等其他严重犯罪。

266. 葡萄牙指出，由于加密技术的使用、难以获得和保存电子证据、网络空间管辖权的行使以及缺少在此方面的国际合作，致使各国在刑事调查中面临困难。加密技术的使用符合保护隐私和行使基本权利的合法需要，也符合企业和公共主管部门的需要；企业已对开发能更好地保护其客户隐私的工具进行投资，并表示弱化加密可能会将隐私信息暴露给可能滥用这些信息的人。安全处理是保护个人数据的重要因素，欧洲议会和欧洲联盟理事会第 2016/679 号条例承认加密是一项安全措施。然而，在保护数据或信息安全的同时，加密技术也为犯罪分子提供了好机会。

267. 鉴于电子证据的规模和复杂性，调查和起诉面临的另一挑战是如何获得并确保存储在计算机系统中的电子证据的安全。网上服务可从任何地方提供，不需要实物机构、设施和人员在相关国家出现。因此，相关证据通常存储在调查国之外的服务器上，可能位于一个或多个境外管辖区域，甚至是未知的管辖区域，而且可能涉及跨国服务提供商。

268. 由于不同管辖区域的调查机构之间缺乏联系，司法合作请求通常需要跨境获取电子证据，而且往往涉及拥有大量服务提供商但与这些程序没有具体关系的国家。通过司法合作获取证据可能需要很长时间，而在此期间，这些证据可能已经不存在了。另一个困难在于，与私营服务提供商的合作没有明确的框架，而各国开展此类合作的方法各不相同。

269. 葡萄牙提到，预防和打击通过互联网及其他信息和通信技术煽动恐怖主义、传播恐怖主义内容和宣扬激进主义和极端主义是各国在国际一级面临的其他挑战。

270. 打击通过信息和通信技术实施的犯罪和网络犯罪是葡萄牙的战略关切，且葡萄牙坚定致力于这一斗争。一项打击计算机犯罪的法律于 1991 年通过（第 109/1991 号法），并在 2009 年进行了修订（第 109/2009 号法（《网络犯罪法》））。目前，正在对《网络空间安全国家战略（2015 年）》进行修订，新的国家战略预计将在未来几个月内发布。新旧战略均将使用信息和通信技术及网络犯罪列为最重要的问题之一。

271. 葡萄牙还报告称，关于保留在提供公开可用的电子通信服务或公共通信网络过程中产生或处理数据的法律已经获得批准。这对恐怖主义和有组织犯罪等严重犯罪的刑事调查尤为重要。

272. 葡萄牙认为，适当的现代国内法律框架、提供适当的程序工具和权力以及从而允许执法机关和检察官能够在尊重嫌疑人和受害者的权利及保障的同时调查和收集数字证据对于打击网络犯罪至关重要。

273. 葡萄牙已在其执法机构和司法机构中设立了专门单位：2011 年，在公诉署设立了网络犯罪办公室，并在刑事警察局设立了国家打击网络犯罪和技术犯罪股，以便在国家一级进行运作和协调。公诉署负责刑事调查，而刑事警察局是执法机关，按照《刑事调查组织法》（第 49/2008 号法）规定，在主管检察官的指导下，专门负责调查网络犯罪和使用信息和通信技术实施的犯罪。这种专业分工提高了调查效率，确保一致应对和国际协调。开展国际合作对从其他国家获取证据很重要，应努力进行能力建设并加强合作，特别是在联合国一级。

274. 关于其他挑战，葡萄牙指出，网络犯罪和利用信息和通信技术实施犯罪不受地域限制；它们可在全球范围内实施。全球服务（如网络邮件服务、社交网络和云服务）在世界各地广泛使用，也可用于犯罪目的，将许多不同国家的受害者作为目标。虽然一些国家意识到涉及电子证据的案件需要快速处理，但其他国家坚持使用司法协助请求等传统工具，而这些工具无法对当前的要求或挑战做出适时反应。目前，没有制定全面的国际法规，而国内框架提供的解决方案各不相同；因此，需要采取一种新的方法。

275. 葡萄牙还提到，《欧洲委员会网络犯罪公约》缔约方正在为该《公约》起草一项附加议定书。该议定书有望在跨境获取数据以及在充分尊重基本权利和自由的同时加强非正式合作、信息共享和发挥司法协助职能以获得存储于其他管辖区域内的数据方面为执法实体和司法机构提供明确指导。

276. 在欧洲联盟一级，正在就有关电子证据的条例和指令进行谈判，这将有助于保护和收集电子证据，有助于加强在此领域的合作。

卡塔尔

277. 卡塔尔指出，通过网络犯罪和电子盗版等方式滥用信息资源和技术的情况正在不断增加，影响各国的安全与稳定。各联合国实体的各种决议已对使用信息资源和技术对发展、和平、稳定和人权的不利影响进行了详细审查。在数字世界实施的犯罪及其不断增加的多样性以及利用此类技术和手段以实现与维护国际稳定和安全目标相违背的目的正在对国家的基础设施完整性产生不利影响，并切实危害其安全。

278. 有必要在国家和国际一级加强涉及网络犯罪的法律措施，并为打击、侦查、调查和起诉网络犯罪提出新的措施。有必要加强国际努力，防止将犯罪资源或信息技术用于犯罪和恐怖主义目的。为维护和平与稳定，创造开放、安全、稳定、和平的信息和通信技术环境，卡塔尔重申支持全面研究网络犯罪问题专家组，并呼吁其继续开展工作。

279. 卡塔尔报告称，它寻求加强国内信息安全，并鼓励在打击网络犯罪方面开展国际合作，特别是因为该国一直是电子盗版的受害者。电子盗版曾为创造一场人为的区域危机进行掩护，严重破坏区域和国际安全与稳定。卡塔尔特别关注其国内立法的制定以及促进有关预防、侦查和起诉数字犯罪行为人的国际联合行动。

280. 卡塔尔发布了打击网络犯罪的 2014 年第 14 号法，这是它在加强打击网络犯罪国家立法和程序方面迈出的先进的一步。该法的一些章节对侵犯信息系统、程序和网络、电子欺诈和伪造以及侵犯知识产权犯罪等网络犯罪进行了定义。该法包括有关调查程序、证据收集、服务提供商的义务、国家机构的义务和国际合作（包括司法协助和引渡）的条款。

281. 卡塔尔最后指出，网络犯罪作为一种新出现的跨国有组织犯罪形式，是一个日益严峻且不断变化的挑战。需要根据共同利益和共同责任原则采取协调一致且日益增加的集体对策。在此背景下，卡塔尔寻求加强与毒品和犯罪问题办公室的合作，以期建设国家能力，加强计算机网络的安全，促进区域和国际合作，以便提供安全和健全的网络环境。

罗马尼亚

282. 罗马尼亚指出，随着技术发展，技术在很多犯罪活动中发挥重要作用，给网上环境造成巨大的冲击和影响。“网络犯罪”一词系指传播勒索软件和其他恶意软件、涉及非现金支付的欺诈行为以及在线交易儿童性剥削材料等一系列的犯罪威胁。

283. 罗马尼亚将“依赖网络的犯罪”定性为只能借助计算机、计算机网络或其他形式的信息和通信技术才可以实施的犯罪。“网络助长的犯罪”可在线实施，也可线下实施。互联网的作用是增加这些犯罪的规模、地理范围和速度。在线儿童性剥削是最严重的网络助长犯罪。此外，暗网还拥有数量与日俱增且专门用于制作、分享和传播儿童性剥削材料的论坛。互联网还提供点到点文件共享和安全数据存储等各种各样的应用程序，为这些犯罪提供便利。

284. 罗马尼亚提到涉及非现金支付的欺诈行为，将其称为另外一种高度组织化、高度专业化且不断发展变化的威胁，并且能够适应对抗措施和新技术。该威胁包含两种截然不同的犯罪类型：主要在线实施的无卡欺诈行为和通常发生在零售店和银行柜员机上的有卡欺诈行为。犯罪分子还通常控制银行柜员机操作系统轻易获得现金。

285. 罗马尼亚报告称，在线商业平台也可用于非法商品和服务交易。表层网和暗网中的非法在线市场均可提供网络犯罪工具包或虚假文件等可用于实施其他犯罪的工具。

286. 罗马尼亚还提到被盗数据是另外一种常在网上交易且随后用于实施欺诈的商品。这些通常是财务数据，例如，被盗支付卡数据或银行账户登录的详细信息。还可能包括从完整的详细个人信息和扫描文件到电子邮件列表和在线账户登录信息等各种数据。

287. 罗马尼亚指出，犯罪分子利用一切可用的通信渠道，不仅用于内部通信，还通过电子邮件网络钓鱼活动或社交媒体等方式联系潜在受害者。犯罪分子还使用安全应用程序及类似服务来隐藏其犯罪活动。犯罪分子和其他恶意行为者使用加密服务的情况日益增加，严重阻碍对包括恐怖主义在内的所有类型犯罪的侦查、调查和起诉。

288. 加密货币、在线支付和银行平台等新的支付形式为犯罪分子提供了新的融资和扩展其非法业务的方式。跨多个管辖区域的交易的快速处理以及加密和匿名工具的激增是金融调查中遇到的一些最重要的阻碍。比特币是与网络犯罪有关的犯罪分子之间最常用的货币。虽然大多数暗网市场和自动银行卡商店都接受比特币，但越来越多地用于网络空间以外的犯罪，比如支付赎金。

289. 罗马尼亚强调，正如 2014-2017 年欧洲警察署报告所述，罗马尼亚的网络犯罪的发展变化与其他全球犯罪现象类似。源自罗马尼亚的犯罪集团在网络犯罪中非常活跃。随着时间的推移，罗马尼亚也成为此类犯罪的目标。这对包括金融体系在内的广义国家安全构成了威胁。

290. 罗马尼亚报告称，它已根据基于《欧洲委员会网络犯罪公约》的法治保障和补救办法做出巨大努力，通过了全面的程序性立法，以涵盖刑事诉讼中有关收集电子证据的不同方面。罗马尼亚于 2003 年批准了该《公约》。正如《公约》第 2 至 9 条所规定的，将非法活动定为刑事犯罪的国家立法涵盖了广泛的不当行为，使专门机构调查相关案例成为可能。这些条款在颁布 15 年后的今天仍然适用于新型网络犯罪。网络犯罪公约委员会通过的指导说明为此类犯罪的构成要件提供了补充指导。

291. 正如报告所称，2004 年，罗马尼亚检察院设立了有组织犯罪和恐怖主义调查局。此外，还在警察部门设立了打击有组织犯罪局，作为支持有组织犯罪和恐怖主义调查局开展活动的专门机构。在过去五年中，已调查了 28,800 多起依赖网络或网络助长的犯罪案件。

292. 罗马尼亚提到了这类犯罪的一个案例，即用于盗取银行卡信息的“盗读”活动涉及犯罪集团在许多不同管辖区域内的活动（部件生产、部件组装和实际欺诈行为）。这些活动属于《刑法》第 365 条的管辖范围。关于作案手法问题，社会工程学、鱼叉式网络钓鱼、多级命令和控制服务器以及漏洞扫描依然是一些最常用

的技术手段。执法面临的一个巨大挑战是，大量行为者越来越多地使用开源工具，因此很难将违法活动归咎于特定的个人或团体。《刑法》第 207 条（勒索）、第 362 和 363 条对恶意软件攻击行为做出了规定。

293. 用于实施欺诈行为的社会工程学策略（网络钓鱼、鱼叉式网络钓鱼、语音钓鱼、短信欺诈）以及主要用于劫持汇款的中间人攻击或浏览器中间人攻击技术手段成为罗马尼亚境内网络犯罪的常见形式。《刑法》第 325 和 249 条将其定为刑事犯罪（视具体情况，还可以提出滥用设备或干扰数据等其他指控）。对利用 Cobalt Strike 平台攻击银行系统的行为按《刑法》第 360、362 至 363、366 和 249 条的有关规定进行调查。

294. 对加密货币挖矿和大多数密码劫持的活动按《刑法》第 360 和 366 条的规定进行调查。对深度插入式银行卡盗读活动按《刑法》第 360 和 366 条进行调查。

295. 罗马尼亚最后指出，基于《欧洲委员会网络犯罪公约》设立的全面法律框架和专门机构有助于解决不断变化的网络犯罪和电子证据问题。目前，需要更多的资源以及进一步的培训和能力建设。讨论在此领域内缔结新的国际条约没有帮助，可能会削弱相关努力。

俄罗斯联邦

296. 俄罗斯联邦指出，长期以来，从规模和程度上看，打击为犯罪目的使用信息和通信技术行为的挑战一直是一个全球威胁，影响到全球所有国家，任何国家都无法幸免。目前，国际社会尚没有统一的方法来应对这一问题。在国际一级，缺乏全面的国际合作法律框架，甚至缺乏共同的术语基础，使得情况更为复杂。在区域一级，一些组织已制定并通过了相关文书，但它们有效处理此类犯罪的能力仍然不足。

297. 俄罗斯联邦指出，很多国家将《欧洲委员会网络犯罪公约》作为一个可能的解决方案。然而，这项文书不足以应对当前的威胁。《公约》制定于 1990 年代末，因此，无法对犯罪分子的很多现代“发明”进行监管。它还有可能违反国家主权和不干涉他国内政原则。因此，仍有以下威胁：让少数国家的特务机构不受控制地收集世界各地用户个人数据以及继续保持一些国家定下的旨在巩固其在信息领域的技术成果并保持发达国家与发展中国家之间“数字鸿沟”的趋势合法化。

298. 俄罗斯联邦强调，俄罗斯推动制定所有相关方共享的普世原则和规范，这将为打击网络犯罪方面的有效国际合作奠定基础。这一文书可以是在联合国支持下缔结的打击利用信息和通信技术实施犯罪的公约，该公约将考虑到当前的现实以及主权平等和不干涉国家内政的原则。作为正式文件分发的俄罗斯所提出的联合国合作打击网络犯罪公约草案（A/C.3/72/12）可作为这项工作的基础。俄罗斯联邦认为，该项目将引起思考，以便在一些主要国际论坛，主要是在联合国，就这一专题展开辩论，巩固和聚焦国际社会在此领域内制定切实可行的解决方案的努力。

299. 俄罗斯联邦认为，鉴于信息犯罪现象具有全球性，仅仅在联合国维也纳论坛（全面研究网络犯罪问题专家组）框架内讨论这一问题是不够的。该专家组的任

务主要局限于对此问题的技术层面进行讨论。在目前情况下，寻求政治解决和建立共识被认为是首要任务。

300. 为此，俄罗斯联邦强调，应坚定执行大会关于打击为犯罪目的使用信息和通信技术的第 73/187 号决议的各项规定。另一个解决办法是在大会内设立一个常设论坛，以综合和平衡的方式对打击网络犯罪国际合作的各个方面进行讨论，其目的是找到一个政治解决方案和建立共识，同时考虑到各国家在此领域的迫切需要以及便利交流在此领域内的最佳做法。该论坛的备选方案之一是设立一个不限成员名额的联合国网络犯罪问题工作组，其任务是拟订和执行由会员国制定的所有相关文件。

沙特阿拉伯

301. 沙特阿拉伯提到其在打击为犯罪目的使用信息和通信技术方面遇到以下障碍：

(a) 数字平台公司与世界各地法律和执法机构合作不畅；

(b) 虚拟世界中缺乏数字身份以及在互联网上使用标识符和虚假数据及冒充他人，特别是在社交媒体上；

(c) 各会员国的立法和刑事法律不同；

(d) 各国在打击网络犯罪方面缺乏协调、合作和协助；

(e) 许多国家对提供电子服务（网络、资源、云环境、服务等）的控制不充分；

(f) 许多国家缺乏先进的信息系统，无法监测可疑行动，无法查明其来源及背后的实施者；

(g) 政府、私营机构和个人在网络安全方面的人力和技术能力不足；

(h) 缺乏将为犯罪目的使用信息和通信技术行为定为刑事犯罪并加以追踪的国际立法，此类立法有助于推动打击此类行为的国际努力；

(i) 需要通过专门的培训方案提升信息安全领域内从业人员的能力素质；

(j) 各国处罚信息技术领域犯罪行为的立法和法律多样且多变；

(k) 盈利是在线商务平台的唯一目标。此外，此类平台还为利用技术隐藏用户身份和实施网络犯罪的软件和应用程序提供了肥沃的土壤；

(l) 利用信息技术实施的犯罪的规模及其潜在的跨境属性导致各国在应对此类犯罪方面缺乏协调和沟通；

(m) 将传统货币换为数字货币，使犯罪集体更容易隐藏其在互联网上的金融交易；

(n) 对信息技术和互联网的安全和最佳使用缺乏认识；

(o) 沙特阿拉伯需要参与有关打击滥用技术的国际立法；

(p) 需要通过提高社区对活跃在互联网上的犯罪团伙所用方法的认识来加强预防。

塞尔维亚

302. 塞尔维亚报告称，2005 年 7 月 25 日生效的《政府主管部门打击网络犯罪的组织和权限法》和 2010 年 1 月 1 日生效的《关于修正<政府主管部门打击网络犯罪的组织和权限法>的法律》对塞尔维亚高科技犯罪特别检察官办公室的组织和管辖权做出了明确规定。因此，特别检察官办公室对塞尔维亚领土上发生的涉及上述犯罪的案件拥有管辖权。

303. 塞尔维亚提及其立法和战略框架，其中包括：

(a) 《政府主管部门打击网络犯罪的组织和权限法》；

(b) 《关于确认<欧洲委员会网络犯罪公约>的法律》；

(c) 《关于确认<欧洲委员会网络犯罪公约>关于将通过计算机系统实施的种族主义或仇外行为定为刑事犯罪的附加议定书的法律》；

(d) 《关于批准<欧洲委员会保护儿童免遭性剥削和性虐待公约>的法律》；

(e) 《刑法典》；

(f) 《刑事诉讼法典》；

(g) 《电子通信法》；

(h) 《信息安全法》；

(i) 《2019-2023 年期间打击高科技犯罪战略》；

(j) 《塞尔维亚 2020 年前信息社会发展战略》；

(k) 《塞尔维亚共和国公共安全战略评估》。

304. 近期的国内立法改革强调了《欧洲委员会网络犯罪公约》及其《附加议定书》的重要性。

305. 2018 年 9 月，塞尔维亚政府通过了《国家打击网络犯罪战略》和随之制定的《行动计划》。此外，司法部还设立了负责修正《刑法典》和《刑事诉讼法典》的工作组。为此，检察官办公室和高科技犯罪特别检察官办公室的代表于 2019 年 3 月在欧洲联盟和欧洲委员会的 iPROCEEDS 联合项目内发起组成一个专家团。他们的任务是对国家立法进行深入的法律差距分析，评估国家立法是否符合《欧洲委员会网络犯罪公约》和关于攻击信息系统行为的第 2013/40/EU 号指令，并取代委员会第 2005/22 号框架决定及其他欧洲联盟和国际标准。分析的目的是要就修订各项法律提出建议，以期实现各项法律的全面统一。

306. 塞尔维亚指出，过去十五年的经验表明，国内以现行国际协定为基础的能力建设和专业化工作进展非常顺利，并且发挥了作用。关于这一领域内新的国际条约的讨论是否有帮助值得怀疑。

307. 在机构框架和行政能力方面，塞尔维亚列出以下有权在网络犯罪领域采取行动的机构：

(a) 高科技犯罪特别检察官办公室；

(b) 贝尔格莱德高等法院；

(c) 内政部打击和制止高科技犯罪司；

(d) 国家其他主管部门。

308. 在统计和分析方面，塞尔维亚报告称，2018 年，高科技犯罪特别检察官办公室登记册登记案件总数为 3,022 起，其中 322 起案件的犯罪人已知为成年人；有 1,306 起案件的犯罪人身份未知，其他 1,394 起案件属于其他刑事犯罪，与 2017 年相比，案件数量增加了 27.46%。

309. 因此，正如塞尔维亚进一步报告的那样，在刑事诉讼各个阶段适用各类程序性行动方面取得了重大积极进展，比如，对 324 名已知犯罪人提出了刑事指控，增长 28.57%；暂缓起诉案件增加了 85.71%，适用认罪协议的案件数量增加了 105%。这一显著增长的原因是报案人数和案件数量增加，特别检察官办公室的人力资源增加以及主管机关的能力建设活动增加。

310. 关于良好做法，塞尔维亚提到了以下由塞尔维亚网络犯罪主管部门参加并因实施《欧洲委员会网络犯罪公约》和在塞尔维亚法律中实施的国际合作条款而取得成功的案例：

(a) 2018 年 2 月，“影子网”行动。接管最大的犯罪论坛之一，即处理被盗信用卡信息的“In Fraud”。一名塞尔维亚公民被捕，并受到刑事指控；

(b) 2018 年 4 月，“断电”行动。接管世界上最大的分布式拒绝服务攻击的犯罪组织“Webstresser”。两名塞尔维亚公民被捕，并受到刑事指控。奥地利、加拿大、克罗地亚、德国、意大利、荷兰、塞尔维亚、西班牙、联合王国和美国以及中国香港的主管部门参与了这次行动。高科技犯罪特别检察官办公室针对两名嫌疑人展开调查，并且首次从其中一名嫌疑人处查扣加密货币；

(c) 2018 年 5 月，“黑暗霸主”行动。该行动针对的犯罪集团盗取个人数据并勒索其所有者的行为。

311. 塞尔维亚报告称，特别检察官办公室在 2018 年的国际合作尤为成功。该办公室参与了欧洲委员会网络犯罪公约跨境犯罪问题小组的工作以及与编写进一步建议和准则以适用该《公约》有关的活动。该办公室还参加了该小组关于起草《公约》第二附加议定书的工作。此外，该办公室还参与了欧洲委员会和欧洲联盟 GLACY+联合项目以及其他国际活动。2018 年，特别检察官办公室的代表参加了针对欧洲联盟的所谓“周边地区”的欧洲委员会 EAP III 项目；针对地中海地区北非、西非和亚洲国家的 Cyber@South 项目；以及将东南欧国家和土耳其包括在内的 iPROCEEDS@IPA 项目。欧洲网络犯罪问题司法网邀请特别检察官办公室出席其在海牙举行的会议。特别检察官办公室的代表还参加了全面研究网络犯罪问题专家组的工作。

新加坡

312. 新加坡提到它所面临的挑战，而这些挑战也是其他管辖区域所共有的。其中包括犯罪分子越来越老练，他们试图利用全球化以及新技术的出现和普及带来的更大便利，以实现其犯罪目的。

313. 新加坡报告称，在过去十年里，对网络空间的使用出现极大增长。这是由于技术价格下降和可得性增加而造成的，从而导致网络犯罪案件数量增加（新加坡《计算机滥用法》规定的罪行以及利用计算设备或网络作为工具实施传统犯罪的罪行）。在这方面，新加坡警察部队发现，国际诈骗者采用从黑客等高端方法到电话欺诈手段的信息和通信技术新手段，致使网络诈骗案件和受害者数量不断攀升。由于利用网络实施的犯罪在各个管辖区域内涉及面广，这类犯罪可在任何地方生根，并且更难侦查、根除和消除。新加坡已经在国家、区域和国际一级做出努力，以应对这一复杂的挑战，详见下文。

314. 关于在国家一级做出的努力，新加坡报告称，2016 年 7 月 20 日，内政部长和法律部长在亚太和日本信息安全大会上宣布了《新加坡国家网络犯罪问题行动计划》。随着世界各地网络犯罪活动的规模、复杂性和严重性继续增长，《国家网络犯罪问题行动计划》的愿景是确保新加坡拥有一个安全可靠的网络环境。该《计划》详细介绍了政府为打击网络犯罪采取的多管齐下的战略，包括：

(a) 教育公众在网络空间保持安全并增强其保持安全的能力；

(b) 提高政府打击网络犯罪的能力和实力；

(c) 强化立法和刑事司法框架；

(d) 加强伙伴关系和国际交往。

315. 关于在区域和国际一级做出的努力，新加坡指出，国际和区域组织以及多方利益攸关方伙伴关系在打击跨境网络犯罪的能力建设、促进信息、分享最新趋势和发展情况、最佳做法和国际合作方面发挥了有益的作用。

316. 主要区域平台包括东盟跨国犯罪问题部长级会议和跨国犯罪问题高官会议。作为东盟网络犯罪问题的自愿牵头人，新加坡发起了有关提高东盟成员国应对网络犯罪能力的新倡议，比如，在 2018 年 7 月主办了东盟+3 网络犯罪问题大会和第五届东盟网络犯罪问题高官圆桌会议。东盟还聚焦于努力提高检察官在起诉网络犯罪案件方面的知识和能力，并于 2018 年 9 月在新加坡举办了东盟网络犯罪问题检察官圆桌会议。以上都属于年度活动，也会在 2019 年举行。

317. 新加坡报告称其与国际刑警组织密切合作，以推动打击网络犯罪的区域和国际合作。新加坡被任命为国际刑警组织欧亚网络犯罪问题工作组副主席，任期为 2017 年至 2019 年。此外，新加坡还在国际刑警组织支持下发起了东盟网络犯罪问题服务处，该服务处于 2018 年 7 月在位于新加坡的国际刑警组织全球综合创新中心启动。该东盟服务处利用国际刑警组织的资源，推动以东盟为中心的打击网络犯罪的联合行动。新加坡还参加了 2017 年 2 月由国际刑警组织全球综合创新中心牵头的东盟网络浪潮行动。这次行动极其成功，涉及七个东盟国家和七个私营部门公司，查明有近 9,000 台服务器受损，数百个网站受到恶意软件感染。

318. 此外，新加坡还是国际刑警组织世界的支持伙伴，国际刑警组织世界是一个国际会议，每两年在新加坡举行一次会议，出席会议的公私部门在会议开展对话并创造合作机会，以应对未来的安全和警务挑战。这是一项独特的活动，为相关利益攸关方讨论全球面临的网络犯罪挑战以及专家介绍最新威胁、趋势和解决方案提供了一个宝贵的平台。

319. 新加坡还积极参与跨管辖区域的国际网络犯罪执法行动。新加坡参与了由美国联邦调查局、欧警署和德国联邦刑事警察局在2016年和2017年牵头的“雪崩行动”。这次行动旨在摧毁犯罪网络用来窃取银行账户信息和个人身份信息并进行洗钱活动的全球僵尸网络以及存在时间最长的恶意软件系统之一 Andromeda。新加坡还积极参加侧重于在执法领域提升全球合作和交流最佳做法的国际平台。这些平台包括：2018 年 7 月 2 日和 3 日在印度尼西亚举行的首届毒品和犯罪问题办公室网络犯罪问题国家圆桌讨论；2019 年 3 月 12 日至 14 日在新加坡举行的毒品和犯罪问题办公室加密货币专家讲习班；国际刑警组织全球网络犯罪问题专家组会议；以及国际刑警组织-欧警署网络犯罪问题会议。

320. 新加坡最后指出，会员国在打击为犯罪目的使用信息和通信技术行为方面面临的挑战是多方面的。显然，进一步讨论以及加强会员国和包括联合国在内的相关利益攸关方在区域和国际层面的国际合作与协作将有利于网络犯罪问题的解决。新加坡致力于打击网络犯罪的国际和区域合作，并且期待在可能的情况下参与能力建设活动。此外，新加坡还将继续支持为应对这些挑战而开展的合作和信息共享。

斯洛伐克

321. 斯洛伐克报告称，它十分重视打击网络犯罪，并认为打击网络犯罪是一项非常重要的挑战。为了有效地解决网络犯罪问题，必须满足两个主要方面的要求：法律和技术。首先，必须制定适当的国内立法。实质性刑事法律条款必须辅之以适当的程序性条款。斯洛伐克认为，必须确保扩大有关搜查房屋以及交出、查扣或没收物品等传统程序性条款的适用范围以涵盖被扣押媒介中包含的数据。因此，关于计算机数据的搜查，需要制定额外的程序条款，以确保可以与搜查和查扣有形数据载体同样有效的方式合法获取计算机数据。基于此，国内法律必须包含允许国家主管机关搜查和查扣计算机所存储数据的条款。必须确保所有国家都拥有适当的条款以防止犯罪行为人隐藏起来以逃避司法。

322. 斯洛伐克认为，《欧洲委员会网络犯罪公约》是一个包含广泛程序性权力的完美范例，除其他外，该《公约》对关于搜查和扣押的条款以及关于计算机数据和数据保全的命令做出了规定。斯洛伐克于2008年批准了该《公约》，并且认为它是载有适当实质性和程序性条款并能够开展有效国际合作的最佳国际标准。有鉴于此，对斯洛伐克来说，成功实施《欧洲委员会网络犯罪公约》所载程序性权力以及明确的政治意愿是制定有力的证据获取框架的关键因素。

323. 此外，斯洛伐克还认为，对发布出示令问题作出规定的《欧洲委员会网络犯罪公约》第 18 条第 1 款(a)项的重要性确实经受住了时间的考验。关键要素不是数据所在的位置，而是数据控制者或持有者在特定领土的存在。这种办法为大多数情况提供了解决方案，即使在云计算时代也是如此。基于上述情况，斯洛伐克认为没有必要制定一项新的网络犯罪问题国际文书，并鼓励尚未加入《欧洲委员会网络犯罪公约》的国家加入该文书。

324. 斯洛伐克进一步指出，几乎每一项刑事犯罪都可能产生电子证据。《欧洲委员会网络犯罪公约》允许收集所有类型犯罪的电子证据，从而使该文书愈发重要。因此，每位法官或检察官都应当知道如何使用现有手段来获得电子证据。在

这方面，斯洛伐克认为国家和国际一级的教育活动和能力建设方案至关重要。斯洛伐克认为，能力建设方案必须具有针对性，如果可能，须避免重复。

325. 除了法律方面，斯洛伐克还提到了技术方面。各国应当牢记，对网络犯罪和利用网络实施的犯罪进行顺利调查的一个关键因素在于不同种类的专业化（关于网络犯罪的检察官、法官地方网络和关于网络犯罪的专门司法机关），也在于对执法和司法机关进行定期培训，从而确保正确运用各种程序性权力并对当前动态作出反应。在各国国内和国际一级建立联系和交流最佳做法是必要的。

326. 为了确保专业化和不断更新专门知识，斯洛伐克在警察部队主席团内设立了一个专门的打击计算机犯罪局。该局有助于更加有效地打击计算机犯罪和通过互联网实施的罪行。该局目前负责的主要领域包括：对信息系统的网络攻击、网上儿童性剥削、非现金支付欺诈以及非法网上内容（包括恐怖主义内容）。它的任务包括查找和监测网络犯罪（包括互联网秘密行动）。它还在检察官需要技术援助时配合其开展工作。合作效果很好。该部还与国际网络犯罪警察界以及斯洛伐克境内和境外的私营部门特别是互联网服务提供商开展对话，因为个人数据往往由私营实体持有或控制，因此，有必要讨论合作的复杂性和挑战。

327. 此外，斯洛伐克还在 2017 年成立了国家打击网络犯罪检察官网络。其主要任务是向网络成员及其他检察官提供与网络犯罪有关的实用信息及分享经验，涉及国内案例及国际合作案例。

328. 在国家层面，斯洛伐克设立了网络犯罪问题多学科专家组。该专家组由来自所有重要国家机关和私营部门的专家组成。除其他外，它还讨论如何修订与为了刑事诉讼目的而披露数据有关的法律问题，以便不需要法院签发命令（在斯洛伐克，调查电话号码或 IP 地址的用户需要法院签署命令）。因此，斯洛伐克认为，在国内和国际层面建立专门网络以便将处理网络犯罪问题的从业人员聚集到一起是有好处的。

329. 斯洛伐克强调，它致力于打击网络犯罪。由于网络犯罪具有全球性，斯洛伐克确认，它非常高兴有可能参加全面研究网络犯罪问题专家组。在此专家组框架内与来自世界各地的专家分享最佳做法和交流观点非常有帮助，专家组至少应在 2021 年之前继续作为联合国一级关于网络犯罪专题的主要进程。

斯洛文尼亚

330. 斯洛文尼亚承认，随着信息技术的迅速发展，新的服务、装备和设备不断进入市场，与此同时，犯罪分子的作案手法也在不断翻新。这就需要执法部门迅速和充分适应这种情况，只有通过与私营部门和研究实体开展有效的密切合作才能确保做到这一点。开展此类合作必然需要安全和快速交流信息、专门知识、调查手段和方法，并且需要对人员进行持续培训。鉴于这种趋势，预计使用现代、数字和虚拟信息或其他技术实施的刑事犯罪数量将会有所增加。

331. 斯洛文尼亚警方注意到，在网络空间，刑事犯罪的行为人在技术方面越来越熟练，并且组织严密；他们在世界各地实施犯罪活动，而留下的能够容易识别其身份的痕迹和证据较少。所有犯罪活动的发生时间都很快，受害者数量不断增加，而恢复正常需要更长的时间。大多数情况下，留下的痕迹仅以数字形式出

现，而且往往分散在若干个国家或大陆，对刑事调查的持续时间和成功造成不利影响。斯洛文尼亚报告的另一个挑战是在每次调查中需要调查和分析的数据量不断增加，而且事实上越来越多的电子设备制造商默认使用强大的数据加密手段。这为犯罪分子提供了很大的酌处空间，使侦查和预防犯罪变得更加困难。

332. 由于技术成果的开发和利用，只有在形成新的预防和限制风险的做法、开发新的方法、工具和机制方面加强合作和互惠，以及只有在预防行动层面加强互惠行动和团结，才能战胜在国际环境方面面临的挑战。证据和行为人的行动分散在世界各地，需要对此采取新的调查形式，需要有更好的立法以及得到改进的资质和设备。

南非

333. 谈到与使用信息和通信技术的现有法律和刑法手段有关的挑战，南非报告称，它已经制定用于打击网络犯罪行为的立法，包括《打击网络犯罪议案》（即将成为议会法案）、《刑事诉讼法》、《电子通信和交易法》、《刑事事项国际合作法》和《个人信息保护法》。此外，南非指出，在一些关键性问题和概念上缺乏国际共识对打击为犯罪目的使用信息和通信技术行为构成挑战，其中包括网络威胁的性质和规模、正式框架的程序和结果的公正性以及将具体行为定为网络犯罪。这些挑战超出了定义要素的范畴，而定义要素各有很大的区别。

334. 南非还提到各国在打击为犯罪目的使用信息和通信技术行为方面的协调与合作问题。尽管有司法协助、指定联络点、电子通信服务提供商和金融机构承担的义务以及各种服务提供商快速披露流量数据等很多现有机制被用于促进协调与合作，但在应对网络犯罪方面仍然存在挑战。以下被确定为具有重要意义的挑战：司法协助过程漫长；不同的机构有不同的任务授权，导致中央协调变得困难；以及协调机制和拟议措施的实施没有得到各利益攸关方的充分支持。虽然现有区域文书可能在促进公约缔约方之间合作以应对网络威胁方面发挥作用，但最大挑战在于这些文书可能无法在全球范围内有效打击网络犯罪，因为非《公约》缔约方的国家可能不会合作。没有普遍商定的网络犯罪定义构成挑战，因此，每个国家都制定了自己的定义，导致在涉及包括引渡和分享电子证据在内的司法协助或国际合作时面临挑战。为了有效执行关于网络犯罪的法律，特别是在需要与其他国家合作时，必须确保一定程度的法律统一，这就需要就网络犯罪的定义达成一致。虽然存在各种具有约束力或没有约束力的旨在应对网络犯罪问题的区域文书，但许多国家可能因为其政治体制、国际议程和社会经济环境原因而不愿意批准任何现有区域文书。

335. 在技术援助方面，南非指出，虽然存在双边和多边协定（例如，《打击有组织犯罪公约》关于司法协助、引渡、移交被判刑囚犯和资产没收的条款），但似乎在实用性方面被一些区域和大陆协定所取代。在大多数情况下，与网络犯罪问题有关的国际合作有限，并且没有保全证据、迅速提供流量数据或确保提供证据等必要程序。

336. 南非认为，各国国内法律仍然各不相同带来的其他挑战包括对网络犯罪的描述不同；与国际合作有关的程序不同；在证据可被法院采信之前必须遵守的国家间正式程序；隐私法；等等。

337. 南非认为，各国缺少具有协调权力的国家机构来协调互助请求，这妨碍了司法协助的成效。旨在应对网络犯罪的各种区域文书导致国家间的合作碎片化和相互独立，并且在确保充分的国际合作方面不成功。在联合国一级缺少处理网络犯罪事项国际合作问题的公认文书是导致这一领域内国际合作低效的一个重要因素。

338. 南非坚信，应当加强毒品和犯罪问题办公室特别是预防犯罪和刑事司法委员会在提供能力建设方面的作用。各国主管部门缺少专业培训资金的事实使它们无法对复杂的网络犯罪案件开展有效调查是个问题。同样，由于私营部门对人才的需求，留住经验丰富和经过培训的人才也很困难。执法培训机构普遍缺乏基础和中级培训方案，此外，有经验的调查人员因工作量大很少有机会参加高级培训课程或讲习班。即使抱有最好的意图并且制定了拟议措施，预算和能力限制也会使执行拟议措施变得困难，而且可供利用的能力和资源往往仅限于某个机构的任务授权，未必能够用于协助其他机构。此外，在网络犯罪领域，没有针对相关利益攸关方之间合作的正式框架和准则。

西班牙

339. 西班牙报告称，由越来越多地使用信息和通信技术导致的网络犯罪是所有国家面临的主要威胁和最重要的挑战之一，这也是跨国有组织犯罪集团采用的犯罪方法多样化的结果。犯罪分子利用通信平台以及新的信息和通信技术创造新的非法商业模式，例如，利用暗网实施其他犯罪（比如贩运枪支和假币），使用复杂的恶意软件（比如勒索软件）和银行基础设施管控者以及提供非法服务的所谓“个人犯罪企业家”。所有这些都对安全人员和整个社会构成挑战。

340. 互联网接入的普及和快速增长以及能够连接互联网的设备数量的增加将导致网络犯罪的潜在受害者数量增加。同样，考虑到发展中国家（主要在非洲）所占人口比例以及这些国家的互联网用户数量增长的估计数不断增长，预测利用互联网实施犯罪特别是经济犯罪的数量将会显著增加不是一件难事。然而，就像犯罪分子学习如何利用新技术开发新的作案手法一样，警察部门也可利用技术创新和采取新的措施，调查和打击有组织严重犯罪构成的威胁。

341. 西班牙认为，将有关在互联网上开展秘密调查的要求纳入国家法律是打击利用信息和通信技术实施有组织和严重犯罪的一项关键工具。在逐步使用无人机、专用软件、云服务和快速访问社交网络等新技术方面也是如此。

342. 在西班牙，打击通过互联网以及一般通过信息和通信技术策划和实施犯罪的措施是 2013 年 12 月发布并且目前正在更新的《国家安全战略》的重要组成部分。因此，打击网络犯罪被视为采取综合模式确保网络空间使用安全性的更大目标的一部分。其中包括公共行政部门、私营部门和公民之间的协调与合作，与此同时，将国际倡议纳入国内和国际法律秩序。这种做法已通过不同方式得以实现。

343. 首先，在立法改革方面，受欧洲条例（第 2013/40 号指令、第 2011/93 号指令和第 2008/919/JAI 号框架决定等）以及《欧洲委员会网络犯罪公约》和《欧洲委员会保护儿童免遭性剥削和性虐待公约》的启发，2015 年第 1/2015 和 2/2015 号组织法对《西班牙刑法典》进行重大修订。这些文书含有新型犯罪的定义，致使对《刑法典》中关于计算机攻击、对未成年人的性骚扰、儿童色情制品、知识产

权、仇恨犯罪、计算机欺诈和恐怖主义犯罪等定义的相关条款进行了广泛修订。此外，受《欧洲委员会网络犯罪公约》启发，西班牙还在 2015 年通过第 13/2015 号组织法对《刑事诉讼法》进行了一次重大修订。此次修订对与数据的登记、存储和保全有关的重要技术措施做出了规定。为了便于解释这些立法方面的发展情况，国家总检察长办公室发布了相关通告。

344. 其次，在组织措施方面，二十多年以来，西班牙所有国家和自治区警察部队都设有专门的单位，由技术研究领域内高素质人才组成，并且拥有有效打击为犯罪目的使用信息和通信技术行为的知识和经验。这项专门知识使警察部门能够利用大数据等新技术以及可以嵌入服装、珠宝和鞋子等产品的网络设备来调查犯罪和确定嫌疑人身份。

345. 西班牙检察官办公室还设立了负责网络犯罪领域的专门机构。自 2011 年以来，专门负责起诉网络犯罪的全国检察官网络在全国 50 个省会城市和其他一些选定城市部署了大约150名检察官。检察官办公室和警方的专门单位与负责网络安全的其他机构保持持续联系，以便确保充分协调以及所有人都能安全地使用网络空间。这些机构包括西班牙数据保护局、国家关键基础设施保护中心、国家网络安全研究所、国家密码学中心和网络联合防御司令部以及包括银行实体或负责电信和其他基本服务的机构在内的私营部门组织和实体。

346. 西班牙认为，必须继续支持对打击网络犯罪专业单位的培训，并增加其人力和物力资源。近年来，针对研究人员和法律人员（主要是法官和检察官）的培训也受到了关注，并且体现为两个层面：

(a) 为参与打击犯罪的所有专业人员提供关于基本和必要知识的一般性准备；

(b) 为专门处理网络犯罪的单位或团体提供专业培训。

347. 西班牙表示，在应对各国共同面临的网络犯罪挑战方面，开展国际合作非常重要。西班牙参与国际合作努力的一些例子包括：积极参加根据《欧洲委员会网络犯罪公约》第 35 条设立的“每周 7 天，每天 24 小时”网络；欧洲打击网络犯罪司法网络；以及欧洲知识产权专业检察官网络。同样，西班牙检察官办公室还促进并参加了伊比利亚美洲专业检察官网络。

348. 西班牙报告称，它是欧洲委员会网络犯罪公约网络犯罪公约委员会和编制《公约》第二附加议定书工作组的积极成员，该议定书旨在加强与私营部门经营者、提供商和实体的国际合作与协作。西班牙参加了与欧洲和拉丁美洲国家共同开展的众多跨国调查，并采用了联合调查组等高级合作手段。它还参加了在其他国家进行的培训，包括作为培训员。

斯里兰卡

349. 斯里兰卡强调，它一直积极参与全面研究网络犯罪问题专家组，该专家组最近审查了自 2013 年 2 月以来的网络犯罪问题全面研究报告草案的第 5 和第 6 章。专家组的下一次会议将重点审查最后两章，即第 7 和第 8 章（国际合作和预防）。

350. 斯里兰卡希望澄清大会第 73/187 号决议寻求获得的信息与毒品和犯罪问题办公室目前就网络犯罪问题全面研究报告草案开展的工作之间的联系，以及是否在重复全面研究网络犯罪问题专家组的工作。

351. 关于网络犯罪的国内立法，斯里兰卡报告称，2007 年第 24 号《计算机犯罪法》是打击网络犯罪方面的主要立法工具。此外，2006 年第 30 号《支付设备欺诈法》专门涉及到关于拥有或使用未经授权或伪造的支付设备问题。

352. 斯里兰卡于 2015 年成为《欧洲委员会网络犯罪公约》的缔约国。这表明它坚定致力于根据现有关于打击网络犯罪的最佳国际标准来统一和完善国家法律。斯里兰卡还致力于改进调查手段和加强刑事司法人员的能力，以便采用更加有效的执法手段。

353. 虽然《计算机犯罪法》第 3 至第 10 节体现的实质性法律条款是以《欧洲委员会网络犯罪公约》第 2 至第 8 条作为基础，但《公约》第 9 条则在 1995 年第 22 号《刑法典（修正）法》第 286A 节当中得到部分体现。2003 年第 36 号《知识产权法》涉及到《欧洲委员会网络犯罪公约》第 10 条所涵盖的罪行。

354. 为了应对不断变化的网络犯罪挑战，斯里兰卡已经着手审查网上儿童安全领域内的国家刑事司法措施。因此，斯里兰卡近期批准了《淫秽出版物法令修正案》，以全面处理与儿童色情制品相关的罪行。该修正案将引入一个题为“通过利用计算机系统传播儿童色情制品”的新章节。

355. 在与网络犯罪和电子证据有关的执法措施方面，《计算机犯罪法》第二部分所载程序性条款对窃听、实时收集用户基本信息和流量数据以及提出保全请求问题做出了规定。这些条款须遵守《欧洲委员会网络犯罪公约》第 15 条规定的保障措施。[9]

356. 根据该法第 18 节，执法机构要想获得服务提供商拥有的用户基本信息需要地方法官签发令状。对通信进行窃听也必须满足类似要求。该法第 19 节规定的数据保全命令要求计算机或信息系统的任何负责人员按执法机构的要求保全数据。但是，保全期间仅限七天以内。只有通过法院发布命令才可延长保全期限。

357. 对这些程序性措施的司法监督防止执法机构向服务提供商提出不必要和任意的请求，同时确保它们协助执法人员有效打击犯罪。国家立法中的这些保障措施未对刑事调查的效率或成效产生不利影响。另一个方面，它们使受害者和企业（特别是银行和金融部门组织）对报告网络犯罪事件更有信心，也使电信服务提供商对配合执法机构有信心。这可以说是发展中国家的最佳做法。

358. 在警察局设立了一个专门的网络犯罪调查股，并设有两个省级分支机构。该调查股发挥《欧洲委员会网络犯罪公约》中所述“每周 7 天，每天 24 小时”联络点的职能。最近，该调查股进行了一次升级，由于国家官员获得了通过下述能力建设措施提供的专门知识，已有 750 多起案件顺利调查完毕。

359. 斯里兰卡强调，从外国服务提供商处获得电子证据对调查和起诉网络犯罪至关重要。由于证据位于不同管辖区域，因此，最重要的一点是需要采取比较有效的调查方法，并辅之以有效的国际合作措施。2002 年第 25 号《刑事事项互助法》对在刑事司法事项方面的国际合作做出了规定。2018 年该法案已在《计算机犯罪

[9] 根据《计算机犯罪法》，采取搜查和扣押计算机或窃听通信等侵入性调查措施须获得地方法官签发的令状（第 18 节）。《斯里兰卡宪法》第三章对若干基本权利做出了规定和保障。斯里兰卡还是《经济、社会及文化权利国际公约》、《公民权利和政治权利国际公约》、《儿童权利公约》以及《禁止酷刑和其他残忍、不人道或有辱人格的待遇或处罚公约》等多项国际人权条约的缔约国。

法》得到引用，2018 年的第 24 号法对 2002 年第 25 号法进行了修正，其中具有《欧洲委员会网络犯罪公约》的一些特点。

360. 在能力建设措施方面，一系列涉及司法部门、检察部门和警察部门的网络犯罪和电子证据方案对加强执法和调查方法进行培训。这些方案是在获得欧洲联盟和欧洲委员会支持的一个项目中进行的。这些能力建设措施增强了国家执法人员的能力，使他们能够在良好做法和经验以及从《欧洲委员会网络犯罪公约》其他缔约国得到的经验教训的基础上采取更加有效的标准作业程序。

361. 斯里兰卡报告称，政府在 2018 年 10 月通过了一项全面的网络安全战略。因此，斯里兰卡目前正在起草网络安全和数据保护立法。这些举措由数字基础设施和信息技术部牵头，并且得到计算机应急响应小组、信息和通信技术局、斯里兰卡中央银行和其他关键利益攸关方的支持。数字基础设施和信息技术部已让私营部门参与这些工作，政府将采取包容性办法，在审查新的立法草案时征求关键利益攸关方的意见。

瑞士

362. 瑞士指出，信息和通信技术的发展为个人、公司、企业和商务提供了前所未有的机会，同时也带来了挑战，特别是在刑事司法乃至法治领域。虽然严格意义上的网络犯罪（即通过计算机系统实施的犯罪，包括在计算机系统上留下电子证据的犯罪）正在发展演变，虽然这些犯罪的证据越来越多地存储在境外管辖区域的服务器上，而且可能是多个不断变化或未知的管辖区域，例如存储在云中，但执法部门受到领土边界的限制，而且必须尊重国家主权。

363. 瑞士关切地注意到司法协助在获取不稳定的电子证据方面的成效有限、数据本地化（知识）损失的情况以及各国在没有国际规则的情况下越来越依赖单边跨境获取数据的事实。

364. 作为《欧洲委员会网络犯罪公约》的缔约国，瑞士强调了该公约的重要性。对瑞士而言，《公约》通过统一法律、建立程序和指定联络点，极大地便利了合作。有必要在该公约的基础上促进和加强国际合作。

365. 服务提供商是否在某个缔约国领土内充分存在或提供服务从而受该国管辖的问题将在今后几年内至关重要。例如，这个问题不仅在刑法方面，而且在税收和版权法方面具有相关性。

366. 瑞士强调，各国必须始终遵守国际法特别是人权法规定的义务，包括在规范网络空间以及在对网络犯罪进行刑事定罪、调查和起诉时。必须牢记和遵守数据保护和其他法治保障原则，特别是在研究和讨论国际合作和跨国调查的新方式时。

阿拉伯叙利亚共和国

367. 阿拉伯叙利亚共和国强调，网络犯罪的威胁日益严重，犯罪网络和恐怖主义集团利用信息和通信技术来实现其犯罪和恐怖主义目的的情况也在增加。这影响到各国及其基础设施和机构的稳定，特别是影响到社会和文化结构以及经济发展

和发展进步。国家间的数字鸿沟的扩大不可避免地损害许多国家预防、起诉和打击此类犯罪的能力。

368. 阿拉伯叙利亚共和国称，毫无疑问，数字世界的高犯罪率和犯罪数量的增长对世界各地恐怖主义犯罪蔓延产生了重大影响，特别是伊拉克和阿拉伯叙利亚共和国境内恐怖主义组织实施的犯罪。数字空间不受控制和无法追踪的特点为恐怖分子实施各种形式的犯罪提供了便利，包括谋杀、贩运人口、偷运文化财产、洗劫宗教古迹和宗教场所以及利用互联网虐待、绑架和招募儿童参加敌对行动和恐怖主义、种族主义行为和煽动仇恨、基于教派、族裔或教义的冲突，以及其他严重违反相关国际法、公约和决议且需要国际社会做出严肃应对的行为。

369. 阿拉伯叙利亚共和国为应对网络犯罪和恐怖主义集团利用数字空间实施最令人发指的跨国恐怖主义犯罪的威胁采取了很多措施，包括通过加强法律框架的方式。在这方面，政府发布了关于打击网络犯罪的 2012 年第 17 号法令，为了提高打击涉及利用信息和通信技术的传统犯罪的成效颁布了《数字刑法》。2018 年第 9 号法律对设立负责信息和通信犯罪的公诉机构和专门法庭做出规定，其目的是提高人们对这种犯罪的严重性的认识以及在国内建设能力和保护受害者。

370.在立法的实际适用中，主管部门面临着许多问题和挑战，认为这类犯罪没有性质限制，从而使执法部门开展刑事调查工作变得更加复杂。这些挑战包括面对发达国家垄断全球互联网问题；以及在与阿拉伯叙利亚共和国有关部门分享犯罪分子通过互联网实施犯罪活动的证据和信息方面使工作政治化以及缺乏合作。此外，阿拉伯叙利亚共和国还报告说，美国和其他国家以及垄断通信技术的欧洲联盟对它实施封锁和单方面的非法胁迫措施，限制了叙利亚有关部门获得打击这些犯罪活动所需技术和工具的机会。

371. 对于阿拉伯叙利亚共和国而言，目前在国际和区域一级使用的刑法法律文书不足以打击在犯罪和恐怖主义行动中非法使用信息和通信技术行为。目前，除了《欧洲委员会网络犯罪公约》外，没有这方面的国际公约，而《欧洲委员会网络犯罪公约》未涉及在恐怖主义行为中使用信息技术问题。

372. 鉴于上述情况，且为了加强打击为犯罪目的使用信息和通信技术行为，阿拉伯叙利亚共和国提出以下建议：

(a) 各国严格遵守其国际义务，严格执行安全理事会有关反恐决议；

(b) 促进有效开展区域和国际合作，包括通过交换信息的方式，并为交换信息和数字证据制定一致的灵活机制；

(c) 会员国就如何审查打击利用信息和通信技术实施的犯罪的解决办法达成初步协定，以便在纽约设立一个不限成员名额的联合国工作组，以确保所有相关国家都能参与这一主题的讨论；

(d) 就这一领域内的国际合作问题制定一项具有约束力且符合会员国利益的国际法律文书，同时考虑到现有刑法法律文书不足以打击信息和通信技术犯罪；

(e) 在事实已经证明无法通过一视同仁地取消针对所有国家的技术和工具转让限制的方式充分防止滥用信息和通信技术带来的后果之后，通过各国放弃其对电子技术及其工具的垄断的方式，消除“数字鸿沟”；

(f) 通过合作和所有国家的积极参与，加强预防和保护措施；

(g) 加快对国际合作请求的回应，特别是为获取和维护数字证据之目的提出的请求，并为这种回应设定时限；

(h) 考虑建立一个全球在线互动平台，让每个会员国的有关国家主管部门参与其中。该平台将促进关于跨国网络犯罪案件的情报共享，并将提供关于安全使用在线数据库的指导方针。此外，还将提供专门方案，以帮助预防网络犯罪和防止加入网络犯罪，以及提供其他指导方针，以确保根据这类犯罪所使用技术的复杂性迅速作出反应；

(i) 建设国家能力和提供技术援助，以提高主管部门的技能，从而有效应对网络犯罪挑战和与数字证据有关的挑战，包括支持各国努力发展和部署互联网基础设施，以提高应对网络犯罪能力，并支持对技术问题和记录保存数字化工作开展培训和提高认识活动；

(j) 拥有必要设备，以获取数字证据，支持培训充足数量的在网络犯罪核查技术和提取相关数字证据方面接受过训练的合格数字调查员；

(k) 就数字空间使用问题制定具有约束力的监管标准，同时考虑到兼顾互联网自由、隐私和国家安全，并为应对滥用数字空间现象制定框架。例如，监控发现，设置比特币兑换网站可能被用于洗钱和资助恐怖主义，社交网络平台可能被用于煽动犯罪；

(l) 加强有关政府机构与互联网服务提供商、蜂窝移动网络等私营部门各公司之间的伙伴关系，根据法律和司法管控规定按要求提供所存储的信息，以完成对信息犯罪的调查和取证。

塔吉克斯坦

373. 塔吉克斯坦指出，信息和通信技术的传播和信息基础设施的发展促成了信息社会的建立。世界实践表明，信息时代扩大了政治暴力机制，增加了说服、操纵意识和其他影响公众意识的宣传方式。

374. 塔吉克斯坦提出了以下建议：

(a) 应鼓励各国政府为其执法人员提供充分的信息和专业培训，并向他们提供充裕资源，以便有效调查与使用互联网及其他信息和通信技术有关的犯罪；

(b) 各国政府应鼓励其执法机关掌握有助于调查网络犯罪并使其能够顺利进行刑事调查的专门技能；

(c) 各国政府必须采取集体行动，确保有效的机构间和区域间信息交流，消除在几个国家调查网络犯罪时遇到的障碍，并对立法、实践和程序做出必要修改，以便加快信息交流、处理各种信息源提出的请求和转让数字证据；

(d) 有必要定期组织具体课程，并确保为执法机关工作人员在打击网络犯罪以及利用互联网和其他信息和通信技术方面进行适当的专业培训；

(e) 认为有必要就合作打击与使用信息和通信技术有关的犯罪问题制定并通过一项符合所有会员国利益的具有普遍性的联合国公约。

泰国

375. 泰国报告说，国内遇到的典型网络犯罪罪行包括黑客攻击、互联网欺诈、入侵、网络骚扰、在线身份盗窃、在线虐待儿童、侮辱性内容、恶意代码和勒索软件攻击。犯罪分子总是通过寻找网络技术漏洞的方式来隐藏其身份，包括采用在区块链系统中使用解密货币（加密货币）进行洗钱等创新办法。

376. 泰国还报告说，在大多数网络犯罪案件中，都会遇到难以收集数字证据的问题。这是因为起诉网络犯罪的重要证据存储在脸书、Line、Instagram、微信和 WhatsApp 等互联网服务提供商和社交媒体服务提供商那里，而这些服务提供商通常在外国注册，无法根据《泰国计算机相关犯罪法》迫使它们提供协助与配合。因此，执法机构可能需要通过司法协助条约的正式渠道获取此类证据。这个过程需要很长的时间，并且在实践中可能会变得困难。通过非正式合作渠道获得的信息虽然有帮助，但可能不适合作为法庭证据。

377. 此外，加密等一些新技术可以阻止访问数据。未经所有者同意，一些“智能”移动电话无法解锁，从而阻止访问其操作系统。此外，由于成本高昂，导致缺乏数字法证工具和软件，这是计算机法证鉴定员面临的共同问题；免费工具和开源软件在计算机法证鉴定方面的能力有限。

378. 泰国还报告说，执法机构可能对数字证据和现代金融银行技术缺乏了解。许多官员可能缺乏阅读财务报表或寻找间接证据的相关经验，包括借助现代网络侦查技术。因此，需要对检察官和其他执法人员进行网络犯罪问题培训，并建立一个分享知识和最佳做法的平台。

379. 尽管《计算机相关犯罪法》规定服务提供商有责任保存流量数据并向主管部门提供所要求的信息，但一些服务提供商并非始终完全遵守这一规定。由于请求数量巨大，有些需要花费时间来提交所请求的数据。一些服务提供商不愿披露数据，因为它们担心泄露客户隐私。

380. 泰国强调，信息和通信技术的使用越来越普遍，随之而来的是更多设备接入互联网服务，这使国家和企业的重要基础设施面临风险。虽然这些设备在技术上可能受到影响和破坏，但信息系统必须保持稳定和绝对安全。保护这一系统需要所有相关机构和所有利益攸关方合作。此外，很难明确识别服务提供商收到的请求的意图。

381. 在泰国，第 B.E.2550 号《计算机相关犯罪法》（2007 年）是起诉网络犯罪的一部重要法律。与《刑法》、《打击贩运人口法》、《麻醉品法》、《版权法》和《防止和禁止参与跨国犯罪组织法》等对网络犯罪相关刑事罪行做出规定的其他法律一起使用。相关法律的颁布必须同时出台包括执法人员在内的工作人员能力建设方案，并建立有效的协调机制。迫切需要提高数字素养和利益攸关方的认识和了解，让他们为实施这些法律做好准备。

382. 在保护包括儿童在内的个人权利方面，泰国报告说，参与贩运人口、网络欺凌和包括诈骗在内的互联网欺诈的人员利用新技术直接与个人沟通，并以犯罪为目的获取他们的信任。与此同时，极端和消极的意识形态也在互联网上日益传播。主要挑战包括：

(a) 有效实施现有法律法规；

(b) 执法人员、金融业者和利益攸关方等有关机构之间的协调；

(c) 多利益攸关方参与促进和保护个人权利。

383. 泰国认为，对相关罪行的调查必须考虑到受害者的想法和情况，因此，需要针对具体情况采取基于人权的办法。在那些处境脆弱的人员中，儿童尤其成为网络欺凌、网络骚扰、网络游戏、色情短信、儿童性虐待材料、网上诱拐和性勒索的目标。应该特别关注脸书、Instagram 和推特等社交媒体网站。

384. 泰国最后认为，任何国家都无法单独预防和制止网络犯罪。因此，会员国之间开展国际合作和对话非常重要。全面研究网络犯罪问题专家组是负责处理这一问题的唯一平台，泰国参加了该专家组。泰国希望该专家组的任务授权和工作将延长到 2021 年以后。

土耳其

385. 土耳其强调，信息和通信技术在涉及公共和私营部门、关键基础设施和个人的广泛网络中得到使用，并在国内和国际上得到广泛使用。因此，信息和通信技术在可持续增长和发展方面发挥着重要作用。然而，技术用得越多，社会就越依赖它，并且技术所带来的风险影响就越大。个人、公司、关键基础设施和国家因网络事件而遭遇一些严重难题。信息和通信系统的安全漏洞可能导致这些系统中断服务或被利用，或可能最终导致失去生命、大规模经济损失、扰乱公共秩序和（或）危及国家安全。另一方面，网络空间为匿名和否认信息和通信技术攻击等提供了便利。信息系统的持续和高级网络攻击的资助者和组织者难以被发现。这种情况使打击网络威胁和攻击者变得困难。

386. 在此背景下，不仅包括公共和私营部门、大学、非政府组织和个人在内的利益攸关方在国家一级开展合作至关重要，而且国际合作和信息共享也至关重要。《国家网络安全战略和行动计划》的主要战略目标之一是打击网络犯罪。在这方面，土耳其支持在打击网络犯罪概念范围内开展国际活动并为之做出贡献。

387.土耳其于 2010 年签署《欧洲委员会网络犯罪公约》。2014 年，通过颁布《关于批准网络犯罪公约的法律》，将《公约》纳入国内法。此外，与网络安全有关的问题也受《土耳其刑法》管辖。

388. 土耳其指出，随着互联网以及日益先进的信息和通信技术的使用越来越广泛，网络空间已经成为所有事物的中心，吸引很多类型敌对行为体。由于互联网的分层结构和使用代理服务器访问互联网，识别网络犯罪分子的身份变得越来越困难。对这种技术的恶意利用为实施网络犯罪提供了必要的手段，也为恐怖主义集团提供了便利的通信媒介。非法组织利用信息和通信技术进行宣扬和传播、收集信息、筹集资金、招募新成员、策划有组织活动、共享信息、谋划或协调恐怖行动。恐怖集团往往利用能够提供加密渠道的应用程序和工具来进行通信或策划或协调其敌意行为。这种情况使执法部门很难查明恐怖分子的身份和活动。

389. 土耳其认为，加强全球一级信息安全和发展国际社会安全文化是每个利益攸关方面临的重要问题。加强国际立法和加强双边或多边国际协定也很重要。在这方面，土耳其认为，制定有助于防止犯罪分子利用信息和通信技术并加强在此领域内国际合作机制的措施将有助于查明恐怖分子的身份和挫败其活动。

390. 另一方面，在互联网上发布非法内容可被视为一个严重问题，对确保网络安全构成挑战。恐怖组织对世界各地的人道主义共同价值观和生存权的恶意攻击以及将通过互联网传播内容作为宣传工具突出了防止利用互联网被用于非法目的的重要性。在此背景下，取缔互联网上的非法内容不仅应被视为各国的责任，也应被视为那些作为互联网最大行为体的全球互联网公司的责任。因此，互联网行为体应与有关国家合作，认真防范所有犯罪组织在其平台上实施的犯罪活动。

391. 土耳其认为，考虑到所有恐怖集团都利用网络空间从事不同动机的犯罪活动，全球互联网中介商迫切需要尽快敏感地回应有关请求，删除与这些恐怖集团有关的非法内容。坚定和持续执行关于删除有关内容的决定非常重要；否则，恐怖集团恶意使用互联网可能会造成不可逆转的伤害。在这方面，相关内容和主机托管服务提供商的配合对于确保充分合作至关重要。全球服务提供商根据国内和国际立法和司法命令执行内容删除请求将大大有助于打击网上平台上的非法内容。

大不列颠及北爱尔兰联合王国

392. 联合王国表示，“为犯罪目的使用信息和通信技术”的概念将被解释为其应对目的不言而喻（且范围比网络犯罪更广），尽管该问题的宽泛框架并未给出直截了当的答案。由于促成利用信息和通信技术实施犯罪的因素各不相同，导致在应对此类犯罪方面面临极其复杂和多样的挑战。这些因素包括犯罪动机、受害者的相应概况和（或）脆弱性、犯罪者采用的方法和技术手段，包括掩盖其活动的具体方法，以及反映以上所有因素的因素；犯罪是否包括网络或系统入侵或涉及犯罪内容（如儿童性剥削材料）。

393. 鉴于这些变化以及信息和通信技术在所有当代犯罪中的普遍性，无论是以数字证据形式，还是在信息和通信技术部分本身构成犯罪的情况下，“为犯罪目的使用信息和通信技术”的概念对判断犯罪性质的作用是有限的。联合王国指出，犯罪中的“数字因素”变为现实已有一段时间，这既反映了犯罪分子如何普遍使用信息和通信技术来扩大其实施犯罪的规模和机会，也反映了整个社会越来越多地使用和依赖互联网。因此，由此给执法部门带来的挑战可以说与社会在打击许多当代犯罪方面整体面临的一些广泛且多样的挑战是分不开的。

394. 尽管在定义方面存在以上问题，但联合王国提到会员国在具体调查和解决含有信息和通信技术犯罪部分的能力方面普遍面临的一些战略性挑战，其中包括：

(a) 开展数字调查的技术能力或实力不足，包括缺乏具备熟练信息和通信技术技能的工作人员，或难以留住这些工作人员，国内执法机构内部尤其如此；

(b) 一些管辖区域没有国内实体法将信息和通信技术相关犯罪定为刑事犯罪并作为通过相互承认此类罪行的方式开展国际合作的依据（双重犯罪）；

(c) 缺少能够允许对信息和通信技术相关罪行进行调查以及在法庭上采信数字证据的国内程序法及适当的人权保障和监督制度；

(d) 在衡量信息和通信技术相关罪行的规模和间接影响方面面临挑战，以及随后在提高公众对这类罪行危害的认识和鼓励举报此类罪行方面面临挑战；

(e) 在鼓励公众提高认识和采用网络安全行为和（或）提高对信息和通信技术相关罪行的认识以减少他们对此类犯罪的脆弱性和（或）为了举报目的而了解此类罪行发生的地点方面面临的挑战；

(f) 因为国家法治薄弱或留有网络犯罪分子的管辖区域不配合而带来的一般性挑战，这反映了此类犯罪的跨境性质以及此类犯罪无需在受害者所在国留下实际足迹的这一事实；

(g) 正如国家打击犯罪局的《2018 年国家战略评估》中所指出的那样，犯罪分子为了更有效地掩盖其活动而采用的技术手段带来的挑战包括犯罪分子使用暗网、加密、虚拟专用网络和虚拟货币等技术。

395. 上述很多挑战尤其与联合王国相关，并且已在就执法和调查以及电子证据和刑事司法专题向全面研究网络犯罪问题专家组第五次会议提交的书面材料中作了概况说明。[10]

396. 除了这两个主题以外，依赖网络的犯罪的少报问题仍然是一个特别重要的挑战。通过比较公共调查和官方犯罪报告统计数据，联合王国发现公众对网络犯罪的经历与报告的犯罪数量之间存在显著差距。

397. 联合王国还面临与一些管辖区域不配合有关的挑战。在《2018 年国家战略评估》中，国家打击犯罪局指出，“很多说俄语的网络犯罪集团在国际上开展活动，依然对联合王国的利益构成威胁”。在许多情况下，此类组织实际设在不允许引渡犯有此类罪行的公民或针对此类集团的合作并非轻易实现的管辖区域。

398. 联合王国认为，全面研究网络犯罪问题专家组为会员国继续探索以协商一致的方式应对网络犯罪提供了难得的机会。特别是，该专家组作为一个专家平台，其任务是系统地审议各种主题，非常适合确保有关应对网络犯罪的讨论考虑到各种各样的观点和可能的解决办法。因此，联合王国认为，必须确保该专家组进程被视为在预防犯罪和刑事司法委员会主持下的网络犯罪讨论的主要平台，与该委员会审议其他犯罪相关事项的任务授权相一致。另外，联合王国鼓励毒品和犯罪问题办公室和会员国充分利用该专家组作为供专家进行技术讨论的平台，以指导毒品和犯罪问题办公室网络犯罪问题技术援助方案的工作。

399. 联合王国还认为，《欧洲委员会网络犯罪公约》是进一步凝聚国际共识和统一网络犯罪应对办法最有效的框架。该《公约》有 63 个缔约方，在许多区域有广泛的共识，并且已经证明其本身与不同法律和体制环境是相容的。网络犯罪公约委员会为《公约》缔约方之间开展对话提供了便利，不仅如此，《公约》还通过该委员会为确保其能够考虑到网络犯罪空间动态并跟上新的挑战和技术发展步伐提供了强有力的机制。因此，联合王国建议尚未成为《公约》缔约方的会员国采取措施，请求加入《公约》，条件是要确保制定适当的人权保障措施和国内程序法。如果国内尚未制定此类规定，欧洲委员会已有旨在建设加入《公约》能力的方案；因此，联合王国认为，会员国应与欧洲委员会接触，以酌情确定是否可为上述目的提供此类技术援助方案。

[10] 可查阅 www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-March-2019/Compilation_12March.pdf。

美利坚合众国

400. 美国报告说，美国面临四大挑战，首先是面临限制专家为国际政策提出建议的压力。虽然传统执法方式有适应网络犯罪的能力，但所带来的挑战复杂且不断发展变化。因此，关于网络犯罪的联合国一切政策辩论都应该直接听取技术专家的意见和建议。尽管对采取这种做法没有得到协商一致的支持，但一些国家就缔结新的全球条约而开展政治辩论问题施加的压力消耗了宝贵的资源，削弱了专家们就如何应对会员国在调查和起诉网络犯罪时面临的核心挑战提出切实意见的能力。专家们的意见对于理解以下复杂问题非常重要：

(a) 保护言论自由；

(b) 适当限制国家权力；

(c) 有效执行现有框架和机制；

(d) 及时向发展中国家提供培训和技术援助。

401. 这一问题在大会通过第 73/187 号决议期间得到证明，当时，分裂投票引起新的大会政治辩论，损害了大会第 65/230 号决议所设全面研究网络犯罪问题专家组执行其任务的能力。第 73/187 号决议妨碍了专家组的工作，在该专家组完成自己的工作计划之前产生了另一份报告，并在执法专家一般不参与的场合推进了该报告的编写工作。会员国应加强执法和刑事司法专家、私营业界和民间社会对联合国决策进程的投入和参与。会员国还应确保根据打击网络犯罪的“一线”国内专家的建议组织政策辩论。

402. 第二项挑战与网络犯罪和跨国犯罪组织的发展演变有关。跨国犯罪组织不仅利用包括暗网在内的信息和通信技术为攻击提供便利，而且还为被盗数据创建在线市场，从而扩大了网络犯罪威胁的范围。会员国正在采取应对措施，包括让更多会员国加入《欧洲委员会网络犯罪公约》。所有区域的国家（包括发展中国家和发达国家）都利用该《公约》加强了本国法律，提高了与其他国家合作的能力，因此，也限制了跨国犯罪组织为犯罪目的利用本国信息和通信技术基础设施的能力。

403. 第三项挑战涉及国家能力有限和国家法律框架过时的问题。如果伙伴国在应对网络犯罪方面的能力有限和（或）没有更新其国内涉及网络犯罪的法律框架和调查权限，那么美国在与它们合作起诉网络犯罪时就会面临挑战。虽然一些国家依赖一般性刑事法规，但最好有打击网络犯罪的专门法规。尽管没有就网络犯罪的定义达成一致，但对应受到处罚的核心罪行清单的行为有普遍共识。虽然有很多不同的法律制度，但国际社会在起草有效、现代和全面的网络犯罪法律方面拥有十多年的经验。可以采用技术中立的角度起草这类法律，以避免需要频繁修改。《欧洲委员会网络犯罪公约》一直是其他文书的主要灵感来源，也是具有不同文化和法律传统的国家（包括一些不考虑加入《公约》的会员国）制定国内法的典范。在与使用打击网络犯罪专门法律的国家合作时，美国与其他国家合作起诉网络犯罪的工作就会更加成功。

404. 美国还在与一些已经成功通过了打击网络犯罪的专门法规的国家合作方面面临挑战，它们有的实施其法律框架的能力可能有限，有的可能在实践中没有为实施这些法规采取措施。此外，美国还在得到会员国协助以查明、逮捕和起诉其管

辖区域内的罪犯以及授权其主管部门在网络犯罪案件开展国际合作方面依然面临严重挑战。例如，迫切需要为刑事司法机关提供有关电子证据的专业培训。这就是美国为毒品和犯罪问题办公室网络犯罪问题全球方案以及美洲国家组织、欧洲委员会、东盟和非洲经济共同体主持的培训方案提供捐助的原因。美国建议会员国进一步关注这些方案，特别是针对发展中国家的方案。会员国应高度重视立法改革援助和能力建设，以确保将新法律转化为行动。

405. 第四项挑战涉及难以获取电子证据问题。与其他会员国一样，美国也在打击网络犯罪斗争中在从外国管辖区域获取电子证据方面面临挑战，而电子证据在执法调查中无处不在。具体而言，如果一些会员国没有有效应对电子证据请求的法律权限和能力，那么美国在得到这些会员国的协助方面就会面临挑战。

406. 在国内，美国在处理来自其他管辖区域的数以千计的电子证据请求方面面临挑战，通常因为这些国家不了解美国的要求，或者提供的信息不充分，不符合美国的法律标准。如果司法协助请求不充分，就需要美国有关部门要求国际合作伙伴提供说明和补充信息，从而延误了对请求的答复。会员国应根据《打击有组织犯罪公约》等文书规定的义务，增强其中央和主管部门的权能，并为其提供充足的资源和培训，从而努力消除这些差距。毒品和犯罪问题办公室也正在开展工作，为中央和主管部门提供新的工具。美国还建议加强会员国在司法协助要求和程序方面的能力建设，包括就起草适当的电子证据请求问题提供培训。

407. 最后，为了获得电子证据，会员国正在利用双边司法协助条约以及《欧洲委员会网络犯罪公约》和《打击有组织犯罪公约》等多边公约作为合作的法律依据。已有 80 多个国家积极参加七国集团“每周 7 天，每天 24 小时”高科技犯罪网络联络点，以便为应对数据保存和其他请求提供便利。美国建议会员国考虑加入并利用这些条约和网络打击网络犯罪。

委内瑞拉玻利瓦尔共和国

408. 委内瑞拉玻利瓦尔共和国政府承认，利用信息和通信技术越来越普遍，国际社会在利用这些技术方面的作用可能有助于实现包括《2030 年可持续发展议程》所载各项目标在内的国际商定发展目标，并有助于应对新的挑战。

409. 委内瑞拉玻利瓦尔共和国强调了消除障碍以缩小数字鸿沟的重要性，特别是那些阻碍各国充分实现经济、社会和文化发展及其人口福祉的障碍，尤其是发展中国家。它强调，应停止使用包括社交网络在内的信息和通信技术违反国际法以及损害会员国的利益的行为。

410. 委内瑞拉玻利瓦尔共和国鼓励国际社会共同努力，确保进入信息社会，并鼓励尊重性别平等和增强妇女权力权能、文化认同、文化、族裔和语言多样性、传统和宗教以及伦理价值观。

411. 委内瑞拉玻利瓦尔共和国报告说，它的目的是根据行为守则和职业道德，实现媒体负责任地使用和处理信息。各种形式的媒体应在信息社会发挥重要作用，信息和通信技术应在这方面发挥支持性作用。委内瑞拉玻利瓦尔共和国重申需要减少影响媒体的国际不平衡，特别是在基础设施、技术资源和人的技能发展方面。

412. 对于委内瑞拉玻利瓦尔共和国来说，以破坏发展中国家政府为目的利用媒体作为敌对宣传的工具问题令人关切。在这方面，委内瑞拉玻利瓦尔共和国强调需要促进自由、多元和负责任且能反映发展中国家和人民的现实和利益的替代通信手段和通信来源。

413. 从这个意义上讲，并意识到当前国际刑法文书不足以打击信息和通信技术相关犯罪，委内瑞拉玻利瓦尔共和国认为有必要制定一项在此领域内已获得批准且基于国际社会共识的联合国合作公约，该公约应鼓励所有会员国建设一个负责任的信息社会，并协助采取措施，以避免且不要采取任何有违国际法和《联合国宪章》以及阻碍受影响国家的人民充分实现经济和社会发展及妨碍其福祉的单方面措施。

414. 对委内瑞拉玻利瓦尔共和国而言，这种对在国际冲突、秘密和非法行动以及在个人、组织和国家通过其他国家的计算机系统攻击第三国的行动中可能使用信息和通信技术问题的关切要求在联合国框架内采取措施，以便在达成一份有助于规范在此领域的使用与合作的文件方面取得进展。

415. 鉴于一些国家政府表示有能力利用常规武器应对此类攻击所引发的关切，委内瑞拉玻利瓦尔共和国重申，预防和应对新威胁最有效的途径是所有国家携手合作，从而避免将网络空间变为军事行动区。委内瑞拉玻利瓦尔共和国认为，促进会员国之间的对话和正在进行的讨论是一项优先事项，以便分享良好做法和国家或区域经验，并特别关注发展中国家。同样，委内瑞拉玻利瓦尔共和国还表示，它支持有关在联合国主持下设立一个政府间工作组的建议，以便在各国平等的基础上寻求解决办法和解决分歧。

416. 委内瑞拉玻利瓦尔共和国还认识到，非法使用信息和通信技术可能对会员国的基础设施、国家安全和经济发展产生破坏性影响，因此，它强调国际社会需要加大在解决这一问题方面的努力。