联合国 A/AC.291/4

大会

Distr.: General
17 November 2021
Chinese
Original: Arabic/Chinese/English/
Spanish

拟订打击为犯罪目的使用信息和通信技术
全面国际公约特设委员会

会员国提交的关于打击为犯罪目的使用信息和通信技术全面国际公约的范围、目标和结构（要素）的意见汇编

秘书处的说明

摘要

为筹备拟订打击为犯罪目的使用信息和通信技术全面国际公约特设委员会第一届会议，秘书处根据特委会主席的指示编写了本说明。本说明载有从会员国收到的关于新公约的范围、目标和结构（要素）的意见。

V.21-08419 (C) 040122 050122

目录

一. 导言

1. 为筹备2021年8月11日的拟订打击为犯罪目的使用信息和通信技术全面国际公约特设委员会第一届会议，特委员主席 Faouzia Boumaiza Mebarki 女士（阿尔及利亚）邀请会员国就新公约的范围、目标和结构（要素）提出意见。提交这些意见的截止日期为2021年10月29日，随后延长至2021年11月5日。

2. 主席还指示秘书处按收到的原文汇编意见，并将其翻译成联合国六种正式语文，供特设委员会第一届会议使用。

3. 本说明是秘书处根据主席的指示编写的，载有从会员国收到的关于新公约的范围、目标和结构（要素）的意见。

二. 从会员国收到的意见

澳大利亚

[原文：英文]
[2021年10月29日]

澳大利亚欢迎有此机会就一项新的网络犯罪问题国际公约的范围、结构和目标提出意见。新公约提供一个无与伦比的机会，以确保就打击网络犯罪的国际合作达成广泛共识，使各国能够更好地打击这一无处不在且不断演变的威胁。

一项新的公约只有在大会第74/247号和第75/282号决议所设立的拟订打击为犯罪目的使用信息和通信技术全面国际公约特设委员会主持下进行的真诚讨论所达成的协商一致意见的基础上，获得大多数会员国的广泛支持，才有价值。为此，澳大利亚致力于一个公开、包容、透明和多利益攸关方的进程，这一进程是确保各国能够达成尽可能多国家都能接受的结果的最佳机会。这与澳大利亚过去给特设委员会的提交件以及澳大利亚已参与的联合提交件中所阐述的原则是一致的。澳大利亚借此机会重申这些提交件中提出的观点。

网络犯罪威胁着所有国家，但给小国带来特别的挑战。打击网络犯罪的有效国际合作对小岛屿发展中国家尤其重要，有助于加强其打击跨国网络犯罪活动的国内能力。小岛屿发展中国家必须能够有意义地参与特设委员会的工作。澳大利亚致力于确保太平洋岛国有充分机会参与特设委员会的工作。澳大利亚欢迎关于支持混合（亲身和在线）参加特设委员会届会的决定，并强调必须确保较小代表团有充分的准备和参与时间。

私营部门实体在打击网络犯罪方面发挥着独特而宝贵的作用。因此，要取得成功，特设委员会的工作必须考虑到业界利益攸关方提供的宝贵专业知识。各国还应当对民间社会组织、学术机构和政府间机构等其他非国家行为体能够对如何最好地打击网络犯罪的讨论作出贡献的广泛见解和专业知识作出回应。为了确保充分知情的讨论和有效的结果，特设委员会应为这些团体提供尽可能多的作出贡献的机会。

范围

鉴于谈判的时间框架很短，各国就构成新公约的许多问题达成协议的时间有限。公约的范围必须明确界定，并应密切关注针对网络犯罪的刑事司法对策。公约不应处理在其他论坛上处理的更广泛的网络安全问题。

为了加快我们的工作，各国应将注意力集中在需要对网络犯罪采取共同办法的领域。特设委员会的工作应采用国际社会已经很好理解的与网络犯罪和刑事司法国际合作有关的概念和术语。我们不需要“重新发明轮子”，也不想制造模棱两可。

因此，新公约应大量借鉴《联合国打击跨国有组织犯罪公约》和《联合国反腐败公约》，并酌情借鉴在联合国预防犯罪和刑事司法大会和联合国其他论坛上以协商一致方式商定的其他概念。公约应参考各国已经在国际和区域层面通过的有效的现有国际文书，如《欧洲委员会网络犯罪公约》，并且必须避免破坏这些协定中确立的现有规范。这符合大会第 74/247 号决议所载的任务，大会在该决议中呼吁特设委员会的工作充分考虑到国家、区域和国际各级的现有国际文书和努力。

特别是，公约应继续使用“网络犯罪”一词。这一术语反映了一个被广泛理解的概念，已在无数联合国文件中使用，其中包括第十二届、第十三届和第十四届联合国预防犯罪和刑事司法大会的成果文件，以及大会各项决议（最著名的是第 65/230 号决议）以及预防犯罪和刑事司法委员会和经济及社会理事会的许多其他决议和报告。

条约要素（结构和目标）

定罪

新公约提供了大幅改善与网络犯罪有关的国际合作的机会。一套核心网络犯罪罪行的统一标准将提高各国在全球、区域和国内各级应对网络犯罪的能力。

为此，澳大利亚认为，公约应当对网络犯罪已实质上变化的犯罪行为类型采取有重点的做法。各国的国内刑法通常足以界定常见的犯罪，如非法侵入、故意破坏、盗窃、与毒品有关的犯罪和暴力犯罪。公约不需要仅仅因为计算机或信息系统涉及犯罪的实施而重新想象这些犯罪。

新公约必须包括将只能通过使用信息和通信系统实施的违法行为定为犯罪的新标准，这些犯罪被以各种罪名称为“纯网络犯罪”或“依赖网络的型犯罪”。在信息和通信网络出现之前，这类犯罪并不存在，各国的国内刑法在适用于这类犯罪方面往往不足或不一致。在这一领域，统一的定罪标准将为各国提供相当多的好处，无论是在本国打击网络犯罪的努力方面，还是在促进更大的国际合作方面。

同样，澳大利亚认为，一些“传统”犯罪的实施范围、规模和容易度因信息和通信网络提供的速度、匿名性和广泛覆盖面而急剧增加。这些有时被描述

为“网络使能的”犯罪。公约应明智地处理这些犯罪，制定一个明确的框架，确定为什么某些犯罪被“网络”因素如此显著地改变，以至于需要一个新的协调一致的国际标准，将这种行为提升到“传统”犯罪之上。公约不需要为每一种可能包含“网络”元素的现有犯罪设立新的犯罪类别，特别是在被定为犯罪的行为的严重性或范围没有因该元素而发生重大变化的情况下。

澳大利亚认为，应被纳入公约的网络犯罪类别有两个明显的候选类别：网上儿童性剥削和虐待构成的严重威胁，以及网络诈骗和盗窃，包括与勒索软件有关的敲诈勒索广泛蔓延和显著增加。澳大利亚对于听取支持纳入其他网络使能的犯罪的论点持开放态度，但出于上述原因，公约应采取克制的方式纳入任何新的犯罪类别。

公约还应适当考虑网络依赖性犯罪和网络使能的犯罪的上游犯罪和附属责任。这应包括《有组织犯罪公约》和《反腐败公约》等文书所载刑事责任的标准延伸。鉴于技术在助长网络犯罪方面的作用，公约还应考虑为涉及生产、采购或提供完全或主要用于实施网络犯罪的技术和软件的犯罪制定统一的刑事标准。

网络犯罪是一个快速发展的领域，网络犯罪分子不断寻求部署新的技术和方法来扩大他们的活动并逃避执法。为了应对这一问题，公约必须确保以技术和方法中立的方式起草定罪标准，以确保条约在未来仍然具有相关性和有效性。

打击网络犯罪的程序性措施

程序法是调查和起诉网络犯罪的关键要素。公约应提供明确的程序性措施框架，以确保执法机关能够获得打击网络犯罪所需的证据。任何程序性措施框架的范围都应支持明确的国内法，国内法应足够强有力，使执法部门或其他相关当局能够通过侦查、瓦解、预防、调查和起诉等方式应对网络犯罪的挑战。

程序性措施还应考虑到电子数据的性质，确保执法部门和其他相关当局能够快速有效地获取此类数据，以确保网络空间的犯罪方法和做法不会扰乱当局的收集工作。所规定的程序性措施类别可包括搜查和扣押的权力、与数据提供有关的权力（例如读取存储的通讯和截取活动），以及要求披露这些数据的紧急或迫切请求或命令。程序性措施必须以充分保护人权和法治的强有力的保障和限制为基础。

各国可能需要考虑如何在一项新的公约中纳入与跨法域收集电子数据有关的国家做法。

国际合作与技术援助

网络犯罪本质上是压倒性的跨国犯罪。在统一定罪的支持下开展国际合作，对于各国有效调查和起诉网络犯罪分子的能力至关重要。

过去几十年来，国际社会在刑事司法国际合作方面取得了重大进展，在一系列关于司法协助、引渡和其他形式的国际合作的现有国际条约中开发了有效

的工具。例如，《有组织犯罪公约》和《反腐败公约》的规定为这种合作提供了良好基础，而且几乎已得到普遍通过。

新公约应尽可能借鉴《有组织犯罪公约》和《反腐败公约》关于司法协助、引渡、移交囚犯和追回犯罪所得的类似规定。事实证明，这些规定是有效的，得到国际社会的广泛支持。根据大会第 74/247 号决议所载任务，还应确保新公约是补充而不是损害其他现有的刑事司法国际合作机制。

其他国际和区域制度以强有力的保障和限制为基础，为打击网络犯罪的国际合作提供有效的框架。新公约应尽可能多地借鉴这些制度。其中主要的是《欧洲委员会网络犯罪公约》，该公约继续为世界各地区大量国家之间的国际合作提供有效的基础。

除了国际合作，新公约应当对提高打击网络犯罪的国际能力的努力提供有意义的推动。措辞应重申联合国毒品和犯罪问题办公室在提供技术援助和能力建设方面的主要作用，包括作为网络犯罪问题全球方案的召集人。

保护和促进人权的保障措施

国家获取个人的电子和电信数据，就其本质而言，会对个人权利产生影响。公约必须重申各国有责任根据国际人权法，在各国打击网络犯罪的努力中促进和保护个人的人权。

个人的隐私权以及意见、表达和结社自由权都必须按照现有的国际标准继续得到充分保护。还必须保护的其他权利包括获得公平审判的权利，包括法律面前人人平等的权利，以及免受酷刑和不人道或有辱人格的待遇或处罚、任意拘留和歧视的权利。国际社会一再重申，这些权利适用于网上，就像适用于线下一样，公约应重申各国在打击网络犯罪行动过程中维护这些权利的现有责任。

工作结构和方法

一旦各国有机会在将于 2022 年 1 月举行的第一届谈判会议上就公约的范围发表意见，澳大利亚期望将会很快就公约的结构达成共识。

在各国于 2022 年 1 月就新公约的范围、结构和目标发表意见后，澳大利亚提议邀请各国就新公约每个结构要素下要列入的条款提交提案（例如，关于定罪和国际合作的提案）。然后，主席应在必要时与主席团协商，努力将这些不同的提案综合成一份草案，然后各国可以进行谈判，根据特设委员会第一次会议确定的工作计划依次审议每套条款。

在就结构的每个要素进行初步谈判之后，可以再次根据特设委员会在第一次会议上确定并由主席此后管理的工作计划，就整个公约进行进一步谈判。

巴西

[原文：英文]
[2021 年 10 月 29 日]

与许多国家的情况一样，巴西一直在应对网络犯罪，网络犯罪现象的频率和复杂性都在不断增加。对于将各种犯罪罪行迁移到数字平台，需要做出果断努力，更新应对威胁（包括国际威胁）的适当的规范性执法对策。网络犯罪的地理范围和作案速度对世界各地传统的执法和法律合作机制构成挑战。

挑战是巨大的。互联网服务提供者持有调查网络犯罪和收集电子证据所需的重要信息，经常将实体总部设在某一个国家，而在不同的大陆提供服务，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，执法机关努力认定并适当处理对数据拥有管辖权和直接访问数据的人员。

管辖权的国际协调一致是起诉网络犯罪的必要步骤。需要更多更好的合作。有效的瓦解需要灵活和直接的合作方式，通过这种方式，执法机构可以及时分享涉及同一犯罪集团的不同案件的证据。

巴西充分参与了关于打击为犯罪目的使用信息和通信技术全面公约的谈判。这是在这方面的最佳传统和做法基础上，在解决这一本质上跨国问题方面建立合作共同标准的难得机会。

巴西的观点是，为了能够应对上述挑战，未来的公约必须在目标、范围和结构方面处理以下要素。

目标

公约的主要目标应当是为国际合作提供具体工具，使缔约国能够及时获得有助于调查和起诉网络犯罪的证据和其他信息。尽管有这一主要目标自主享有的优点，但理想情况下，文书还应考虑另外两个目标：(a)各缔约国的每个管辖区都确定最低限度的刑事定罪义务（实体刑法）；以及(b)规定最低限度的义务，以便各缔约国的每个管辖区都能及时进行应对、调查和起诉（程序性刑法）。

巴西完全致力于制定一项全球性公约的想法。我们对谈判一项包含最低刑事定罪标准的文书的挑战很敏感，特别是考虑到这种现代和不稳定的现象。然而，在这个方向上有成功的先例。在其他犯罪领域，例如现有的全球犯罪问题公约，有效的谈判使世界大多数国家能够承诺遵守最低限度的实质性标准。辩论不应从地理范围和定罪范围之间的预设对立开始，而应从这样一种理解开始，即谈判本身将是就关于网络犯罪的实体刑法达成尽可能最低共识的最安全方法。尽管可能受到限制，但关于定罪的最低共识——真正以中立和一般概念为基础——可限制网络犯罪分子对管辖区的选择，促进经验交流，并减少要求适用双重犯罪原则进行合作的国家之间的规范性争议。

国际合作的及时性将始终取决于最多样化的管辖区的调查人员、检察官和法官可以使用的程序性工具。传统的法律合作工具，如调查函和承认外国判决，凭其本身在任何地方都无法确保对网络犯罪做出充分的应对。这一现象固有的跨国性和极端波动性要求程序标准化，即使在考虑所涉国内法律制度的所

有特殊性时具有所需的灵活性和一般性也是如此。然而，这一程序标准化的核心应涉及一些最低标准，以便能够迅速保全由灵活和直接的国际渠道启动的电子证据，否则将无法认定犯罪分子，特别是在有组织犯罪案件中。

范围

公约应为交换与以下方面有关的证据和数据提供基础：(a)针对计算机系统的犯罪；及(b)任何通过电子手段实施的犯罪。理想情况下，应该对与连接、内容和订户相关的电子数据进行寻址。

公约还应允许缔约方提出国际合作请求（为加速保全电子数据和司法协助），并向其他管辖区发送自发信息。必须有一章专门涉及建立一个国际从业者网络，这些从业者将负责应对紧急情况。这种运作机制加强这样一种理解，即这样一项公约需要建立一个决策机构来监测和审查其执行情况。

作为一项框架文书，该条约可以确立将谈判协议作为额外工具的可能性，这将深化关于特定网络犯罪类型的合作。

因此，公约应成为刑法实际适用的文书，而不是深入研究关于国际和平与安全、网络防御的政策或与国内、区域或全球各级互联网的结构或治理有关的问题。

结构

鉴于上述考虑，巴西认为公约应具有以下结构：

第一章　定罪

第二章　刑事诉讼法促使及时侦查和起诉

第三章　国际合作

A. 快速保全电子数据

B. 司法协助

C 自发信息

第四章　合作网络

第五章　监测和审查执行情况的后续机制

加拿大

[原文：英文]
[2021 年 11 月 1 日]

加拿大目前的提交件是响应拟订打击为犯罪目的使用信息和通信技术全面国际公约特设委员会秘书处 8 月 11 日的关于请会员国就新公约的范围、目标和结构（要素）提交意见的邀请。

在编写这些意见时，加拿大受联合国内部在预防犯罪和刑事司法委员会主持下 20 多年来在网络犯罪问题上所做重要工作的启发，特别是全面研究网络犯罪问题政府间专家组、联合国毒品和犯罪问题办公室（通过其网络犯罪问题全球方案）以及联合国预防犯罪和刑事司法大会所做的工作。这些举措为拟订一项联合国公约奠定了基础，该公约应完全侧重于打击网络犯罪，而不是处理其他联合国论坛所更好地处理的网络安全、网络治理和其他相关事项。

根据大会第 75/282 号决议以及加拿大过去向特设委员会提交的意见，加拿大谨重申，新公约的谈判必须是一个透明和包容性的进程，让民间社会和其他相关利益攸关方有一个有意义的参与机会。

范围

新公约应提供一个框架以打击经常通过使用计算机系统实施的网络犯罪和严重刑事犯罪，其中包括以下内容：

(a) 对实质性网络犯罪以及调查和起诉经常通过使用计算机系统实施的网络犯罪和严重刑事犯罪作出规定；

(b) 对与上述有关的国际合作以及获取其他刑事犯罪的电子证据作出规定；

(c) 含有旨在防止网络犯罪的措施的规定；以及

(d) 含有鼓励会员国和其他利益攸关方提供持续技术援助和能力建设举措的措施的规定。

新公约的内容必须符合国际人权义务，特别是与表达、意见和结社自由有关的义务，以及不受非法或任意干涉个人隐私的权利。

目标

新公约应当有以下目标：

(a) 在共识的基础上，确立实质性刑事犯罪、程序权威和国际合作打击网络犯罪的的基线；

(b) 确保以技术中立的方式起草条款，以确保条款不会随着技术的发展而过时或无法执行；

(c) 推动并便利在共同打击网络犯罪的斗争中开展国际合作；

(d) 确立收集、获取和分享其他犯罪的电子证据的权威；

(e) 消除网络犯罪实施者的安全庇护所；

(f) 确保遵守国际人权义务，特别是与表达、意见和结社自由有关的义务，以及不受非法或任意干涉隐私的权利；

(g) 确保与联合国在预防犯罪和刑事司法领域的现有条约，特别是《联合国打击跨国有组织犯罪公约》和《联合国反腐败公约》保持一致，并考虑到已

证明在打击网络犯罪方面有用的多边文书，特别是《欧洲委员会网络犯罪公约》；以及

(h) 支持会员国通过技术援助和能力建设加强应对网络犯罪的能力。

结构

关于新公约的结构，除了明确的定义和最后条款外，加拿大认为应将以下五个要素作为公约结构的组成部分：

(a) 实质性犯罪条款要求会员国采取必要的立法和其他措施：

㈠ 将影响计算机系统、网络和计算机数据的机密性、完整性和可用性以及滥用计算机系统、网络和计算机数据的行为定为犯罪；以及

㈡ 确保其刑法充分涵盖经常利用计算机系统实施的特定传统犯罪，例如传播儿童色情；

(b) 程序性条款要求会员国采取必要的立法和其他措施，以确立保全和获取存储在外国、多个或未知管辖区的计算机系统上的刑事犯罪电子证据的权力。虽然新公约应包括更一般的调查权，如搜查令、扣押令和提供令，但也应包括更专门的调查工具，以应对犯罪的实施速度以及电子证据的瞬时性和波动性。这些条款应受到保障措施的约束，以确保执法活动符合国际人权义务；

(c) 国际合作对打击网络犯罪非常重要。新公约需要包括促进正式和非正式国际合作的机制，以侦查、调查和起诉网络犯罪，以及获取其他刑事犯罪的电子证据；

(d) 新公约需要包括类似于《有组织犯罪公约》和《反腐败公约》规定的预防措施，例如关于提高认识和教育举措的规定。多方利益攸关方伙伴关系和民间社会可以发挥重要作用，这一点应反映在这些条款中；

(e) 新公约应鼓励会员国通过技术援助和能力建设加强应对网络犯罪的能力。这可包括以下方面的条款：

㈠ 支持多利益攸关方参与；

㈡ 鼓励与联合国毒品和犯罪问题办公室及其网络犯罪问题全球方案协作，提高从业人员和中央机关利用技术促进在打击网络犯罪方面开展国际合作的技能；以及

㈢ 为调查人员和检察官制定培训方案，并支持与相关利益攸关方分享信息和经验。

智利

[原文：英文]
[2021 年 11 月 5 日]

智利政府高兴地响应在执行大会第 74/247 号和第 75/282 号决议方面邀请会员国就新公约的范围、目标和结构（要素）提交意见。

智利认为，新公约不应与其他先前存在的关于网络犯罪的条约或协定相冲突。它应基于国际合作和技术援助，作为打击网络犯罪的多边办法的基础。必须平等考虑所有国家的意见，以保持一个开放、包容、透明和多利益攸关方的进程。

1. 一般方面

(a) *管辖权*。新公约是讨论这一问题的绝佳机会，这是可以处理的许多程序性工具的基础；

(b) 确保以全面的方式起草定义，以确保其在快速技术变革的背景下的相关性和适用性。包括定义，例如不同类型数据的定义。

2. 实体刑法

(a) *纳入收受计算机数据罪*。虽然有些国家对这种犯罪类型有一个有限的概念，但是当被盗的“货物”对应于计算机数据，并且任何存储这些数据的人都知道或不能不知道其虚假来源时，将从事这类行为的非法行为包括在内似乎是合适的；

(b) 从作案者和参与的角度来看，具体处理通过计算机诈骗非法窃取的金钱或证券的收受者提供的合作似乎是适当的，因为考虑到这类犯罪在绝大多数案件中展现出的特殊性和调查挑战，对那些通常构成犯罪链中第一个环节的人所受起诉予以特殊对待是适当的，因此，在他们参与的基础上增加他们作为诈骗作案者的身份是适当的，不影响在他们对抓捕剩余的计算机犯罪分子给予有效配合的情况下提供减轻处罚的可能性。

3. 程序法规则

(a) 应当讨论当局可以用来对正在精心制定或打算在互联网上实施的犯罪进行侦查的可能的新想法和工作工具，以及打击这类犯罪的最有效方式；

(b) 似乎应当讨论必须在必要和适当地保护公民和个人数据与刑事调查之间取得平衡，因为过度保护这类信息可能会在制定能够正确和及时地对这类犯罪提起刑事诉讼的调查程序方面产生后果，这归因于这类行为带来的匿名性、跨国性和缺乏可追溯性。

4. 关于国际合作的章节

(a) 确立刑事事项司法协助原则十分重要；

(b) 各国应探讨如何帮助确保及时、安全地在处理网络犯罪的调查人员和检察官之间交换信息；

(c) 缔约国应当在符合本国法律制度和行政管理制度的情况下相互密切合作，以加强打击网络犯罪的执法行动的有效性。各国应采取有效措施，在其主

管机关、机构和服务部门之间建立沟通渠道，以便利安全、快速地交换有关网络犯罪所有方面的信息；

(d) 认为司法协助的电子传输是一种有效和永久的形式，而不仅仅是在紧急情况下；

(e) 数据的保全和交付；

(f) 分析 24/7 网络作为对国际合作的创新贡献的积极贡献；

(g) 管控紧急情况；

(h) 各国应共同查明国家间“数字鸿沟”的存在，一些发展中国家缺乏预防、侦查和打击网络犯罪的能力，在面对网络犯罪挑战时更加脆弱。

5. 国际合作特殊工具

(a) 互联网服务提供者提供数据及其与各国的关系；

(b) 跨境数据存取；

(c) 特殊侦查手段：网上密探、联合调查组、联合调查等。

6. 预防

(a) 预防网络犯罪需要各种利益攸关方的参与，包括政府、执法机关、私营部门、国际组织、非政府组织和学术界；

(b) 促进以受害者为中心的、处理人际网络犯罪的预防战略；

(c) 各国应考虑实施与业界合作的机制，包括向国家主管机关移交案件和移除有害的犯罪材料，包括儿童性剥削材料和其他令人憎恶的暴力材料。

7. 网络犯罪公约背景下的性别视角

(a) 在执行和评价公约各项规定的影响时纳入性别视角，并在使用信息和通信技术时，特别是在提到与网络犯罪有关的针对性别的问题时，考虑到性别敏感的分析，以促进性别平等和在线上线下增强妇女权能；

(b) 应对网络犯罪，预防和打击针对妇女和儿童的暴力行为。

中国

[原文：中文]
[2021 年 11 月 5 日]

中国欢迎联合国关于制定打击为犯罪目的使用信息和通信技术全面国际公约的特委会主席邀请成员国提交对公约范围、目标和框架（要素）的意见。根据联大第 75/282 号决议，特委会应向第 78 届联大提交公约草案。中方期待各国

在主席领导下开展建设性讨论，如期达成一项具有普遍性、权威性、为各方所接受的新公约，为在全球范围内加强打击网络犯罪合作提供法律框架。

此前，各国已利用联合国相关机制就打击网络犯罪问题开展深入讨论，形成了一些共识，还有国家提出了完整的公约文本草案，这些都为公约谈判提供了重要参考。中方支持主席鼓励各国积极提交意见和案文建议，并在各国建议基础上汇总形成公约零案文，争取尽早启动公约案文谈判。

为支持主席和特委会工作，中方草拟了对联合国打击网络犯罪公约范围、目标和框架（要素）的意见，并愿与各方开展建设性磋商。

一. 目标

㈠ 秉持网络空间命运共同体理念，促进和加强各项措施，以便更加高效而有力地预防和打击为犯罪目的使用信息和通信技术；

㈡ 基于信通技术特殊性和打击相关犯罪行为的需要，促进、便利和支持预防和打击为犯罪目的使用信通技术方面的国际合作，包括协调各国定罪标准，为解决管辖权冲突提供指导，在执法合作、司法协助、引渡、资产返还等方面制定更有针对性的制度安排等；

㈢ 着眼最广泛国际合作的需要及发展中国家利益和需求，强化在人员培训及提供技术援助方面的合作，并促进该领域的信息交流，以更好预防和打击为犯罪目的使用信通技术；

二. 适用范围

本公约应当适用于预防、侦查和起诉由个人或犯罪集团实施的为犯罪目的使用信通技术，以及查封、冻结、扣押、没收和归还相关犯罪所得。

为犯罪目的使用信通技术，至少应当包括针对信通技术设施、系统和数据的犯罪以及利用信通技术实施的犯罪。

三. 框架（要素）

公约可分为 7 个章节，分别是：总则、预防、定罪和执法、国际合作、技术援助和信息交流、执行机制和最后条款。

有关章节要素初步建议如下：

㈠ 总则

除目标、适用范围外，还应包括以下内容：

1. *保护主权*。《联合国宪章》确立的主权平等原则是当代国际关系的基本准则，主权原则适用于网络空间也已得到各国普遍支持。公约应明确，缔约国在履行其根据本公约所承担的义务时，应当恪守各国主权平等和领土完整原则以及不干涉他国内政原则。

2. 术语。可对“电子证据”、“个人信息”、“关键信息基础设施”、“云存储”、“网络服务提供者”、“恶意软件”、“僵尸网络”、“有害信息”、“网络攻击”等公约可能涉及的重要术语作出界定。

㈡ 预防

应突出预防为犯罪目的使用信通技术的重要性，将“预防为主、打防并重”作为基本原则，明确各国政府和私营部门在预防犯罪方面的责任，政府应当制定有针对性的预防犯罪措施，同时鼓励社会参与和公私合作。具体可包括以下内容：

1. 鼓励各国确定专门机关负责制定关于预防为犯罪目的使用信通技术的政策措施并定期进行评估；建立关键信息基础设施安全保护和网络安全等级保护制度，对不同的网络设施采取不同的信息安全技术和管理措施，重点确保关键信息基础设施不受犯罪分子或集团的攻击；强化政府相关部门在预防犯罪方面的能力建设。

2. 各国应制定或完善国内立法，明确网络服务提供者等私营部门在预防为犯罪目的使用信通技术方面的责任，包括安全防范（如制定网络安全事件应急预案，及时处置系统和硬件漏洞、计算机病毒、网络攻击、网络侵入，以及在发现其服务可能被用于犯罪时及时采取处置措施等）、日志信息记录留存（政府部门应明确留存日志的内容标准和期限）等。在确定网络服务提供者所应承担的责任时应充分考虑不同规模网络服务提供者在能力方面的区别，并作出分层分级且符合比例原则的安排。

3. 鼓励政府、私营部门和社会各界开展多种形式的公私合作，特别是应努力做好公共宣传，提升公众预防犯罪的意识。

㈢ 定罪和执法

当前，犯罪分子和犯罪集团更倾向于滥用信通技术实施各种类型的犯罪，还滋生了专门开发可用于犯罪的信通技术以及交易相关技术和数据的黑色产业链。公约应当立足当前和未来信通技术发展和打击犯罪的需要，在协调定罪方面提供更具灵活性和前瞻性的框架，同时在管辖、执法、电子证据等方面作出配套的制度设计。

1. 要求各国应将侵入、破坏信通技术设施、系统、数据或关键信息基础设施的行为规定为犯罪，可包括：非法访问计算机信息系统、非法干扰计算机信息系统、非法获取计算机数据、非法干扰计算机数据、侵犯关键信息基础设施等。

2. 对于国际社会有普遍共识的、利用信通技术实施的犯罪行为，公约可以酌情列举，包括：网络勒索、网络诈骗、网络色情特别是儿童色情、利用信通技术侵犯著作权和邻接权、利用网络煽动、实施恐怖主义、传播有害信息等。

3. 对于利用信通技术实施的其他犯罪，可强调，未在本公约中列明，不妨碍各国依据本公约、其他国际公约和各自国内法，预防和打击有关犯罪并开展国际合作。

4. 针对利用信通技术实施犯罪日益产业化的现状，应将犯罪黑色产业链纳入定罪范围，加强对帮助行为和预备行为的打击，可包括开发、出售、传播用于犯罪的信通技术和数据等。

5. 关于“电子证据”，应当对电子证据在刑事司法程序中的认定规则作出规定，包括如何认定电子证据的真实性、完整性、合法性、关联性等。

6. 应要求各国制定或完善国内立法，明确网络服务提供者等私营部门配合执法部门监测、侦查和打击犯罪的义务，包括按照统一的内容标准和期限留存日志信息，保存数据，固定证据，配合执法行动等。在确定网络服务提供者所应承担的义务时应充分考虑不同规模网络服务提供者在能力方面的区别，并作出分层分级且符合比例原则的安排。如网络服务提供者不履行相关义务，各国应当根据国内法对其实施有效的行政和刑事处罚。

7. 应为解决管辖权冲突提供指导。应立足网络空间和信通技术的特殊性，争取就如何确定管辖权、避免管辖权冲突提供指导标准，主张管辖权应基于与犯罪行为存在“真实、充分”的联系，优先考虑犯罪结果发生地、犯罪行为实施地和犯罪行为人（集团）所在地；如难以形成有关标准，可争取提出排除标准，如一国不能仅依据数据途经该国即主张对有关案件有管辖权。在管辖权冲突的情况下，应依据有利于起诉和财产损失追回的原则协商确定管辖。

8. 还应对教唆和帮助犯罪、犯罪预备、犯罪未遂、单位犯罪等作出规定。

㈣ 国际合作

为犯罪目的使用信通技术具有极强的跨国性，是国际社会面临的共同挑战。同时，犯罪行为的匿名性、智能化以及电子证据的不稳定、易灭失等特点，给现有国际法律框架下的司法协助等国际合作机制带来巨大挑战。各国应在预防和打击为犯罪目的使用信通技术方面最大程度给予相互合作，秉持对等原则，并积极探索制度创新，提出更有针对性的国际合作新机制。

1. 跨境调取电子证据是打击为犯罪目的使用信通技术的需要，但应尊重证据所在地的国家主权，遵守正当程序，尊重相关个人和实体的正当权利，不得采取侵入性和破坏性技术侦查手段跨境获取电子证据。一国不得违背数据存储国法律，直接向企业、个人或采用绕过网络安全保护措施的技术手段等方式调取存储在外国的数据。应探索获取境外电子证据新的制度安排，如相互委托进行电子证据鉴定、视频（音频）取证等，努力平衡尊重各国主权和打击犯罪等多重目标，为解决跨境调取电子证据问题提供统一、权威的指引。

2. 应制定快速开展执法合作的方式，各国可指定具体机关负责联络，允许在特殊需要的情况下快速交换犯罪线索、提供技术咨询等执法合作。

3. 为提高刑事司法协助效率，各国可建立主管部门之间的快速联络响应机制，确保在有需要的情况下可以随时联系到相应国家的主管部门。可在国家

数据跨境传输安全管理制度框架下，考虑通过采用电子签章等技术手段实现跨境取证法律文书和电子证据网上交换。可进一步规定紧急情况下的司法协助，电子证据的快速保全，数据保全后的快速披露等。

4. 在通过国内法明确网络服务提供者等私营部门配合执法部门监测、侦查和打击犯罪义务的基础上，各国特别是网络资源发达国家应进一步强化国际合作，如一国网络服务提供者所掌握的信通技术设施、系统或网络被他国嫌疑人用于犯罪，只要该国也对此类行为规定为犯罪，该国应主动或应他国请求，要求相关网络服务提供者采取技术措施和其他必要措施有效应对犯罪活动。

5. 应强化相关措施，防止和阻断犯罪所得的国际转移，加强资产追回方面的国际合作。各国应以快速、有效返还资产为原则，不应为返还资产设定司法程序之外的其他前提条件。

㈤ 技术援助和信息交流

为有效预防和打击为犯罪目的使用信通技术，为发展中国家提供技术援助，并加强信息交流至关重要。

1. 对发展中国家的技术援助应包括：对执法、司法人员进行培训，培养法律素养和技术知识兼备的专业团队，特别是应当加强电子证据取证能力建设；酌情提供相关设备和技术，帮助发展中国家强化打击犯罪的能力；鼓励联合国毒罪办等国际组织、私营部门和专家学者共同参与技术援助和能力建设。

2. 鼓励各国分享在法律和政策制定及实施、预防、打击犯罪、犯罪趋势等方面的经验和数据。

㈥ 执行机制

为促进公约的执行，应设立缔约国大会以及有关专家组或者工作组，如技术援助工作组、国际合作工作组等，为各国交流经验、促进合作提供平台。

㈦ 最后条款

略。

哥伦比亚

[原文：英文]
[2021 年 11 月 5 日]

鉴于大会通过了第 74/247 号决议，经由该决议设立了一个不限成员名额特设政府间专家委员会，以拟订一项打击为犯罪目的使用信息和通信技术全面国际公约，并响应特设委员会主席邀请会员国就未来的网络犯罪公约应具有的范围、目标和结构提出意见，我们谨提交哥伦比亚的以下初步意见。

范围

新公约应侧重于国家机关预防、调查、起诉和惩治网络犯罪罪行的国际法律合作工具的目标，并处理与电子证据有关的事项。因此，应避免不侧重于网络犯罪法律问题和电子证据管理的讨论。

应避免讨论可能具有政治敏感性和与拟谈判的公约实质内容没有直接关系的问题。

新公约必须考虑到现有的国际法律框架和文书，包括《联合国打击跨国有组织犯罪公约》、《联合国反腐败公约》和《布达佩斯网络犯罪公约》，因为大多数国家的国家立法和做法与现有协定保持一致或基于现有协定；因此，今后的标准必须符合这些协定。此外，应确保拟制定的规则不会与各国承担的其他国际义务不兼容或相冲突。

在这方面，公约应采取补充办法，即谈判原则上应考虑到国际社会多年来在打击网络犯罪方面已经开展的工作，而不应与各国承担的相关国际义务相抵触。因此，应当利用《联合国打击跨国有组织犯罪公约》在既定原则和司法合作工具方面带来的潜力和进展。

应考虑到目前的多边、区域和双边司法协助框架，以避免法律法规中的潜在冲突，补充和适用现有国际文书，并避免妨碍其有效执行。因此，应当建议不仅要彻底考虑多边先例，如《联合国打击跨国有组织犯罪公约》和《网络犯罪公约》，而且要彻底考虑双边和区域协定，如《美洲刑事事项互助公约》。

具体而言，应考虑到《网络犯罪公约》（2001 年，布达佩斯），因为它涵盖了已经广泛讨论的概念，并反映了 20 年的实际国际经验。不这样做就有可能走上一条削弱在打击网络犯罪方面已经取得的进展的道路。

这一进程还应考虑到联合国框架内的全面研究网络犯罪问题专家组的工作成果，并应借鉴会员国在该专家组的会议期间提出的初步结论和建议清单。

我们强调，必须以包容和透明的方式并尽可能在协商一致的基础上拟订新公约，就像联合国以前缔结《有组织犯罪公约》和《反腐败公约》的进程所做的那样，以帮助防止今后的争端。

目标

公约的总体目标应当是采用一个国际司法合作框架，对在打击为犯罪目的——“网络犯罪”——使用信息和通信技术方面的预防、调查和起诉作出全面规定，并处理与电子证据有关的事项。

结构

- 随着时间的推移仍然有效的关键定义和标准化技术概念。
- 实质性规定（国家立法确立的刑事犯罪）。

在这方面，公约应将影响计算机系统和信息的一系列行为定为犯罪。

就原则和方法而言，完全侧重于“核心”网络犯罪罪行是合乎逻辑的：与通过非法访问计算机系统罪而未经授权以数字方式访问计算机网络或系统有关的罪行；网络间谍活动，包括通过拦截或获取存储在计算机系统中或通过通信网络传输的数据、通信、文件或数据库而侵犯自然人和法人隐私的所有行为，还包括拦截计算机数据、破坏个人数据和创建网络钓鱼网站以获取个人数据的罪行；以及计算机破坏，旨在扰乱、损坏、使其无法使用、锁住或干扰计算机系统、数据库或数据处理、传递和传输过程，包括非法扰乱计算机系统或电信网络的罪行。

此外，该文书可涵盖一些由于以数字手段实施而产生严重和深远影响且难以调查的行为；这将使公约具有足够的灵活性，可作为打击与其他犯罪有关的非法活动的工具：

- 双重犯罪条款：这一机制对于促进司法协助十分重要，无论引起这种协助的行为是否根据被请求国的法律应受惩罚，从而除其他外确保在没有共同标准立法的情况下，网络犯罪分子在一些国家找不到安全避难所。

- 有利于有效法律合作的程序性规定：在这方面，必须加强在调查网络犯罪罪行方面的国际合作，特别是在数字证据管理、监管链、数据保留和法证分析方面。数据的传输和存储是一个需要紧急关注的问题，也需要确定各种机制，使不同国家的对应机关能够通过适当和安全的数字渠道进行快速通信和作出反应。

- 适用于使信息和数据保护的合法权利受到影响的行为的加重处罚情节，例如与大规模捕获个人数据有关的行为、侵犯人权或针对关键基础设施和基本服务的行为。

- 国际司法合作：通过具有适当保障措施的数字渠道并通过标准格式，便利、扩大和加快司法协助请求。

- 界定收集数字证据的特别调查机制，特别是与存储在不同法域的证据有关的数字证据。

- 会员国必须商定机制，确保在通过国际文书交流信息的过程中充分保护个人数据，这不仅是因为在数字环境中保护个人数据的重要性，而且是为了避免每个国家的特定规则可能造成的可能性妨碍国家间有效交流信息。

- 促进技术援助，传播与调查、起诉和惩罚有关的知识和良好做法。此外，为了弥合数字鸿沟，公约必须涵盖执法机构和其他国家司法机关的能力建设，特别是在作为一种预防形式的教育和培训方案方面。

- 通过区域培训学校促进技术合作。鉴于调查通过数字手段实施并妨碍有效调查的犯罪的复杂性和特殊性，有必要以有组织和持续的方式，并根据列有预期成果的预先确定的工作计划，向检察官和调查人员提供专门培训。

- 促进公共和私营部门在网络犯罪领域开展强有力的、以信任为基础的合作至关重要，因此必须就这一问题达成共同立场，并为包括互联网

服务提供者和通信公司在内的数字领域行为者收集数字证据提供便利。

- 促进和便利主管机关利用能力建设和信息交流合作平台以及网络犯罪调查的分析和背景工具。
- 为在紧急情况下及时获得信息提供便利的规定。
- 最后，建议公约规定建立一个每周 7 天、每天 24 小时运作的联络点网络，以回应与网络犯罪有关的国际法律合作请求。此外，该网络还可由以下方面的联络网加以补充：(a)促进分享关于网络犯罪和相关犯罪的知识和经验；(b)创建和传播良好做法；以及(c)优化和精简国际司法合作。

多米尼加共和国

[原文：英文]
[2021 年 11 月 5 日]

多米尼加共和国欢迎有机会与所有会员国一起为这项集体工作作出贡献，以期分别根据大会 2019 年 12 月 27 日第 74/247 号决议和 2021 年 5 月 26 日第 75/282 号决议，就一项关于网络犯罪的新国际文书的范围、目标和结构提出意见。

网络犯罪是一种新兴的跨国犯罪形式，也是全世界增长最快的犯罪之一。它的兴起与信息和通信技术的演变和指数级发展密切相关，每年影响到数百万公民和企业。

我们区域——拉丁美洲和加勒比——已特别受到这一现象的影响。发展中国家在很大程度上缺乏打击网络犯罪所需的能力，这种情况已直接影响到被大量记录为此类犯罪受害者的人。

此外，最近的 2019 冠状病毒病（COVID-19）大流行突出了国际社会对网络犯罪的脆弱性，这种情况突出了不仅在会员国之间，而且在各国政府与非政府组织、民间社会、学术界和私营部门之间开展合作与协调的基础上采取全球对策的重要性。由于网络犯罪的复杂性和规模如此之大，任何对策要想有效，就必须以多学科办法为基础。

多米尼加共和国完全支持国际社会的这一努力，并重申愿意与所有会员国共同努力，在任何时候都以透明、公正和包容原则为指导，缔结一项代表我们每一个人的国际条约。

范围

多米尼加共和国认为，一项关于网络犯罪的新国际文书的主要目的是为预防、侦查、调查和刑事起诉网络犯罪提供有效工具，同时充分尊重隐私、数据保护、公民自由和人权。

特别是，该文书应促进刑事调查进程，使得能够及时收集和随后使用数字证据，从而减少这类犯罪的有罪不罚现象，这种有罪不罚现象是实地执法人员面临的主要制约因素之一。

文书还应促进和便利会员国之间的国际合作以及在需要网络犯罪问题方面的这种支持的缔约国的技术援助和能力建设。

多米尼加共和国还认为，应明确规定新文书应限于网络犯罪领域；它不应处理其他论坛正在讨论的与网络安全和互联网治理有关的问题。

不过，我们的理解是，应考虑到现有国际和区域文书的规定，以避免与将这些文书作为国家立法基础的会员国的法律制度不必要地不一致，或与这些文书的适用不必要地不一致。因此，必须借鉴在执行有关文书方面取得的经验，确定新公约可能处理的优点和缺点。同样应考虑到全面研究网络犯罪问题专家组等专门小组所作的努力。

目标

预防和打击网络犯罪的新国际文书除其他外应：

- 促进和便利缔约国之间迅速、实际和有效的国际合作。
- 涵盖预防、侦查、调查和刑事起诉该文书适用的网络犯罪，以及涵盖收集和处理与其他犯罪有关的数字证据，为缔约国提供打击这类跨国犯罪的必要工具。
- 明确确定新公约条款将适用的犯罪类型，以及在所有缔约国的法律制度中应被视为非法行为的犯罪类型。
- 促进和便利需要这种能力建设的缔约国的能力建设，以防止创建“网络庇护所”。
- 促进分享良好做法和经验教训。
- 为确立管辖权确定明确的规则，以便向“全球”互联网服务提供者索取数字证据，这是目前减少有罪不罚现象和支持网络犯罪受害者的最大挑战之一。
- 确立明确的保障措施和对不遵守这些保障措施的惩罚制度。
- 确立足够的权力以调查所涵盖的刑事犯罪，同时在任何时候都考虑到尊重隐私、数据保护、公民自由和人权。
- 鉴于技术的迅速发展，公约应具有广泛和长期的愿景；因此，应使用技术中性的措辞，以确保随着时间的推移公约的适用性不受技术发展的影响。
- 创建一种多学科办法，使公共部门和私营部门能够积极合作。

结构

- 定义。
- 刑事犯罪。
- 调查的程序工具。
- 保障措施。
- 国际合作。
- 获取数字证据。
- 技术援助和调查能力建设。
- 标准运作程序。
- 预防措施。
- 执行机制。

埃及

[原文：阿拉伯文]
[2021 年 10 月 28 日]

阿拉伯埃及共和国希望为制定一项打击为犯罪目的使用信息和通信技术的全面联合国公约的国际努力作出积极贡献，并遵守本国在与人权和打击跨国犯罪有关的国家、区域和国际条约和公约下的承诺，因此编写了本提交件，其中包括提议列入上述公约正文的暂定内容，希望通过加强国际合作和制定旨在打击所有信通技术相关犯罪的共同的打击犯罪政策来实现预期目标，以期避免这些犯罪对国家的安全和利益及其社区和公民的安全构成的危险。

一. 目标

公约应旨在加强联合国会员国之间在打击为犯罪目的使用信通技术方面的合作，以防止任何威胁信通技术完整性和保密性的行动，将为非法目的滥用信通技术定为刑事犯罪，促进调查和起诉犯罪者的手段。公约还应规定消除与信通技术有关的犯罪的后果，包括暂停与因实施公约所述任何非法行为而获得的资产有关的交易，并没收和返还此类犯罪的所得，通过建立国际合作安排，提供足以有效打击与信通技术有关的犯罪的权力，以便利侦查、调查和起诉此类犯罪以及引渡。

二. 范围

1. 除另有规定外，公约应适用于预防公约本身提到的犯罪。

2. 各缔约国均应采取一切必要措施，在下列情况下确立对根据公约确立为此类犯罪的刑事犯罪和其他非法行为的管辖权：

(a) 犯罪发生在该缔约国领域内；或者

(b) 犯罪发生在犯罪时悬挂该缔约国国旗的船只或已根据该缔约国法律注册的航空器内。或者

(c) 具有跨国性质，以及有组织犯罪集团参与了实施犯罪。在下列情况下实施的犯罪应被视为具有跨国性质：㈠犯罪系在一个以上国家实施；㈡犯罪系在一个国家实施，但在另一个国家部分筹备、计划、指导或监督；㈢犯罪系在一个国家由在一个以上国家从事犯罪活动的有组织犯罪集团实施；或㈣犯罪系在一个国家实施，但在另一个国家造成严重后果。

3. 为执行公约，公约所述犯罪或其他非法行为并不是一定造成物质损害，除非公约另有规定。

4. 缔约国应考虑限制声明保留意见，以便能够广泛适用上述措施。

三. 保护主权

1. 各缔约国均应根据本国立法和宪法原则，按照国家主权平等和不干涉他国内政的原则，履行因适用公约而产生的义务。

2. 公约不应授权一缔约国主管机关在另一缔约国领土内行使该另一国本国立法规定的专属于该国当局的管辖权和职能。

四. 拟由公约涵盖的犯罪

1. 各缔约国均应采取必要的立法和其他措施，防止实施《公约》所述犯罪或任何其他与信通技术有关的犯罪，包括阻断和移除与此类犯罪有关的内容；侦查罪行；起诉犯罪者；引渡罪犯；以及促进国际合作和证据收集程序。

2. 各缔约国还应采取必要的立法和其他措施将下列行为定为刑事犯罪：

第 1 条. 非法使用通信和信息服务和技术，包括从通过信息网络或信通技术设备传输的电信服务或音频或视频渠道中非法获益，或教唆他人非法获益。

第 2 条. 非法访问和（或）超过访问权限制，包括：

1. 以在时间或访问级别方面超过权限的限制的方式使用获准访问网站、私人帐户或信息系统的权限。

2. 非法访问全部或部分信息技术系统或与全部或部分信息技术系统进行通信，并继续进行这种访问或通信。

3. 如果此类访问或通信导致以下情况则应加大对这种罪行的处罚：

(a) 擦除、修改、扭曲、复制、转移或毁坏保存的数据、电子设备和系统或通信网络，或损害用户和受益人；

(b) 获取机密政府信息。

第 3 条. 通过非法损害、扰乱、减慢、扭曲、隐藏或改变公司、机构、设施或自然人的网站设计来攻击网站设计。

第 4 条. 通过任何技术手段或通过切断信息技术数据的发送或接收来故意和非法地截取数据流。

第 5 条. 通过故意非法毁坏、擦除、阻碍、修改或阻断信息技术数据侵犯数据完整性。

第 6 条. 滥用信息技术，生产、销售、购买、进口、散播、提供或拥有任何经设计或改造的工具或软件、密码或类似信息，以此可访问某个信息系统，意图利用该信息系统实施公约所述犯罪之一，或者制作意图毁坏、阻断、修改、复制或传播数字信息或使其安全特征失效的恶意软件，但合法研究目的除外。

第 7 条. 进行伪造，以造成损害的方式利用信息技术改变信息的真实性，意图将改变了的信息用作有效信息。

第 8 条. 进行诈骗，故意和非法对受益人和用户造成伤害，诈骗的意图是以非法方式为犯罪人或其他人实现利益和好处，包括借助与虚拟货币（数字货币或加密货币）有关的诈骗性电子犯罪。

第 9 条. 威胁或敲诈，利用信通技术或任何其他技术手段威胁或勒索某人实施或不实施某种行为。

第 10 条. 色情，其中：

1. 信通技术被用于制作、展示、散播、提供、出版、购买、销售或进口用于淫秽目的的色情材料。

2. 信通技术被用于制作、展示、散播、提供、出版、购买、出售或进口儿童或未成年人色情材料，包括在信通技术中或在任何信通技术存储介质上拥有此类材料或描绘儿童或未成年人的猥亵材料。

第 11 条. 其他与色情有关的罪行，包括性剥削或骚扰，特别是对妇女、儿童或未成年人的性剥削或骚扰。

第 12 条. 通过包括互联网在内的信息和通信网络施加心理或其他压力，无论是通过直接互动还是通过流行技术或电子游戏，鼓励或强迫自杀，包括鼓励或强迫未成年人自杀。

第 13 条. 利用信通技术使未成年人参与实施危害其生命或身心健康的非法行为。

第 14 条. 利用信通技术侵犯隐私，包括创建电子邮件、网站或私人账户，并将其错误地归于自然人或法人。

第 15 条. 利用信息技术实施与恐怖主义有关的犯罪，包括：

1. 传播恐怖主义集团的思想和原则或为恐怖主义辩护。

2. 资助恐怖主义行动或为这种行动提供培训，便利恐怖主义组织之间的联系或向进行恐怖主义行动的人提供后勤支助。

3. 传播制造炸药的方法，特别是用于恐怖主义行动。

4. 传播狂热、煽动叛乱、仇恨或种族主义。

5. 缔约国应采取必要措施，禁止通过信通技术手段传播此类内容，包括阻断和移除与这些犯罪有关的内容。

第 16 条. 金融犯罪，如洗钱，包括：

1. 利用信通技术实施金融犯罪或滥用虚拟货币（数字货币或加密货币）。

2. 进行洗钱活动，或请求协助或传播进行洗钱的方法。

第 17 条. 非法使用电子支付工具，包括：

1. 以任何手段伪造、制造或创造便于伪造或模仿任何电子支付工具的任何装置或材料。

2. 挪用任何支付工具的数据、使用这种数据、向他人提供该数据或教唆他人获取这种数据。

3. 利用信息网络或信息技术获得对支付工具的代码或数据的未经授权的访问。

4. 明知是伪造的支付工具而予以接受。

第 18 条. 与利用信息技术实施的有组织犯罪或跨国犯罪有关的犯罪，包括：

1. 销售或贩运麻醉药品或精神药物。

2. 非法分销假冒药品或医疗产品。

3. 偷运移民。

4. 贩运人口。

5. 贩运人体器官。

6. 非法武器贸易。

7. 贩运文化财产。

第 19 条. 与侵犯著作权和相关权利有关的罪行，包括侵犯缔约国法律所界定的著作权和相关权利，如果该行为是故意实施的。

第 20 条. 未经授权访问关键信息基础设施，包括：

1. 创建、散播或使用旨在提供对关键信息基础设施的未经授权访问的软件或其他数字信息，包括毁坏、阻断、修改或复制其中所含信息或使其安全功能失效。

2. 违反为旨在存储、处理或传送关键信息基础设施或信息系统所载受保护数字信息或受缔约国国家立法保护的信息的介质以及属于关键

信息基础设施的通信网络制定的操作规则，或违反访问这些信息的规则，如果此类违规行为损坏了关键信息基础设施。

第 21 条. 煽动颠覆或武装活动或其他刑事犯罪，包括通过信通技术呼吁开展针对另一国政府的颠覆或武装活动，破坏公共安全和稳定，或呼吁实施可处以不少于一年监禁的刑事犯罪。

第 22 条. 与极端主义有关的犯罪，包括散发宣传基于政治、意识形态、社会或族裔动机的非法行为或为其辩护的材料，或煽动族裔或宗教仇恨或一般敌意的材料；或提供对这些材料的访问。

第 23 条. 未遂实施公约规定的任何犯罪，包括作为共犯参与和（或）组织或指挥他人实施公约规定的任何犯罪。

第 24 条. 其他非法行为。

公约不应排除缔约国将通过信通技术故意实施的造成重大损害的任何其他非法行为定为犯罪。

五. 法律责任、刑事程序、执法和国际法律援助

第 1 条. 法人的责任

在服从本国立法的情况下，各缔约国均应规定法律实体对其代表以其名义或为其利益实施的任何犯罪的刑事责任，但不妨碍对实施犯罪的自然人（如站点管理人）进行处罚。

第 2 条. 服务提供者/站点管理人的责任

在不妨碍公约规定的情况下，服务提供者/站点管理人及其下属应遵守以下义务，违反这些义务应被定为犯罪：

1. 将所述信息系统日志或任何信息技术的日志保存并存储一段待确定的时间。要保全和存储的数据应包括：

(a) 能够识别服务用户的数据；

(b) 与客户信息系统内容有关的数据，无论何时在服务提供者控制下；

(c) 与通信量有关的数据；

(d) 与通信外围设备有关的数据；

(e) 国家为执行公约而规定的任何其他数据。

2. 对已保存和存储的数据保密，并禁止在未经主管机关合理命令的情况下披露此类数据，包括任何服务用户的个人数据或与此类用户或同用户有通信联系的个人或实体访问的网站或私人账户有关的任何数据或信息。

3. 确保数据和信息的安全，以保持其机密性并保护其免受破坏和损坏。

4. 服务提供者/站点管理人应以方便、直接和持续访问的形式和方式向服务用户和任何主管机关提供以下数据和信息：

(a) 服务提供者的名称和地址；

(b) 服务提供者的联系信息，包括电子邮件地址；

(c) 许可证数据，以确定服务提供者和监督服务提供者的主管机关。

5. 如果国家规定的主管机关提出要求，服务提供者/站点管理人应提供允许主管机关行使其权力的所有技术能力。

第 3 条. 刑事程序

1. 各缔约国均应采取必要的立法和其他措施，确立预防、识别、侦查、调查犯罪行为和其他非法行为并采取针对这些行为的法律行动的权力和程序。

2. 各缔约国均应将上述权力和程序适用于：

(a) 公约确立的犯罪行为和其他非法行为；

(b) 利用信通技术实施的其他刑事犯罪或其他非法行为；

(c) 以电子方式收集犯罪证据。

3. 刑事程序应包括：

(a) 加快保全使用信息技术存储的数据，包括已经使用信息技术存储的流量数据，特别是如果认为这种信息会丢失或修改，为此命令有关人员保全其所拥有或在其控制下的信息的完整性，使主管机关能够进行搜查和调查，同时对在这方面采取的任何行动保密；

(b) 加快保全和部分披露流量数据，无论是否有一个或多个服务提供者传递信息，并确保主管机关迅速披露相当数量的信息，使缔约国能够查明服务提供者和传输信息的途径；

(c) 发布命令，移交缔约国境内某人所拥有并存储在信息技术或存储介质上的信息，或在缔约国境内或在缔约国控制下提供服务的服务提供者所拥有的信息；

(d) 检查或读取存储在信息技术或存储介质中的信息；

(e) 控制、复制和保全所存储的信息，以完成搜索和访问信息的程序；

(f) 实时收集流量数据，管辖区内的服务提供者有义务收集、记录和维护信息的机密性；

(g) 拦截信息内容，使主管机关能够通过技术手段收集和记录通过信通技术实时传输的信息；

(h) 各缔约国均应采取必要的立法和其他措施，使其主管机关能够停止传输和广播构成公约规定的犯罪的任何内容。

4. 数字证据的接受：

从装置、设备、电子媒介、信息系统、计算机程序或任何信通技术手段获得或提取的数字证据，如果符合缔约国法律所要求的技术条件，则应具有刑事证据中法证证据的价值和证明力。

第 4 条. 国际法律和司法合作

1. 缔约国应根据公约或对等原则促进相互合作，以交流信息，以期防止实施信息技术犯罪，协助调查此类犯罪并追踪此类犯罪的犯罪人。

2. 缔约国应根据本条的规定和关于刑事事项国际合作的其他国际文书，并根据对等原则以及相关国家立法，尽可能充分地开展合作，以预防、制止、侦查和起诉与使用信通技术有关的犯罪。

3. 为引渡和刑事事项司法协助的目的，公约所述任何犯罪都不应被视为政治罪。因此，不得以涉及政治罪、与政治罪有关的罪行或出于政治动机的罪行为由拒绝与此类罪行有关的引渡或刑事事项法律协助请求。

5. 管辖权：

在下列情况下，各国均必须采取必要措施，将其管辖权扩大到上述罪行：

(a) 罪行是全部或部分在缔约国领土内实施或犯下的；

(b) 罪行是全部或部分在悬挂缔约国国旗的船只上实施或犯下的；

(c) 罪行是全部或部分在根据缔约国法律登记的航空器上实施或犯下的；

(d) 罪行是全部或部分由一缔约国的国民实施或犯下的，条件是该罪行根据犯罪所在地的国家立法应予惩罚，或者如果罪行是在任何国家的管辖范围之外实施的；

(e) 罪行影响到国家的一项更高利益。

6. 引渡：

(a) 缔约国之间应交换上述罪行的犯罪人，条件是这些罪行根据有关缔约国的立法应受到惩罚。缔约国在本国立法允许的情况下可同意针对本公约所涵盖的根据其本国立法不应受惩罚的罪行提出的引渡某人的请求；

(b) 就缔约国之间现有的任何引渡条约而言，上述罪行应被视为实施这些罪行的犯罪人的可引渡罪行；

(c) 以订有条约为引渡条件的缔约国，如收到未与其订有引渡条约的另一缔约国的引渡请求，可将本公约视为进行引渡的法律依据；

(d) 引渡应符合被请求缔约国立法规定的条件或适用的引渡条约所载的条件，包括缔约国可拒绝请求的理由；

(e) 各缔约国均可不引渡其公民，在这种情况下，如果另一缔约国向其提出起诉该公民的请求，则应在其管辖范围内起诉在任何其他缔约国实施的根据两缔约国立法应处以剥夺自由刑罚的罪行的公民，并附有其所拥有的档案、文件、资料和证据；应向提出请求的缔约国通报就其请求所做的工作，并应确定犯罪人在被请求引渡的罪行发生之日的国籍；

(f) 对于本条所适用的任何犯罪，缔约国应当在符合本国法律的情况下，努力加快引渡程序并简化有关的证据要求；

(g) 被请求缔约国在不违背本国法律及引渡条约规定的情况下，可以在认定情况必要而且紧迫时，根据请求缔约国的请求，拘留被请求缔约国领域内的被请求引渡人，或者可以采取其他适当措施，确保该人在进行引渡程序时在场；

(h) 如果为执行法院裁决而提出的引渡请求以被请求引渡的人是被请求缔约国国民为理由而被拒绝，被请求缔约国应在其国家立法允许并根据其国家立法的情况下，应根据请求缔约国的请求，考虑执行根据请求方国家立法判处的刑罚，或执行尚未执行的刑罚的任何部分；

(i) 在对任何人就本条所适用的任何犯罪进行诉讼时，应当确保其在诉讼的所有阶段受到公平待遇，包括享有其所身处的缔约国本国立法所提供的一切权利和保障；

(j) 如果被请求缔约国有充分理由认为提出引渡请求是为了以某人的性别、种族、语言、宗教或国籍为理由对其进行起诉或者处罚，或者按请求执行将使该人的地位因上述任一原因而受到损害，则不得对本公约的任何条款作规定了被请求国引渡义务的解释；

(k) 缔约国不应仅仅因为犯罪是与金融事项有关的犯罪而拒绝引渡请求；

(l) 被请求缔约国在拒绝引渡前应当在适当情况下与请求缔约国磋商，以使后者有充分机会陈述自己的意见和提供与其请求中所列事实有关的资料；

(m) 各缔约国在交存批准书或通过书时，均应有义务将负责引渡或程序性逮捕请求的主管机关的联系信息通知一个有待商定的专门机构，并定期更新该机构的信息；

7. 互助：

(a) 所有缔约国均应尽可能充分地为调查、与信息和信息技术犯罪有关的程序或收集犯罪的电子证据相互提供协助；

(b) 双边协助请求及其有关来文应以书面形式提交。各缔约国均可在紧急情况下提交紧急请求，包括通过电子邮件提交，条件是这种通信须合理安全（包括使用加密）并有参考，而且传输须应缔约国的请求得到确认；

(c) 除公约的规定外，双边协助应符合被请求方立法或互助条约规定的条件，包括被请求方可拒绝合作的理由；

(d) 如果请求互助的缔约国只能在存在双重犯罪的情况下提供协助，则应视为满足了双重犯罪的条件，无论缔约国的立法对相关犯罪的归类是否与请求缔约国相同。

8. 自行提供信息：

一缔约国可根据本国立法，在未经另一缔约国事先请求的情况下，转交在本国调查期间收集的信息，条件是该缔约国认为披露此类信息有助于该另一缔约国启动或进行与根据本公约确立的此类犯罪有关的调查，或可能导致该缔约国提出合作请求。

9. 与合作和互助请求有关的程序：

(a) 在请求缔约国和被请求缔约国之间没有根据现行立法订立互助与合作条约或公约的情况下，应适用本款各项。如果存在这种条约或公约，则不应适用上述各项，除非有关各方同意予以全部或部分适用；

(b) 各缔约国均应指定一个中央机关，负责传送、接收和批准司法协助请求或将其转交主管机关。该中央机关的联系信息应定期更新；

(c) 根据本条提出的互助请求应按照请求缔约国规定的程序执行，条件是这些程序不得与被请求缔约国的立法相抵触；

(d) 被请求缔约国可推迟采取应所提请求而采取的措施，条件是这些措施可能影响其主管机关正在进行的刑事调查；

(e) 被请求缔约国在拒绝或推迟协助之前，应在与请求缔约国协商后，确定是否部分批准请求或在符合其认为适当的条件的情况下批准请求；

(f) 被请求缔约国应将请求的执行结果通知请求缔约国。如果请求被拒绝或最后执行被推迟，被请求缔约国应有义务通知请求缔约国这种拒绝或大幅推迟的理由；

(g) 请求缔约国只能在符合将请求付诸履行的情况下，才可要求被请求缔约国对请求保密。如果被请求缔约国不能遵守保密请求，应当将此情况通知请求缔约国。然后，请求缔约国应决定所提请求可在多大程度上得到履行；

(h) 在紧急情况下，互助请求可由请求缔约国的司法机关直接发送至被请求缔约国的司法机关。在这种情况下，请求缔约国的中央机关必须同时将请求副本发送至被请求缔约国的对应机关；

(i) 根据上一分段发出的通信和请求可通过国际刑事警察组织（国际刑警组织）发出；

10. 拒绝提供协助

(a) 被请求缔约国除了以上述各段所述拒绝理由拒绝提供协助外，如果认为执行请求会侵犯其主权、安全、秩序或基本利益，亦可拒绝提供协助；

(b) 对本公约所述罪行的司法协助请求不应以这些罪行是政治罪或类似罪行为由拒绝。

11. 保密和使用限制：

如果请求缔约国和被请求缔约国之间没有根据现行立法订立互助条约或公约，则必须适用本条。如果存在此类公约或条约，则不应适用，除非有关缔约国同意全部或部分适用。

12. 加快保全信息系统中存储的信息：

(a) 任何缔约国均可请求另一缔约国紧急保全利用位于其领土内的信息技术存储的信息，提出请求的缔约国希望就此提出互助请求，以搜查、扣押、保护或披露这些信息；

(b) 被请求缔约国如认为执行保全请求会威胁其主权、安全、秩序或利益，可拒绝执行。

13. 当被请求缔约国在执行关于保全某些通信的相关流量数据的请求的情况下发现来自另一个国家的服务提供者参与了信息的传输时，它应向请求缔约国披露足够数量的流量数据，以便能够查明该服务提供者以及所寻求保全的信息的传输路径。

14. 与获取存储的信息技术信息有关的双边合作和协助：

(a) 任何缔约国均可请求另一缔约国搜查、获取、扣押、保护或披露在被请求缔约国领土内存储和放置的信息技术信息，包括已保全的信息；

(b) 被请求缔约国应有义务按照本公约的规定答应请求缔约国的请求；

(c) 如果相关信息可能丢失或修改，应紧急答复请求。

15. 跨境获取信息技术信息：

任何缔约国均可在未获另一缔约国授权的情况下获取公开（开放源码）的信息技术信息，不论信息的地理位置如何。

16. 在实时收集流量数据方面的双边合作和协助：

(a) 缔约国应相互提供双边协助，实时收集与本国境内某些通信有关并通过信息技术传送的流量数据；

(b) 各缔约国均应提供这种协助，至少应针对为国家立法所规定的类似案件实时收集流量数据的情况所涉犯罪提供这种协助。

17. 内容数据方面的双边合作与协助：

缔约国应有义务在适用的条约和国家立法允许的范围内，在实时收集信息技术传输的具体通信的内容数据方面相互提供双边协助。

18. 专门机构:

(a) 各缔约国均应根据本国法律制度的基本原则，确保设立一个专门机构，每周 7 天、每天 24 小时确保为与信息技术犯罪有关的调查或程序提供立即协助，或收集特定犯罪的电子形式证据。这种协助应包括促进或执行：

㈠ 提供技术咨询；

㈡ 保全基于相关条款的信息；

㈢ 收集证据、提供法律信息和确定嫌疑人所处地点；

(b) 任何缔约国的专门机构均应有能力与其他缔约国的类似机构进行紧急联系；

(c) 如果任何缔约国指定的专门机构不是该缔约国负责国际双边协助的机关的一部分，则应授权该专门机构迅速与这些机关协调；

(d) 各缔约国均应确保提供合格的人力资源，以便利上述机构的工作。

六. 技术援助和培训

1. 技术援助的一般原则：

(a) 缔约国应考虑为各自的打击与信通技术有关的犯罪的计划和方案相互提供最广泛的技术援助，特别是为发展中国家提供最广泛的技术援助，包括本公约所述领域的物质支持和培训，以及培训、援助、转让技术和知识以及交流最佳相关经验和专门知识，这将促进缔约国之间在引渡和司法协助方面的国际合作；

(b) 缔约国应当加强努力，在国际组织和区域组织内并在有关的双边和多边协定或者安排的框架内最大限度地提高业务和培训活动的效果；

(c) 缔约国应考虑根据请求相互协助，就各自国家中所实施的与信通技术有关的犯罪的类型、原因和影响进行评价、研究和调研，以期在主管机关和主要行为者的参与下制定打击这些类型的犯罪的战略和行动计划；

(d) 缔约国应考虑建立筹资机制，以期通过技术援助方案和项目向发展中国家所做的努力提供援助；

(e) 缔约国应考虑交流与网络犯罪和电子形式证据收集有关的法律、政策或技术发展情况的信息。

2. 培训和能力建设：

(a) 各缔约国均应在必要时为负责预防和打击与信通技术有关的犯罪的工作人员制定、实施或改进特定的培训方案。这些培训方案可以涵盖以下方面：

㈠ 采取有效措施，预防、侦查和调查与信通技术有关的犯罪，并惩罚和打击这些犯罪，包括使用电子证据收集和调查技术；

㈡ 防止转移本公约确立的犯罪的所得，并追回此类所得；

㈢ 侦查和阻断与转移本公约确立的犯罪的所得有关的交易；监测本公约确立的犯罪的所得的转移情况；并监测用于转移、隐藏或伪装这种所得的方法；

㈣ 建立适当和有效的法律和行政机制和方法，以便利扣押和没收本公约确立的犯罪的所得；

㈤ 用以保护与司法机关和执法机关合作的被害人和证人的方法；

㈥ 制定和规划打击信通技术犯罪的战略政策。各国应投资于建立和加强数字取证能力，包括提供安全培训和资格认证，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，为成功起诉网络犯罪提供支持；

㈦ 编写符合本公约规定的条件的司法协助请求书；

㈧ 调查网络犯罪、电子证据处理、监管链和法证分析；

㈨ 在与打击信通技术相关犯罪有关的所有活动中提供语言和专业培训，并保护和加快与专门机构的沟通，以侦查和控制相关犯罪；

(b) 在网络犯罪领域拥有更先进能力和基础设施的缔约国在向其他国家特别是发展中国家提供司法协助时，以及在打击网络犯罪领域向其提供支持和咨询并转让知识时，应承担与这些能力相称的责任。

欧洲联盟及其成员国

[原文：英文]
[2021 年 11 月 2 日]

本文件反映了欧洲联盟及其成员国[1]对拟订一项新的关于打击为犯罪目的使用信息和通信技术行为的联合国公约时需要考虑的范围、目标和结构（要素）的观点和立场，并对根据大会第 74/247 号决议为此目的设立的拟订打击为犯罪目的使用信息和通信技术全面国际公约特设委员会第一届会议的筹备工作作出贡献。

这一贡献不妨碍欧洲联盟及其成员国今后在关于未来联合国公约的范围、目标和结构的谈判过程中可能采取的任何立场。

一. 目标

欧洲联盟及其成员国强调，未来的联合国公约应成为刑事执法和司法机关在全球打击网络犯罪的实用工具，目的是增加国际合作的价值。正如大会第 74/247 号和第 75/282 号决议所反映的那样，未来的联合国公约应充分考虑到有组织犯罪和网络犯罪领域经过反复试验的国际和区域文书的现有框架。因此，任何新的公约都应以任何方式补充和避免损害现有文书的适用或任何国家对这些文书的进一步加入，并尽可能避免重复。

未来的联合国公约应规定保护人权和基本自由，既适用于线下也适用于线上，并与这一领域的相关文书相兼容。

大会第 75/282 号决议商定的未来联合国公约应充分考虑到全面研究网络犯罪问题不限成员名额政府间专家组的工作[2]和成果[3]。

二. 范围

为此，欧洲联盟及其成员国认为，未来联合国公约的范围应主要侧重于实体刑法和刑事诉讼法以及相关的合作机制。该公约还应遵守国际人权标准，努力以最有效的方式打击网络犯罪，从而保护受害者。

欧洲联盟及其成员国认为，这项新文书应准确界定其使用的术语，并优先考虑现有国际文书中已经商定的概念。

---

[1] 奥地利、比利时、保加利亚、克罗地亚、塞浦路斯、捷克、丹麦、爱沙尼亚、芬兰、法国、德国、希腊、匈牙利、爱尔兰、意大利、拉脱维亚、立陶宛、卢森堡、马耳他、荷兰、波兰、葡萄牙、罗马尼亚、斯洛伐克、斯洛文尼亚、西班牙和瑞典。

[2] 见 www.unodc.org/unodc/cybercrime/egm-on-cybercrime.html。

[3] 见 UNODC/CCPCJ/EG.4/2021/2。

欧洲联盟及其成员国建议，该公约的内容应紧凑，侧重于刑事司法的基本要素，因此应尽可能排除任何附属要素。

根据上述原则，欧洲联盟及其成员国认为，未来的联合国公约应包括以下要素：

1. 与应当被未来联合国公约所有缔约国定为刑事犯罪的网络犯罪相关的**实体刑法规定**。这些规定一般应只涉及高技术犯罪和网络依赖性犯罪，如非法访问、拦截或干扰计算机数据和系统。[4]

实体刑法规定必须得到明确和狭义地界定，并完全符合国际人权标准和全球、开放、自由、稳定和安全的网络空间。将未来的联合国公约或其他普遍法律文书没有明确界定的行为类型定为刑事犯罪的模糊规定，有可能不适当和不成比例地干扰人权和基本自由，包括言论和表达自由权，同时也造成法律上的不确定性。

实体刑法规定应尽可能以技术中立的方式起草，以涵盖未来的技术发展。[5] 同时，应鼓励就进一步技术发展带来的新挑战交换意见和信息。

必须避免与其他国际公约不兼容，特别是在某些罪行，如贩运武器或非法分销麻醉药品，已经被国际公约的现有条款广泛涵盖的情况下，因此，将这些类型的行为列入一项关于网络犯罪的公约不会有额外价值。

一般而言，未来的联合国公约应避免在现有模式（如《联合国打击跨国有组织犯罪公约》第十一条第一款）之外为制裁或惩罚特定犯罪制定（最低）标准。

关于管辖权的规则，未来的联合国公约应仿照现有法律文书中规定的办法，如《有组织犯罪公约》第十五条中规定的办法。

2. **适当的实质性和程序性条件和保障措施**，以确保符合人权和基本自由，包括执法行动的合法性、必要性和相称性原则，以及具体的实质性和程序性保证措施，特别是确保隐私权和个人数据保护，言论和信息自由权以及公平审判权。这种保证措施应以其他相关国际法律文书所载的保障措施为基础，并至少与之处于同一水平。

3. **关于未来联合国公约缔约方之间合作机制的程序措施和刑事程序规定**，包括酌情在调查和其他司法程序以及在获取电子证据方面进行合作，同时确保这些证据能够在刑事诉讼中收集、保全、认证和使用。这种措施和规定必须符合并借鉴其他相关国际法律文书所载措施和规定提供的模式，并辅之以适当的保证措施，包括在紧急情况下的合作的保证措施。[6]

4. 与人权相一致的要素，涉及**能力建设、分享最佳做法和经验教训以及技术援助**，包括联合国毒品和犯罪问题办公室在这些领域的重要作用。

---

[4] 根据 2021 年 4 月 6 日至 8 日在维也纳举行的全面研究网络犯罪问题专家组会议通过的关于刑事定罪的建议 5（见 UNODC/CCPCJ/EG.4/2021/2，附件，建议 5）。

[5] 见 UNODC/CCPCJ/EG.4/2021/2，附件，关于立法和框架的建议 1。

[6] 同上，建议 16，关于电子证据和刑事司法。

欧洲联盟及其成员国认为，必须将下列各项排除在未来联合国公约的范围之外：

- 与国家安全或国家行为有关或规范国家安全或国家行为的事项
- 与互联网治理规则有关或规范互联网治理规则的事项，已在专门的多利益攸关方政策和论坛中得到处理

最后，作为一项政府间文书，未来的联合国公约应避免直接对非政府组织，包括互联网服务提供者等私营部门的非政府组织施加义务。

三. 结构

在上述基础上，未来的联合国公约可包括以下不同的章节：

序言（未来联合国公约的范围和目标）

一. 犯罪的类型和准确定义

二. 国内程序规则和在这方面应尊重的基本原则，例如，尊重人权，包括隐私权和个人数据保护权、必要性和相称性

三. 国际合作

四. 技术援助、培训和能力建设，以及联合国毒品和犯罪问题办公室在这方面的作用

印度尼西亚

[原文：英文]
[2021 年 10 月 28 日]

一般背景和目标

印度尼西亚作为世界上最大的互联网用户之一，认识到信息和通信技术对社会的重要性。然而，信通技术的进步被用于了不负责任的行为，最值得注意的是网络犯罪和网络恐怖主义，破坏了信通技术为政治、经济和社会发展的使用。

网络犯罪与其他跨国犯罪一样，由于技术和网络空间的独特性和无国界性质，影响到了国际社会。因此，国际合作至关重要。印度尼西亚赞扬大会第 74/247 号决议获得通过，其中大会决定设立一个不限成员名额特设政府间委员会，以拟订一项关于打击为犯罪目的使用信息和通信技术行为的全面国际公约。

印度尼西亚认为，在拟订打击为犯罪目的使用信息和通信技术全面国际公约特设委员会框架内讨论特定的网络犯罪公约是非常及时和关键的，并希望各国利用这一势头，以包容和透明的方式讨论和谈判一项能够应对网络犯罪挑战的国际文书。

在过去十年中，在讨论和制定旨在确定预防网络犯罪最有效方法的国际文书方面取得了显著进展。因此，在考虑未来的网络犯罪文书时，各国应考虑所有现有平台和框架，包括全面研究网络犯罪问题政府间专家组的工作和《联合国打击跨国有组织犯罪公约》。

关于这一网络犯罪公约的讨论应主要旨在加强和促进国际合作，支持国家、区域和国际努力打击为犯罪目的使用信通技术行为，包括提供技术援助，以改进会员国的国家立法和框架，并建设国家机关处理此类犯罪的能力。

此外，公约应规定国家之间的适当和有效措施，并酌情与有关国际和区域组织合作。

原则

与许多国际公约一样，我们的审议应反映会员国根据各国主权平等和领土完整以及不干涉他国内政原则承担的义务。此外，各国在根据本国国情和需要制定打击网络犯罪的政策和立法时，应尊重其他国家的主权权利。

未来的文书必须认识到为犯罪目的使用信通技术行为对安全的影响以及社会经济和人道主义后果。同时，该公约必须确保打击网络犯罪的措施侧重于犯罪行为，不危及信通技术的发展，包括研究、开发和技术转让。

促进为和平目的使用信通技术符合所有人的利益，对共同利益至关重要。尊重主权、人权和基本自由以及可持续和数字发展仍然是这些努力的核心。

印度尼西亚还认为有必要确保根据每个国家的国内法制定、执行和适用刑事程序，同时也承认需要应对各国刑事程序差异带来的挑战，以及每个国家根据相关国际文书承担的义务，例如根据《有组织犯罪公约》和关于国际人权、知识产权以及双边引渡和司法协助的条约。

此外，会员国必须强调需要保持一个公开和透明的多利益攸关方进程，使所有会员国能够真诚地谈判，以找到知情、基于共识和现实的解决办法。

范围

此公约的范围必须能够应对为犯罪目的滥用信通技术行为带来的当前和未来挑战，保护信通技术用户，并减轻和防止对人员、数据、系统、服务和基础设施的伤害。

公约还应能够确保会员国能够采取必要的立法和其他措施，把从事公约禁止的活动，特别是计算机犯罪和与计算机有关的犯罪，以及为进一步非法目的的活动，定为刑事犯罪。

印度尼西亚认为，未来的公约应涵盖一系列核心网络犯罪。这些包括但不限于：

(a) 非法进入或用黑客手段侵入计算机系统；

(b) 非法拦截计算机和系统数据；

(c) 诈骗；

(d) 为犯罪目的滥用计算机数据和系统；

(e) 侵犯著作权及相关权利；

(f) 操纵计算机数据和系统；

(g) 散播和传播非法内容和材料，例如色情、儿童色情、虚假信息、阴谋、恶作剧和含有基于种族、民族、宗教或政治的敌意的材料。

会员国应考虑采取必要措施，开展此公约概述的刑事诉讼，包括但不限于：

(a) 保全数据和系统以及保全单个或多个服务提供者存储的流量数据，并指出在本国领土内保全数据的时限和所存储数据的分类受本国国内法监管；

(b) 个人或法律实体提交或传输存储的计算机数据，并制定适当措施，迫使在线系统服务提供者提交或转让存储的计算机数据，包括与所提供服务类型有关的数据；

(c) 搜查和扣押数据和计算机系统，创建和保存计算机数据副本，以及修改和传输储存的数据；

(d) 收集和记录实时流量数据，以及从在线服务和（或）系统提供者获得流量数据。

考虑到这一点，会员国应确保根据隐私保护、保密、公共服务可持续性、保持公共服务连续性和维护公共利益以及数据集成等原则开展网络犯罪调查进程。

合作

应在国家一级和跨国层面有效调查网络犯罪和利用信通技术来便利实施的犯罪。因此，该文书应成为打击为犯罪目的使用信通技术行为的国际合作的有效机制。这种合作应根据国家立法，在互利和对等的基础上进行，同时考虑到现有文书和现行机制和框架。

鉴于多利益攸关方办法对预防、侦查和根除网络犯罪的重要性，讨论还应侧重于促进与处理网络犯罪的实体的有力合作，包括执法机关与信通技术服务提供者之间的合作。在这方面，与私营企业进行合作，并在可行时通过公私伙伴关系加强这种合作，对于增进知识和提高应对网络犯罪的对策的效力至关重要。会员国还应投资于提高公共和私营部门对网络犯罪的认识。

我们的审议还应强调采取措施，使主管机关能够进行调查，通过司法协助机制收集和没收数据，会员国不妨考虑在这方面利用其现有的法律框架。

在司法协助方面，我们的审议工作应尽可能充分考虑到调查、起诉和司法程序方面的相关法律、条约和协定。鼓励会员国除其他外，讨论加快收集电子证据的安排或相关主管机关之间的信息共享机制。

该公约关于国际合作的规定必须提供一个基本的法律框架，以应对国际合作中的程序挑战、差距和机制不足，特别是在调查、信息共享、数据和电子证据收集以及起诉方面，并为便利各国之间的引渡提供便利。还鼓励会员国指定联络人或主管机关，以加快执行该公约关于国际合作的规定。

此外，会员国不妨考虑通过有助于提高会员国复原力的能力建设和技术援助努力，加强其侦查、调查和应对为犯罪目的使用信通技术行为的国家能力。这些能力建设措施应以相互信任为基础，由符合国家确定的需要的需求驱动，并充分承认国家自主权。

由于在预防和消除网络犯罪方面的合作仍然是我们讨论的优先事项，未来的文书至少应包括一份通过以下措施改进合作的活动清单：

(a) 分享关于网络犯罪威胁的信息；

(b) 促进增强执法机构、检察官和司法机关之间的合作与协调；

(c) 分享与跨境调查网络犯罪有关的最佳做法和经验；

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

(e) 制定服务提供者协助执法机构调查网络犯罪的准则，包括数字证据和信息的保全格式和期限方面的准则；

(f) 在政策中发展人力技能和人力资源，使会员国能够提高对数字技术的适应能力；

(g) 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能力和法律能力。

通过这一机制，会员国还应继续提高国内机构间协调和协同增效的效力，包括与区域组织、私营部门、计算机应急小组和计算机安全事件应急小组、民间社会组织和其他利益攸关方分享信息和接触，以促进有效的国际合作。

讨论还应包括一个审查未来文书规定的所有承诺和义务的适用或执行情况的机制。

牙买加

[原文：英文]
[2021 年 10 月 29 日]

根据拟订打击为犯罪目的使用信息和通信技术全面国际公约特设委员会秘书处关于请各国就一项打击为犯罪目的使用信息和通信技术的国际公约的范围、目标和结构提出意见的请求，现提交以下意见。

牙买加期待着与其他会员国合作，为起草一项网络犯罪公约的工作作出贡献。牙买加期待着这样一项公约，即其将为全球社会服务，寻求保护公民免受网络威胁或其他犯罪攻击，并将得到普遍接受和批准。牙买加欢迎民间社会专家参与这一领域的工作，为我们的审议提供信息。

牙买加认为，制定一项打击为犯罪使用信息和通信技术（信通技术）行为的公约的进程是全球应对各国因这一威胁而遇到的问题的一个重要步骤。在国际安全背景下推进网络空间负责任国家行为政府专家组的 2015 年协商一致报告中适当概述了这样一项公约的目标，该报告第 13 段(d)分段规定，各国应考虑如何进行最佳合作，以交流信息、相互协助、起诉为犯罪使用信通技术的行为，并采取其他合作措施应对这种威胁。[7]

合作交流信息以协助各国打击和起诉为犯罪使用信通技术的行为应是该公约的首要目标。由此产生的目标是提高各国对网络犯罪方面不同观点的了解。希望这将导致各种办法的统一，创建一个适用于所有人的国际框架。然而，这一目标的成功取决于一个以平衡、公平、透明和包容的方式考虑包括小岛屿发展中国家在内的所有国家的立场的进程。

应考虑到能够有助于但不会不适当地拖延在缔结一项公约方面取得进展的其他进程。应遵守为谈判和完成公约草案而商定的时间表，以表明我们对打击网络犯罪的重视程度。

不言而喻，术语定义是谈判的起点。条款确定该公约的范围，对实现参与者的共同目标很重要。因此，定义应明确、独特和精心拟订，以确保它们不是过度限制性或宽泛的，而是适合公约的背景和宗旨。

打击为犯罪目的使用信通技术是一项广泛的任务。因此，这些罪行必须“不受未来影响”。它们的框架不应将含义限于现有技术，而应能够得到充分的解释，以跟上未来技术和不断演变的信通技术环境。

公约应突出能加强各国打击网络犯罪的可用工具包的定罪，这些定罪不侵犯个人的基本权利和自由，而是力求促进对这些权利的遵守和尊重。因此，应考虑国际人权条约。

新公约的条款应适当考虑到国家主权原则以及《联合国宪章》和国际法中概述的关于刑事诉讼程序、执法和国际合作事项的其他原则。

牙买加认为，公约必须充分处理国际合作问题，因为这将鼓励在全球打击网络犯罪方面加强合作。在国家之间没有司法协助条约的情况下，公约应当就提出和答复请求的程序向各国提供指导。这应包括费用责任等事项。

公约必须承认各国的能力不同，这反过来又影响到它们为取得最佳成果而需要进行广泛合作的能力。因此，必须提供技术援助，以建设各国为打击网络犯罪全球框架作出更大贡献的能力。在这方面，能力建设应是可持续的，有明确的目的，符合国内需要，并满足这一专门领域人力资源开发的目标。还应考虑建立一个供资机制，以支持为实施网络犯罪公约进行能力建设。

[7] A/70/174。

日本

[原文：英文]
[2021 年 10 月 29 日]

日本作为一个重视为起草即将出台的联合国网络犯罪公约而实现包容、透明和公平的进程的会员国，很高兴在正式起草开始之前为新公约提供投入，并赞赏主席主动提供这一机会。

虽然不同国家面临不同的网络犯罪挑战，但日本认识到，网络犯罪是对所有会员国的不断演变的共同严重威胁。为了打击容易超越国界的网络犯罪，必须确保所有会员国相互合作。因此，日本认为，我们应力求确保自由、公平和安全的网络空间，并通过使新的国际公约的实质内容具有普遍性并为所有会员国所接受，加强我们在全世界预防和打击网络犯罪的能力。

这些意见概述了日本对新公约的范围、目标和结构的看法，以促进根据大会第 74/247 号决议设立的拟订打击为犯罪目的使用信息和通信技术全面国际公约特设委员会内的讨论。

范围

为了加强打击网络犯罪的全球措施并创建一个普遍的国际框架，国际社会首先应制定一个坚实的框架，重点是关于刑事犯罪和刑事程序的基本和必要规定，以及这一领域的司法协助和其他国际合作。

被新公约定为犯罪的行为应限于网络犯罪；新公约确立的犯罪应首先涵盖网络依赖性犯罪，只有在必要且会员国达成广泛共识的情况下，才应涵盖网络使能的犯罪。

新公约应坚定地以现有打击网络犯罪框架下以往和当前的讨论为基础，同时考虑到涉及网络犯罪讨论的其他论坛的讨论和工作，以避免重复或损害工作。

为了建立一个普遍适用于信息和通信技术的各种使用的国际框架，而不论国家之间的差异，并对技术的未来发展作出反应，新公约的条款应以技术中立的方式拟订。

尽管打击网络犯罪很重要，但打击网络犯罪的措施不得损害正当程序原则或对人权施加不合理的限制。这种保障是国际合作成功的先决条件，因此，新公约应包括确保正当程序和人权的具体规定。

目标

新公约的主要目标应是促进应受保护的信息和通信技术所涉每个人的安全和保障，并保护他们的利益。要做到这一点，可以在全球加强打击网络犯罪的措施，创建一个最广泛适用于各种跨国形式的网络犯罪的普遍国际框架，并支持在刑事调查和起诉方面开展有效的双边或多边合作。

为了实现这一目标，新公约应规定可由尽可能多的会员国遵守和执行的基本和必要规定，从而提高全世界的打击网络犯罪措施水平，并加强现有框架。

结构

日本认为，以下基本结构将有效地组织新的公约，但支持在即将举行的谈判中对更详细的结构采取灵活态度：

(a) 术语定义；

(b) 会员国应采取的国内措施清单：

㈠ 刑事定罪：

a 归类为网络依赖性犯罪的罪行；

b 在网络使能的犯罪中应定为刑事犯罪的罪行；

㈡ 关于保全、披露和制作数据的程序规定；

㈢ 保障人权和其他利益的保障措施；

(c) 引渡、司法协助和其他形式合作方面的国际合作；

(d) 最后条款。

约旦

[原文：阿拉伯文]
[2021 年 10 月 28 日]

范围

公约应涵盖与以下方面有关的犯罪：

- 电子服务的机密性、完整性和可用性。
- 未经授权访问信息网络、信息系统或其任何部分。
- 扰乱关键基础设施。
- 蓄意破坏信息网络或信息系统。
- 暗中监视信息网络或信息系统上的数据流。
- 诈骗、伪造和冒充。
- 拦截金融系统数据或信息。
- 侵犯隐私和知识产权。
- 硬件、解密软件和访问码。
- 互联网地址诈骗。

- 色情。
- 剥削和虐待儿童。
- 传播虚假消息。
- 种族歧视。
- 剥削和虐待妇女。
- 煽动叛乱、煽动或传播仇恨言论。
- 通过信息网络或网站进行非法贩运。
- 传播、支持或宣传恐怖主义意识形态。
- 为恐怖主义目的使用信息和通信技术。
- 侮辱宗教、国家和象征。
- 供应链。
- 勒索软件。
- 电子钓鱼。
- 软件盗版。
- 服务提供者未经授权使用数据。

目标

该公约的目标应是：

- 加强国际合作与协调，打击为犯罪目的使用信通技术。
- 制定国际立法，打击为犯罪目的使用信通技术。
- 强调通过打击为犯罪目的使用信通技术来保护关键基础设施的重要性。
- 宣传建设和提高国家和国际能力的重要性，并提高个人和社会对打击为犯罪目的使用信通技术的认识水平。

结构

- 导言。
- 定义。
- 目标。
- 范围。
- 义务和责任。
- 国际合作。

- 能力建设和提高认识。
- 执行机制。
- 根据事态发展对公约不断进行更新。

公约的范围应广泛，涵盖世界上尽可能多的国家，重点是作为主要技术孵化器的国家。

它应包括关于针对人员或资金的信息技术犯罪的商定国际概念。

重点应是创造各种方式，使缔约国执法机关能够相互分享信息，并根据国家立法和尊重隐私，创建追踪电子诈骗犯罪所得资金和查明此类犯罪的行为人数字身份的机制。

应在缔约国之间建立常设联络点，对恐怖主义或对儿童的性剥削等案件立即作出反应。还有必要创建机制，促进与国际社交媒体公司的合作，以提供打击这类犯罪所需的技术信息。

应通过培训班、讲习班和交流经验，促进国际合作，建设缔约国打击网络犯罪机构的工作人员的能力。

科威特

[原文：阿拉伯文]
[2021 年 9 月 17 日]

1. 公约草案的总体主要表述应强调，公约旨在增进和加强合作，以打击和减少基于各国主权平等和不干涉其内政的信息技术犯罪的风险，包括与行使管辖权、尊重法治、维护公共秩序和安全以及尊重社会价值观有关的程序。

2. 公约的范围应考虑到防止恐怖主义行为的国际文书和《联合国打击跨国有组织犯罪公约》及其各项议定书，以包括在一个以上国家实施的犯罪、在其他国家筹备、计划、指挥或监督的犯罪、在其他国家实施的犯罪、或在一国实施但在另一国造成严重后果的罪行。

3. 应根据缔约国国家立法中被定义为上游犯罪的新出现的与信通技术有关的犯罪形式，确定将在公约下定罪的行为，特别注意与内容、仇恨言论和暴力有关的犯罪。

4. 应为以下方面建立框架：法律和司法合作，引渡罪犯，交流信息，允许在缔约国认为披露信息有助于对犯罪展开调查的情况下不经事先请求提供信息，就紧急披露和保全利用信息技术储存的信息进行合作，获得跨境信息技术，在实时收集流量数据方面的双边合作和援助，创建保密要素，以及对作为互助主题的数据的使用的限制。

5. 还应根据缔约国适用的机制建立评估该公约执行情况的框架。应指定缔约国的相关机构和联络点，并应努力利用联合国毒品和犯罪问题办公室内的现有信息网络。

列支敦士登

[原文：英文]
[2021 年 10 月 28 日]

列支敦士登谨感谢拟订打击为犯罪目的使用信息和通信技术全面国际公约特设委员会秘书处和主席阁下 Faouzia Boumaiza 女士征求会员国对新公约的范围、目标和结构（要素）的意见。列支敦士登的一般立场如下。

列支敦士登的一个主要目标是确保新的网络犯罪公约符合现有的国际和区域文书，包括《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》，并以包括人权法在内的国际法为基础。

因此，列支敦士登的目标是制定一项简短、实用的公约，重点关注网络空间特有的犯罪，如非法访问和存取、非法拦截、干扰数据、干扰系统、滥用设备、与计算机有关的伪造、与计算机有关的诈骗以及与侵犯著作权和儿童色情有关的犯罪。对网络空间具体犯罪领域以外的其他类型犯罪的深远定罪应由其他公约和论坛涵盖，因此应予以拒绝。此外，列支敦士登反对重复其他特定条约所涵盖的犯罪。

由于网络空间环境迅速变化，列支敦士登为拟订一项使用技术中性措辞的公约作出努力，以便实质性刑事犯罪可适用于当前和未来所涉技术。具体类型网络犯罪的广泛技术定义今后可能过时，因此应在公约中避免。

列支敦士登认为，另一个核心方面是数据保护规定和人权，这必须在公约中占有重要地位。数据保护和人权标准必须得到充分尊重。

列支敦士登将在新的网络犯罪公约的谈判期间提出更详细的立场。

墨西哥

[原文：英文]
[2021 年 10 月 21 日]

对墨西哥政府来说，信息和电信技术、数字平台和网络环境为加强发展、缩小不平等差距和促进包容、福祉、正义和权利提供了巨大的机会。

然而，墨西哥认识到，通过这些技术实施犯罪和带来非法市场增长是各国政府、企业、民间社会组织和所有个人日益关切的问题。

现在比以往任何时候都更需要国际合作以及法律协助和信息交流机制。墨西哥致力于多边主义，特别是联合国在对这一全球挑战作出全面和有意义的反应方面的作用。

墨西哥认为，大会授权拟订一项关于打击为犯罪目的使用信息技术的全面公约，是实现一种实质性、坚定、多元、包容和透明的进程的理想机会，这一进程借鉴从与该专题有关的联合国其他进程以及从其他相关区域经验吸取的经验教训。

墨西哥政府希望，以下几点将指导拟订和确定未来公约内容的进程。

公约的方法、范围和类型

该公约应是一项全面、具有约束力的法律文书，涵盖实质性和程序性事项，旨在创建一个国际合作和分享信息、经验、专门知识和最佳做法的框架。

希望公约将有助于促进标准，以改进调查、减轻和起诉，虽然公约不排除缔结关于同一主题的其他国际文书，但它将成为统一框架的基准，使对网络犯罪的起诉更加有效。

它应包括以下内容：

- 一般定义、基本类型和称职的行为者。
- 各国应有适当调查和起诉网络犯罪罪行的基本程序措施。
- 应由国家立法者审议的一般刑事犯罪。
- 获取信息和促进有效合作的机制。

未来的公约还应当对提出保留和解释性声明作出规定，并对灵活的修正程序作出规定，以促进其更新，并建立解决争端的机制。最好是以交存 50 份批准书为生效条件。

一旦确定了公约的内容，最好商定一个以同行审议为基础、不给各国造成负担的有效、普遍的执行情况审查机制。

与其他国际文书的相关性

墨西哥政府认为，该公约必须以确认国际法适用于网络空间为基础，因此，应考虑到以下现有国际法律文书：

- 《联合国打击跨国有组织犯罪公约》及其三项议定书。
- 《国际法院规约》。
- 《欧洲委员会网络犯罪公约》。
- 关于个人数据保护和跨境流动的条约。
- 国际人权条约和保障对司法程序所涉人员的保证的条约。
- 适用于知识产权的条约。
- 关于引渡、刑事事项司法协助和其他形式国际法律合作的双边条约。

此外，谈判进程可有益地以联合国和其他有关国际论坛通过的文件为指导，主要是以下文件：

- 全面研究网络犯罪问题专家组 2018 年、2019 年和 2020 年会议产生的结论和建议汇编。
- 2019-2021 年推进网络空间负责任国家行为政府专家组的最后报告以及 2013 年和 2015 年的前两份报告。

- 从国际安全角度看信息和电信领域发展不限成员名额工作组的最后报告。
- 国际电信联盟制定的《全球网络安全议程》利用准则草案。
- 大会关于数字时代隐私权的决议。
- 人权理事会关于在互联网上增进、保护和享有人权的决议。

应予处理的网络犯罪罪行/犯罪行为

墨西哥政府认为，该公约应着重于被国际法确认为非法（根据在联合国框架内通过的其他条约的规定）并且是通过电子手段进行的行为。

虽然预计公约不会包括一个详尽的犯罪目录，也不会所有类型都符合不同的法律制度，但起草过程最好产生对话，作为以下方面的一般参考点：

- 识别盗窃和网络钓鱼。
- 诈骗和敲诈。
- 使用勒索软件。
- 恶意软件和与恶意代码的制作、存储、散播、销售和执行有关的犯罪行为。
- 暴露个人或机构信息，损害其所有者。
- 与贩运人口、儿童色情和侵犯性隐私有关的罪行。
- 诱骗和网络欺凌。
- 数字暴力，包括基于性别的暴力和基于仇恨、种族、国籍、宗教或政治敌意的暴力。
- 攻击方法（网络钓鱼、语音钓鱼、短信诈骗、域名欺骗）。
- 侵犯国家主权的罪行，如恐怖主义、破坏、间谍活动和侵入载有因国家安全原因而分类的信息的系统。
- 针对关键信息基础设施以及信息的机密性、完整性和可用性的犯罪行为。
- 侵害儿童和青少年的罪行。
- 侵犯表达自由。
- 侵犯知识产权的罪行。
- 危害金融系统的罪行。
- 非法销售武器、动物、受管制药品和系非注册保健品的药品。
- 伪造货币和伪造公文。
- 将加密货币和两用资产用于犯罪目的。

- 非法修改门户网站（毁损）。
- 法人的责任。

在起草公约时，还应讨论是否可能规定对未遂行为的惩罚和确立需予更严厉惩罚的加重情节。

与主权和管辖权有关的方面

- 重申尊重国家主权和不干涉他国内政的原则。
- 借鉴其他法律文书和程序中的类似规定，制定确定管辖权的一般规则。
- 制定获取流量和内容数据的共同措施，同时防止非法阻断或拦截数据。
- 制定在获取、保留、保全和提交数字证据方面创建确定性的机制。
- 明确传票或逮捕等调查步骤。
- 制定关于在刑事调查中提交技术和内容数据以及迅速披露计算机数据的规定。
- 规定技术运营者、服务提供者和互联网内容提供者，无论其实际所处位置如何，都有在调查期间向主管机关提供信息的法律义务。

与信息共享和国际合作有关的方面

墨西哥政府认为，该公约的主要目标之一应是在信息共享和国际合作方面创建确定性，并创建有效执行公约的进程。希望除其他方面外处理以下问题：

- 司法协助。
- 引渡。
- 为调查和情报目的请求、回应、接收和交流信息的共同机制。
- 能够在调查期间进行迅速有效合作的司法监督程序。
- 合作进行警方调查和获取供司法程序使用的证词，同时考虑使用信息和通信技术。
- 制定预防和侦查网络犯罪行为的准则、标准、方法和最佳做法。
- 促进国家计算机应急小组或计算机安全事件应对小组在预防网络犯罪方面的合作。
- 协调调查。
- 建议一个透明度和信息保护的最低限度共同框架，以便无论每个国家的国家政策如何不同，都可以分享调查和司法程序的数据。
- 规定保留数据和保全数字证据的最低时限。

- 建议拦截私人通信和实时地理定位应遵守的规则和条件。
- 建立遵守和监管隐私政策的一般参数。
- 促进地方、区域和全球统计的统一。

与保护和行使人权有关的方面

根据未来公约执行的所有措施都应符合国际人权文书规定的义务。预计其规定也将符合与表达自由有关的标准。

墨西哥政府希望在拟订该公约的过程中处理以下问题：

- 与营商和人权有关的概念和事态发展。
- 强调调查、起诉和惩处通过互联网侵害儿童和青少年的性别暴力和犯罪行为。
- 鼓励调查、起诉和惩处煽动暴力或旨在造成排斥或隔离的种族主义行为。
- 网络中立的最低共同要素。
- 关于互联网服务公司保护信息机制的建议。

与能力建设和技术援助有关的要素

墨西哥政府认为，为了有效实施未来的公约，有必要制定促进预防和起诉网络犯罪方面的能力建设的条款。最好是：

- 鼓励致力于培训、技术援助和最佳做法，以及进行计算机取证和获取有效数字证据的标准化程序。
- 促进以预防为导向的教育倡议和可推广的提高公众认识运动。
- 还鼓励在金融、教育、贸易和能源等各部门建立或加强计算机应急小组。
- 制定促进采用最佳做法的指南、准则和建议。
- 扩大针对以下不同利益攸关方的培训活动范围：调查人员、检察官、法官、外交官、立法者和非国家行为体。

与相关非国家行为体（民间社会、私营部门、学术界）的参与有关的方面

墨西哥政府认为，不妨通过起草进程探讨促进民间社会组织、私营部门、服务提供者、学术界和研究中心参与和提供投入的机制。最好考虑以下几点：

- 可能让这些行为体参与旨在预防和打击网络犯罪的进程。
- 促进与私人计算机应急小组、运营商和各种电信公司的协作环境。

- 与经营关键信息基础设施或在战略部门工作的私营企业以及提供电子邮件、即时通讯、微博和在线运输服务等免费互联网服务的公司进行对话。

支持自我监管和社会意识，促进营商与人权的概念。

新西兰

[原文：英文]
[2021 年 10 月 29 日]

在执行大会第 74/247 号和第 75/282 号决议方面，新西兰高兴地响应拟订打击为犯罪目的使用信息和通信技术全面国际公约特设委员会主席邀请会员国就新公约的范围、目标和结构提出意见。新西兰欢迎有机会分享其观点，并期待着其他国家的贡献，并在我们以透明、包容的方式共同努力拟订一项新的公约时讨论前进的道路。

网络犯罪是一个跨界挑战。因此，植根于包容性和多利益攸关方办法的全球合作是确保国际社会能够有效应对这一日益严重的威胁的唯一途径。在网络犯罪相关问题上的国际合作需要一致、有效的网络犯罪法律，以便能够调查和起诉跨境网络犯罪。促进这种合作从未如此重要。随着工作、研究和社交互动转移到网上，包括在 2019 冠状病毒病（COVID-19）大流行期间，网络犯罪分子的机会领域扩大了，我们看到网络犯罪事件的频率和严重程度都有所增加。

关于网络犯罪的国际合作对小岛屿发展中国家尤其重要，这些国家必须能够有意义地参与特设委员会的工作。新西兰致力于确保太平洋岛屿国家能够有意义地参与特设委员会的工作。我们支持以混合（亲身和在线）方式参加特设委员会届会，并强调必须让较小代表团有充分的准备和参与时间。

范围

新的网络犯罪公约必须与现有文书相辅相成而不是相冲突。所有会员国都同意，国际法适用于网络空间，这意味着这项新公约不会存在于真空中。如果它补充和加强现有文书和现行法律制度，其中包括《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》等处理网络犯罪的工具，将是最有效的。这符合大会第 74/247 号决议所载的任务，大会在该决议中呼吁特设委员会的工作充分考虑到国家、区域和国际各级的现有国际文书和努力。

新西兰认为，制定的任何文书都必须保护人权，维护由多个利益攸关方管理的自由和开放的网络空间。因此，该网络犯罪公约必须符合各国保护和尊重网上人权的义务，包括表达自由权和隐私不受任意和非法干涉的权利。打击网络犯罪的措施必须符合国际人权法。

该条约应明确侧重于核心网络犯罪问题，以便有效加强合作，应对这些问题对个人、行业和政府构成的威胁。我们认为，只有在利用信息和通信技术扩大犯罪范围、速度和规模的情况下，条约才应涵盖网络依赖性犯罪以及网络使

能的犯罪。我们认为这类犯罪有两种明显的候选案：网上儿童性剥削和性虐待，以及网络促成的诈骗和盗窃，包括勒索软件。

新西兰认为，对于其他法律文书所涵盖的犯罪，如腐败、贩运或恐怖主义，没有必要仅仅因为这些犯罪可能是使用信息和通信技术进行的而予以重复涵盖。这种做法有矛盾和混乱的风险，不会产生一个提高我们处理网络犯罪的集体能力的有针对性的实用文书。

这一进程的任务明确规定，我们应侧重于制定一项刑事司法文书，通过国家执法机构采取的行动改进对网络犯罪的国际对策。这需要界定和制裁网络空间的犯罪行为，并要求各国实施适当的程序和立法工具，使各机构能够查阅和分享数字证据，以有效瓦解和制裁网络空间的犯罪行为。它不要求界定网上非犯罪行为的规范。我们认为，值得学习其他成功的刑事司法条约，这些条约侧重于核心刑事问题，以及作出广泛的国际合作规定和支持所有会员国的能力建设。

最终公约的措辞必须切实可行、技术中立和尽可能适应未来，以确保它经得起时间的考验，不需要不断修订。这意味着我们需要关注活动，而不是用于进行该活动的特定形式或方法。

现阶段确定公约执行机制可能需要什么还为时过早。有多种模式可供考虑，但在更明确地界定文书的范围及其目标之前，可以搁置条约的这一方面。

目标

新文书的主要目的应当是为各国之间的合作与协调建立一个统一、现代和有效的全球框架，以应对网络犯罪对个人、企业、关键基础设施和政府构成的日益严重的威胁。它应包括提供支持和技术援助，使所有国家能够发展应对这些挑战的能力。这将提高各国在国家、区域和国际各级有效应对网络犯罪的能力。

这意味着条约需要支持国家执法、检察和司法机构在预防、调查和起诉条约所列罪行方面的双边或多边合作。这对于打击网络犯罪至关重要，因为由于其跨界性质，网络犯罪往往涉及多个法域的犯罪者和受害者。就网络空间中什么构成刑事犯罪以及哪些犯罪应在国内司法管辖区受到惩罚达成共识，将有助于促进这一点，特别是如果辅之以与国际伙伴获取和分享数字证据的一致框架，并提供适当的保障措施。

使用调查和起诉条约规定的罪行的权力必须遵守现有国际条约规定的与人权和基本自由有关的有效保障措施。还必须有保障措施来确保公平和适当地使用相互合作权力，并允许各国在不符合某些标准时拒绝合作。此外，新西兰认为，条约必须承认国家执法和检察机构的独立性，是否采取行动的决定完全由各会员国的这些机构决定。

有效的国际合作最好通过一项得到广泛支持的条约来实现。新西兰认为，这要求条约谈判具有包容性和透明度，尽最大努力达成共识，以确保公约获得尽可能最强有力的授权。所有会员国都应能够交流意见，并在民间社会、业界和其他相关利益攸关方的专门知识和观点的支持下，有意义地参与谈判。应纳

入土著人民，包括新西兰奥特亚罗瓦的毛利人以及其他少数群体的观点，以及网络犯罪和打击网络犯罪的努力对这些群体的潜在影响。

打击网络犯罪的国际合作并未如其可达到的那样有效。这不是因为会员国缺乏意愿，而是因为缺乏能力或专门知识。对执法机构的技术援助和能力建设是一项关键要求，公约需要支持全球范围的能力发展。

结构

我们期待着通过这一进程并在 2022 年 1 月的第一次谈判会议上听取其他国家对公约范围和目标的看法。在此之后，我们预计将迅速出现结构方面的明确前进道路。

尼日利亚

[原文：英文]
[2021 年 11 月 5 日]

尼日利亚认为，为了有效应对快速演变的网络犯罪威胁，迫切需要界定和制裁网络空间的犯罪行为，提高跨国警务能力的协同作用，改进程序工具，改革和（或）加强国际合作，同时尊重人权。因此，拟订关于这一主题事项的联合国公约目前必须侧重于打击网络犯罪，而不是试图涵盖网络安全和其他与网络有关的事项，因为这些事项在政治上不稳定，在其他联合国论坛上得到更好的处理。新公约的谈判必须是一个透明、包容和推动达成协商一致的进程，使由此产生的公约得到更广泛的接受和（或）通过。

范围

新的网络犯罪公约应创建一个打击网络犯罪的法律和体制框架，其中包括以下要素：

(a) 实质性网络犯罪罪行的刑事定罪：界定并规定对网络依赖性犯罪（即计算机或数据成为犯罪活动目标的犯罪）和某些网络使能的犯罪以及清洗网络犯罪所得行为的制裁；

(b) 为调查和起诉已确立的网络犯罪罪行以及为获取和分享其他刑事犯罪的电子证据提供程序性权力；

(c) 关于可持续能力建设和技术援助的规定或措施；

(d) 关于网络犯罪所得的追回及归还的规定或措施；

(e) 关于改进执法机构与私营部门之间合作与协调的规定或措施；

(f) 加强与上述事项有关的国际合作的规定或措施，包括与互联网服务提供者直接合作；以及

(g) 预防网络犯罪和提高认识的规定或措施，包括与民间社会组织、私营部门、服务提供者、学术界和研究中心合作。

目标

新公约应着眼于以下目标：

(a) 对实质性刑事犯罪罪行、程序性权力和国际合作打击网络犯罪的既定基线有共同的理解；

(b) 促进以技术中立的方式对罪行进行刑事定罪，以确保实质性刑事条款不仅涉及当今的技术和犯罪手段，而且涉及未来的技术和手段；

(c) 按照适当程序和保护人权和基本自由，建立收集、获取和分享网络犯罪和其他犯罪的电子证据的权力和能力；

(d) 促进和便利在打击网络犯罪方面的国际合作，消除网络犯罪行为者的安全庇护所；

(e) 促进能力建设和技术援助，以加强执法机关处理网络犯罪的能力，并利用国际刑事警察组织（国际刑警组织）数据库等现有机构能力；

(f) 促进会员国利用已经证明在打击网络犯罪方面有用的多边文书，如《欧洲委员会网络犯罪公约》，以及与预防犯罪和刑事司法领域现有联合国条约的联系，尤其是《联合国打击跨国有组织犯罪公约》和《联合国反腐败公约》；

(g) 促进从业人员一级的政府间和多利益攸关方可信信息共享进程，以确定未来的网络犯罪趋势、威胁和缓解措施；以及

(h) 建立一个机制，以监测和（或）促进有效使用和实施公约、交流信息和审议任何审查报告和（或）今后的修正。

结构

除了序言、明确的定义和适当的最后规定外，认为重要的是，以下要素构成新公约结构的一部分：

(a) 总则和（或）目标及其适用；

(b) 类似于《有组织犯罪公约》和《反腐败公约》所载的预防网络犯罪措施，例如关于提高认识和教育举措的规定；

(c) 实质性网络犯罪罪行和处罚；

(d) 程序法规定和一般调查权；

(e) 确保执法活动符合国际人权的保障措施；

(f) 开展打击网络犯罪的国际合作，包括开展正式和非正式国际合作，以发现、调查和起诉网络犯罪，以及获取其他刑事犯罪罪行的电子证据；

(g) 关于能力建设和技术援助的规定，以提高从业人员的技能并加强应对网络犯罪的能力；

(h) 规定从业人员一级多利益攸关方合作，以便与相关利益攸关方可信地分享信息和经验；

(i) 规定建立一个机制以监测和（或）促进有效使用和实施公约、交流信息和审议任何审查报告和（或）今后的修正。

挪威

[原文：英文]
[2021 年 11 月 3 日]

在执行大会第 74/247 号和第 75/282 号决议方面，挪威王国政府高兴地响应关于请会员国就新的打击为犯罪目的使用信息和通信技术公约的范围、目标和结构提出意见的邀请。国际合作是应对不断发展的网络犯罪威胁的关键，挪威政府期待着参加关于这一事项的全面公约的谈判。

范围

大会在第 74/247 号决议中决定设立一个代表所有区域的不限成员名额特设政府间专家委员会，以拟订一项关于打击为犯罪目的使用信息和通信技术行为的全面国际公约。由于该决议明确针对犯罪行为，对核心网络犯罪罪行的刑事定罪应成为该公约的一个核心部分。

有关网络安全和网络治理的问题不属于大会赋予的任务范围，不应成为该公约的专题。这些事项须由联合国其他论坛和进程处理。试图列入关于网络安全和网络治理的规定将使创建一个吸引广泛支持的文书变得更加困难。

几十年来，网络犯罪一直是一个挑战，犯罪者往往领先国家执法机构一步，这是一个持续存在的问题。明天的网络犯罪与今天的网络犯罪不同，正在进行的数字革命给国际社会带来了一项艰巨的任务。在这方面，最重要的是努力列入一份经得起时间考验的最新和现代的犯罪目录。

尽管网络犯罪每天都在发展，但国家和国际机构设法查明了核心的、反复出现的行为类型。今天，许多会员国已经将这些犯罪定为刑事犯罪。在这方面，挪威王国政府建议至少考虑以下依赖网络和网络使能的犯罪：

(a) 非法访问，即未经授权访问计算机或计算机系统；

(b) 非法拦截，即实时非法拦截通信内容或与通信相关的流量数据；

(c) 干扰数据或系统，即恶意软件、拒绝服务攻击、勒索软件以及数据删除或修改；

(d) 滥用设备，即贩运或使用允许获取资源的信用数据、密码和个人信息；

(e) 与儿童性虐待材料有关的犯罪；

(f) 与计算机辅助诈骗有关的犯罪，即操纵计算机系统或数据用于诈骗目的，如网络钓鱼、损害营商电子邮件和拍卖诈骗；

(g) 与侵犯著作权及相关权利有关的犯罪；

公约还应包括关于未遂、协助、教唆和共谋、网络犯罪所得的洗钱以及公司和其他法人的责任的规定。

由于网络犯罪不断发展，拟订打击为犯罪目的使用信息和通信技术全面国际公约特设委员会必须侧重于国家执法机构的最新报告以及区域和国际组织的同等报告。联合国毒品和犯罪问题办公室关于网络犯罪的全面研究很重要。挪威王国政府还谨提请注意欧洲联盟执法合作署（欧警署）一年一度的《互联网有组织犯罪威胁评估》，这是关于主要类型网络犯罪的一个重要信息来源。

除了关于刑事定罪的规定外，公约还应包括关于程序权威的规定，特别是关于收集和分享电子证据的规定。这些规定必须符合正当程序和保护人权和基本自由。

应对现代网络犯罪的挑战，公约应要求会员国列入专门针对电子证据的国内规定，例如关于在严重犯罪案件中快速保全所存储的计算机数据、搜索和扣押所存储的计算机数据以及实时收集计算机流量数据和内容数据的规则。此外，公约应允许开展合作，收集和获取任何类型犯罪的电子证据，而不仅仅是网络犯罪。

特设委员会尤其应审议关于在所谓的“云”中获取电子证据的规定。在过去十年中，在云中存储计算机数据一直是国家执法机构面临的一个经常性挑战，这特别是由于与管辖权有关的问题和对其他国家的依赖。因此，一项现代和最新的网络犯罪公约应反映会员国如何合作确保其他国家通过云存储的证据。

公约还有必要包括关于国际合作的规定。在这方面，特设委员会应借鉴现有条约的经验，特别是《联合国打击跨国有组织犯罪公约》和《联合国反腐败公约》。应当考虑到关于引渡和互助的规定。

公约还必须反映会员国遵守所建议的规定的不同能力，特别是关于技术基础设施和能力的规定。因此，公约应创建能力建设工具，并为会员国寻求这种援助提供渠道。

最后，公约应涉及公民、企业、组织和其他利益攸关方如何与政府合作以保护自己和社区免遭网络犯罪。尽管网络安全不属于公约的范围，但预防网络犯罪自然具有相关性，应予以考虑。

目标

特设委员会应力求制定一项强有力的公约，其中要求会员国通过国家立法，改进全球的网络犯罪预防和处理。关于对某些类型网络犯罪进行刑事定罪的国内规定以及关于程序权威和国际合作的规定将特别重要。

即将开展的起草进程的一个目标应当是制定一项经得起时间考验、跟得上所有现代形式的网络犯罪以及最有可能出现的趋势的文书。此外，目标还应当是起草一项能够充分应对核心网络犯罪挑战的雄心勃勃的文书。与此同时，以协商一致为基础的办法至关重要。

挪威王国政府还谨重申，必须保持一个开放、包容、透明和多利益攸关方的进程，使所有会员国能够真诚地谈判达成知情和切合实际的解决办法，我们认为，这是确保广泛加入新公约的关键。

结构

考虑到该公约的拟议范围和目标，公约的主要部分已予确定。然而，特设委员会和会员国对公约的结构持开放态度将是富有成果的。尽管关于刑事定罪、程序权威和国际合作的规定应构成公约的核心部分，但其他事项也可能影响最终结构。挪威王国政府建议对公约的结构采取开放的办法。

人权

国际人权法适用于网络活动，就像它适用于任何其他活动一样。各国必须遵守其在网络空间的人权义务，就像其在现实世界中必须遵守的那样。各国必须尊重和保护人权，包括表达自由权和隐私权，以及其他相关的数据保护原则。

不言而喻，《公民权利和政治权利国际公约》所载的人权标准需要为任何关于网络犯罪的新规定建立一个重要的框架。无论如何，挪威王国政府愿重申人权在即将到来的谈判中的重要性，特别是关于要求程序权威方面国家立法的规定。

阿曼

[原文：阿拉伯文]
[2021 年 10 月 18 日]

将民用设施——特别是重要的基础设施，包括电力和供水网络、金融机构和运输部门——作为侵犯目标的行为应被定为犯罪。这种设施不应变成国家间冲突和解决争执的场所。

巴拿马

[原文：西班牙文]
[2021 年 10 月 28 日]

技术的不断发展使各国有必要采取机制预防和打击新形式的犯罪。COVID-19 大流行加剧了一个已经越来越明显的问题：我们没有为打击网络犯罪和通过技术手段实施的犯罪做好充分准备。

要为这场战斗做好准备，就需要除其他外认识到，对网络犯罪和通过数字手段实施的犯罪的调查不能脱离该专题的国际层面。所有国家都受到那些在跨国主义中找到实现其目标和逃避责任的沃土的人的犯罪活动的影响。

鉴于上述考虑，关于打击为犯罪目的使用信息和通信技术的全面国际公约应成为便利各国调查此类犯罪的工具。为此，重要的是，该公约不仅应涵盖直

接影响信息、计算机系统和技术本身的行为，而且还应涵盖通过技术手段实施的行为，而不论有关的受法律保护的权利如何。

我们认为，鉴于信息的波动性，这一新工具应制定措施改进国家间正式和非正式沟通的制度，以便进行更有效的调查。

根据加强的通信系统，应处理界定扣押数据和通信、保全数据和处理电子证据等调查措施的法律概念。

虽然我们意识到在某些问题上可能存在相互冲突的立场，但目标仍然是一样的：制定一项有助于打击为犯罪目的使用信息和通信技术行为的文书。

俄罗斯联邦

秘书处的说明：俄罗斯联邦的提交件载于题为“2021 年 7 月 30 日俄罗斯联邦驻联合国临时代办给秘书长的信”的 A/75/980 号文件，以及载于该信的题为“联合国打击为犯罪目的使用信息和通信技术公约草案”的附件，该提交件已提供给大会第七十五届会议。应特设委员会主席的邀请，该提交件将转交拟订打击为犯罪目的使用信息和通信技术全面国际公约特设委员会，作为会员国就新公约的范围、目标和结构（要素）提交意见的一部分。

瑞士

[原文：英文]
[2021 年 10 月 28 日]

信息和通信技术（信通技术）对我们的社会产生了深刻影响，为社会、文化和经济各级的发展提供了机会，但也为在网络空间进行的具有犯罪目的的活动提供了基础。随着我们的世界日益数字化，网络犯罪也在增加。大会通过第 74/247 号决议设立了一个拟订一项打击为犯罪目的使用信息和通信技术全面国际公约的不限成员名额特设政府间委员会。本答复概述瑞士对该文书的目标、范围和结构的看法。

目标

瑞士认为，一项关于打击为犯罪目的使用信通技术的联合国公约的总体目标是保护信通技术用户，使他们能够自由使用信通技术并享受其好处。信通技术的全球和开放性质确实是加快在实现社会和经济发展方面取得进展的推动力。因此，公约的目标是用户的安全，这不应妨碍他们使用信通技术的自由。用户必须能够在网上行使其人权和基本自由，从而充散播挥包容性数字化世界的潜力。因此，公约应在确保自由、可信和安全的信通技术方面更进一步。

一项联合国公约可以帮助我们实现这一总体目标。为此，公约应规定在打击网络犯罪方面采取协调一致的办法。由于信通技术固有的跨国性质，网络犯罪很可能涉及处于多个国家的犯罪者和受害者。因此，国际合作是确保防止网络犯罪的最佳保护水平的关键。公约应旨在就什么构成信通技术方面的刑事犯罪罪行以及哪些罪行应根据国家法律受到惩罚达成共同理解。这种共同理解是

促成任何类型的合作的第一块基石。在这一共同理解和词汇的基础上，公约应旨在创建有效国际合作的框架，以保护信通技术用户并为网络犯罪受害者伸张正义。

只有通过包容性进程，才能在全球一级采取协调一致的办法打击网络犯罪。所有会员国都应能够进行有意义的参与；它们应有机会在拟订打击为犯罪目的使用信息和通信技术全面国际公约特设委员会实质性会议期间就公约提出自己的意见，并讨论其他国家提出的意见。特设委员会应尽可能争取达成共识。

网络犯罪是跨国的，但也必然涉及非国家行为体。如果我们想要一项适合目的的公约，就需要在拟订过程中听到每一个声音。让所有利益攸关方，包括相关的非政府组织、民间社会组织、学术机构和私营部门，参与拟订工作的每一个协调步骤，是确保公约能够实现其目标的关键。[8]

范围

国际法适用于网络空间。未来的公约不会存在于真空中，也不会使以前的国际协定失去其意义。瑞士深信，该公约必须创建在现行法律制度的基础上，并应加强现行法律制度。它的设计应补充国际社会已经采取的举措，并依靠协同作用有效应对网络犯罪。

由于公约将是一项刑法条约，它应以国际刑法为基础并尊重国际刑法。处理网络犯罪问题的全球工具已经存在。与《联合国打击跨国有组织犯罪公约》一样，《欧洲委员会网络犯罪公约》是包括瑞士在内的全球各国实现网络犯罪法律现代化的标准，也是互联网时代国际合作的重要基线。一项联合国公约应以这一经验为基础。特设委员会的工作应以其他小组和论坛的工作为指导，包括全面研究网络犯罪问题专家组的工作。

公约必须充分反映、保障和加强人权法。由于网络犯罪对个人人权构成威胁，应对网络犯罪的努力需要保护而不是损害这些权利。个人在线下拥有的同样权利也必须在线上得到保护。为打击网络犯罪而采取的措施必须符合国际人权法。

结构

瑞士认为，使上述目标具体化的一个有希望和有效的办法是遵循在联合国范围内谈判达成的现有国际刑法文书的结构。因此，公约的结构可安排如下：

(a) 总则；

(b) 预防措施；

(c) 定罪和执法；

(d) 国际合作；

[8] 根据大会第 75/282 号决议第 9 至 10 段。

(e) 技术援助和信息交流；

(f) 执行机制；

(g) 最后条款。

瑞士认为，没有必要仅仅因为可能（也是）通过信通技术实施的而重复特定条约已经涵盖的罪行（例如腐败、贩运和恐怖主义）。相反，公约应侧重于特定于网络空间的犯罪。广泛列举的罪行即使都可能是通过计算机系统实施的，也会带来相矛盾的风险，应予以避免。

与内容有关的罪行应保持在最低限度，并应始终根据其附加值予以评估。

瑞士强调程序保障具有必要性和重要性，可确保诉讼的合法性和公正性以及受影响者的权利，特别是在司法协助、信息交流和根据有关国家规定的条件进行引渡方面。必须充分保障隐私权。必须确保充分保护个人数据。

必须考虑和实行适当的条件和保障措施，特别是在维护和加强人权方面，包括不歧视原则。

土耳其

[原文：英文]
[2021 年 11 月 4 日]

土耳其极为重视在世界各地自由、公开和安全地使用信息和通信技术。

信息和通信技术的发展增加了为犯罪目的滥用这些技术的风险。消除对关键基础设施安全以及基本权利和自由的这些风险和威胁应是国际议程的最高优先事项之一。由于网络空间的跨国性，这一领域的攻击影响可达全球一级。只有在全球一级开展有效合作，才有可能减少这些攻击的影响。

在这一点上，土耳其极为重视开展有效的国际合作，以在全球一级创建一个更加稳定和安全的网络空间。在这方面，土耳其已经准备好向拟订打击为犯罪目的使用信息和通信技术全面国际公约特设委员会作出贡献和提供支持。在此背景下，我们愿介绍我们对该公约的范围、目标和结构的初步看法。

需要在公约范围内考虑下列问题：

(a) 发展各国之间的有效合作渠道；

(b) 明确界定与为犯罪目的使用信息和通信技术有关的事项；

(c) 发展各国之间的紧急通信渠道；

(d) 改进用以收集和获取网络威胁情报的资源；

(e) 发展国家有关机构之间的情报共享；

(f) 在涉及为犯罪目的使用信息和通信技术的案件中分享信息。

此外，公约应包括防止犯罪分子和恐怖分子的内部通信及其宣传活动的有效措施。

2019 冠状病毒病（COVID-19）大流行大大增加了远程电信的使用；因此，在公约谈判期间，我们还应考虑这一大流行疫情对为犯罪目的使用信息和通信技术的影响。

此外，在公约范围内考虑在打击犯罪和网络攻击中安全使用云计算、5G、区块链、物联网和人工智能等新一代技术将是有益的。

大不列颠及北爱尔兰联合王国

[原文：英文]
[2021 年 10 月 28 日]

范围

联合王国认为，新的国际网络犯罪公约应侧重于加强合作，以应对犯罪活动对公民、企业和政府构成的日益严重的威胁。

现有的一些区域和国际网络犯罪条约已经为打击网络犯罪的努力作出了重大贡献。重要的是，既要在此类条约成功的基础上再接再厉，又要承认《联合国反腐败公约》和《联合国打击跨国有组织犯罪公约》等刑事司法条约的相关规定。

条约的范围应包括：(a)调查和起诉条约所界定的罪行；(b)发展各种能力，使所有会员国都能够处理这些犯罪；以及(c)确认一个专家论坛，通过该论坛可以查明新的和正在出现的威胁。

联合国网络犯罪条约应涵盖网络依赖性犯罪以及网络使能的犯罪，在这些犯罪中，犯罪的规模、范围和速度因使用计算机而增加。如果条约所列罪行得到所有法律制度的共同理解和承认，合作就是有效的。

条约中的罪行不应损害表达或见解自由的行使。

这是一项刑法条约，因此应侧重于国家行政部门开展的活动。条约还应考虑如何通过多利益攸关方办法，使公民、非政府组织、民间社会组织、学术机构和私营部门共同努力保护自己免受网络犯罪之害。

任何条约都必须载有强有力的保障措施，其中包括尊重国际人权法所规定并得到大会和人权理事会通过的相关决议承认的隐私权和其他人权。

必须以包容和透明的方式制定条约，尊重所有会员国的意见，并有广泛的利益攸关方，包括非政府组织、民间社会组织、学术机构和私营部门的积极参与。此外，条约的规定，例如关于执行和能力建设的规定，也应鼓励采取包容和透明的办法处理网络犯罪。

措辞应在技术上保持中立，以确保条约经得起时间的考验，不需要不断更新。

条约不应重复已经完成或应在其他地方适当完成的工作。条约不应扩大到大会第一委员会已经处理的网络安全事项，或专门的多利益攸关方论坛已经处理的互联网治理事项。

目标

条约的主要目的应是支持国家执法和检察机构在调查和起诉条约所列罪行方面进行双边或多边的有效合作。一项得到广泛支持的条约将促成尽可能广泛的国际合作。

为了支持有效的相互合作，必须有以下选择：以双重犯罪为由拒绝，拒绝政治罪，特别是在所指控的罪行涉及行使表达自由情况下，以及拒绝为以种族、宗教、性别或其他受保护特征为由惩罚或迫害个人而提出的请求。最好规定提出请求的当局必须确认其已达到的最低标准，例如请求是必要的、相称的、有时限的和在特定级别得到授权的。

使用调查和起诉条约规定的罪行的权力，包括在双边或多边案件中使用的这种权力，必须遵守国际人权法规定的与人权和基本自由有关的有效保障措施。

条约必须承认国家调查和检察机构的业务独立性，是否采取行动的决定完全由这些机构作出。

该条约应支持全球能力发展，并支持能力建设。

来自网络空间犯罪活动的威胁将发生变化，条约应确定一个政府间和多利益攸关方进程以查明未来的威胁，但不影响这一进程是否构成条约的一部分。

鉴于不同性别以不同方式受到网络犯罪的影响，条约应具有性别包容性，以帮助我们更有效地应对网络犯罪。制定一项认识到其条款的性别方面含义的网络犯罪条约，将鼓励更多的妇女在所有各级和所有进程中的参与。这将产生更多样化、更丰富并最终更好的解决方案。在 2021 年 4 月举行的全面研究网络犯罪问题政府间专家组会议上，所有会员国一致认为，它们应特别促进妇女专家的参与。

条约应促进采取“全社会”办法应对网络犯罪，并鼓励会员国与政府以外的行为体，包括专家、业界和公众，在提高认识、改善教育、进行性别和网络犯罪问题培训以及向受害者提供支持等领域开展合作。

结构

联合王国认为，以下结构将是组织该条约的有效手段：

(a) 总则

总则应包括条约的基础和宗旨，以及整个条约将使用的定义。这些定义必须得到所有缔约方的共同理解和商定，在技术上必须是中立的，同时考虑到区域文书中广泛商定的并在国家法律框架中使用的术语；

(b) 核心犯罪

这些犯罪必须包括网络依赖性犯罪（例如非法访问），并附有所有各方都能接受的描述和定义。如果犯罪主要在网上进行，计算机改变了犯罪的规模

和速度，以及犯罪的定义得到普遍理解，则应列入网络使能的犯罪（例如对儿童的性剥削和性虐待或诈骗）；

(c) 人权和保障措施

条约的运作和执行必须以切实的程序性保障和有力的人权保护为基础，并参考国际人权法；

(d) 预防措施

与《反腐败公约》和《有组织犯罪公约》一样，条约应包括鼓励各国采取措施预防网络犯罪的规定，其中包括与所有相关利益攸关方合作；

(e) 程序法规定

支持调查和起诉的权力必须允许有关当局为国内和国际调查保全、搜查和扣押通过计算机实施的任何犯罪的电子证据，或与犯罪有关的证据为电子形式的电子证据；

(f) 国际合作

国际合作条款必须涵盖司法协助和紧急情况下的协助，包括要求各国设立24/7 联络点。在实际分享证据的同时，专家组 2021 年 4 月提出的建议明确指出，会员国希望继续分享经验和最佳做法以及关于新的和日益严重的威胁的信息；

(g) 技术援助和能力建设

应鼓励能力建设，联合国毒品和犯罪问题办公室应发挥重要作用，并应通过全球网络专门知识论坛等现有结构协调此类工作。联合王国注意到专家组于 2021 年 4 月商定了大量侧重于能力建设的建议，包括为从业人员提供关于网络犯罪调查、电子证据处理、监管链和法证分析的专门和最新培训；

(h) 执行

应有执行该条约的明确计划。

美利坚合众国

[原文：英文]
[2021 年 10 月 28 日]

在执行大会第 74/247 号和第 75/282 号决议方面，美利坚合众国政府高兴地响应对会员国就新公约的范围、目标和结构（要素）提交意见的邀请。美国期待着与其他会员国和有关利益攸关方合作，起草一项全球文书，重点是根据并借鉴现有权利和义务，改进对网络犯罪的调查和起诉。美国重申，必须保持一个开放、包容、透明和多利益攸关方的进程，使所有会员国能够真诚地谈判达成知情、基于共识、切合实际的解决办法，我们认为这将鼓励广泛加入一项新的全球打击网络犯罪文书。

即使在正常情况下，我们的工作的拟议最后期限也会造成一个很紧的时间表，但我们目前的努力将在全球大流行疫情的背景下进行。因此，我们更加必须有重点和有效地努力谈判达成一项全球打击网络犯罪文书。不幸的是，尽管世界大多数国家已努力地抗击2019冠状病毒病（COVID-19）大流行疫情，但网络犯罪分子利用了由此产生的全球转变和对数字技术的依赖。网络犯罪是对全世界社会和人民的安全和福祉的直接威胁。在建设我们打击这种剥削的集体能力方面进行了长期合作，我们可以继续在这些成功的基础上再接再厉，认真考虑切实可行的解决办法。鉴于网络犯罪威胁的紧迫性，我们在谈判一项全球打击网络犯罪文书的努力中更加必须有重点和深思熟虑。

这一打击网络犯罪文书应旨在加强国际合作，并提供实用工具，使国家执法机关能够应对网络犯罪，就像联合国其他文书针对包括腐败、贩毒、贩运人口和偷运移民在内的其他形式的跨国犯罪所做的那样。该文书还应确保国内有权收集和获取与任何类型犯罪（不仅仅是网络依赖性犯罪）有关的电子证据，并促进在此类案件中的国际合作。与每一项联合国打击犯罪文书一样，这些工具应包括现有国内框架范围内的适当限制和保障措施，以处理隐私和公民自由问题，同时充分尊重人权。打击网络犯罪文书还应处理日益增长的技术援助需求，并为会员国寻求此类援助提供渠道。

随着会员国开始起草进程，必须认识到我们不是在真空中这样做。虽然界定这项文书应涵盖的内容很重要，但同样重要的是认识到哪些内容超出了其适当范围。联合国和其他政府间和多利益攸关方论坛正在就网络犯罪范围以外的其他网络相关问题开展有价值的工作。重要的是，我们不要重复或损害这项工作，既是为了避免义务冲突，也是为了不减损我们制定一项有针对性的、切实可行的打击网络犯罪文书的目标。试图在这一刑事司法文书中处理每一个与网络有关的问题有可能使这些谈判陷入重点不突出和无关紧要的辩论，这对打击网络犯罪毫无帮助，只会减缓我们在制定一项有用文书方面的进展。

特别是，会员国不应在专门打击网络犯罪的犯罪文书中深入探讨广泛的网络治理或网络安全专题。虽然经常被视为同一枚硬币的两面，但网络犯罪执法基本上是政府的责任，而网络安全是一系列公共和私人行为体的责任。拟订打击为犯罪目的使用信息和通信技术全面国际公约特设委员会的任务授权侧重于制定一项关于刑事事项的刑事司法文书，以促进对网络犯罪的国际对策，其中涉及界定和规定对网络空间犯罪行为的制裁。特设委员会无权规定网上非犯罪行为的全球规范。将网络治理和网络安全概念纳入网络犯罪条约将无法实现一项会吸引会员国广泛支持的精简和有效的文书的目标。

正如大会第 75/282 号决议所重申的那样，至关重要的是，关于一项新的打击网络犯罪文书的谈判不应妨碍现有机制，包括已经为有效打击网络犯罪提供了一系列工具的多国和区域文书。我们最好能够通过借鉴已证明成功的现有文书，为这项新文书凝聚共识，避开政治性和有分歧的问题。我们应当以在执行如《联合国打击跨国有组织犯罪公约》等其他联合国刑事司法条约方面的成就为指导。《有组织犯罪公约》已证明极为有用，因为该文书针对核心类型的有组织犯罪活动，同时还包括广泛的国际合作规定，这些规定可适用于三人或三人以上为牟利而实施的任何类型的严重犯罪。因此，缔约方已成功地利用《有组织犯罪公约》数千次，包括打击勒索软件事件和儿童性剥削等犯罪。

美国再次重申，必须保持一个开放、包容和透明的进程，使所有会员国和有关利益攸关方能够真诚地谈判达成知情、基于共识、切合实际的解决办法，我们认为这是鼓励广泛加入一项新的全球打击网络犯罪文书的最佳途径。

将核心网络犯罪罪行定为刑事犯罪

首先，任何新文书都应确保国内有权收集和获取任何类型犯罪的电子证据。这种权力对于各国能够有效调查和起诉几乎每一类犯罪至关重要，因为当今的犯罪很少完全在数字领域之外进行。该文书还应促成在分享任何类型犯罪的电子证据方面开展国际合作，但须遵守《有组织犯罪公约》和《联合国反腐败公约》所载的灵活的双重犯罪规定。[9]

此外，有效的国际合作要求会员国制定适当的国内立法，将核心网络犯罪罪行定为刑事犯罪。会员国对核心实质性犯罪的共同理解和支持程序权威对于避免为网络犯罪分子创造安全庇护所至关重要。联合国毒品和犯罪问题办公室（毒品和犯罪问题办公室）的研究表明，各国普遍同意应通过具体的网络犯罪法规将核心行为定为刑事犯罪，许多多国协定和国家刑事法规载有共同规定。同样，国际上对支持有效网络犯罪调查的合法类型的程序权威的理解也得到了解决。因此，从业人员在调查网络犯罪方面积累了二十年的各种经验，表明调查网络犯罪的普遍采用的各类实质性和程序性权威仍然可行。

一项新的打击网络犯罪文书应界定并适用于网络依赖性犯罪，即计算机或数据成为犯罪活动目标的犯罪，以及某些网络使能的犯罪，即利用计算机为犯罪提供便利的犯罪。这一新文书将界定的第一类也是主要的一类罪行包括那些不滥用计算机或网络系统就不可能实施的罪行，因此在计算机系统出现之前并不作为犯罪存在的罪行。网络依赖性犯罪可以完全发生在数字领域。对于拒绝服务攻击或损坏计算机和数据等依赖网络的核心刑事犯罪，需要制定专门针对网络的法规，因为在大多数法域，刑法被严格解释，涵盖非法侵入和破坏等熟悉概念的传统法律往往不足以适用于网络犯罪。此外，适用于在计算机网络外实施的犯罪的某些刑法规定可能不容易适用于通过计算机实施的行为。

相比之下，我们应注意不要仅仅因为计算机涉入了传统犯罪的策划或执行就将该传统犯罪视为“网络犯罪”。尽管是滥用计算机实施的犯罪，但一些应受惩罚的行为可能由一般法规所涵盖，因为在这种行为中使用计算机系统没有什么特殊或独特之处。相反，一些网络使能的犯罪由打击网络犯罪的文书适当处理，例如，在计算机使用增加的情况下：

(a) 犯罪的范围，例如涉及数千名受害者或数百万支付数据记录被盗；

(b) 攻击的速度，因为计算机大幅度增加完成这种犯罪的能力；

(c) 对受害者的损害或伤害的程度；或者

(d) 犯罪者的匿名性。

[9] 见《联合国打击跨国有组织犯罪公约》第十八条第九款和《联合国反腐败公约》第四十六条第九款。虽然这两项公约的规定略有不同，但都给予被请求缔约国在提供协助特别是强制措施方面的很大的酌处权。

在适用这些概念时，一些传统犯罪案件，如诈骗和剥削儿童，也可以合理地被视为属于本次谈判的范围。然而，会员国应明智地确定我们所寻求应对的网络使能的犯罪的范围，以免扭曲长期存在的刑事司法概念。长期存在的刑事法规和文书不会仅仅因为犯罪涉及某种“网络”成分而失去其适用性。

一项全球打击网络犯罪文书还应呼吁各缔约方颁布立法，以技术中立的方式将核心网络犯罪罪行定为刑事犯罪，同时确保程序保障。以技术中立的方式将犯罪定为刑事犯罪（即，将影响计算机数据机密性、完整性和可用性的活动定为刑事犯罪，而不是将所使用的特定形式或方法定为刑事犯罪，如网络钓鱼或勒索软件）确保实质性刑事规定不仅处理当今的技术和犯罪手段，而且也处理未来的技术和手段。一个说明技术发展有多快的例证是，即使 2013 年网络犯罪问题全面研究草案的明确意图是具有全面性，也还是缺乏关于研究时未广泛使用或刚刚出现的技术或手段的细节，包括勒索软件、物联网、加密货币、以及移动技术的快速发展和优势。反映这种关注的是，在全面研究网络犯罪问题专家组会议上，会员国商定的结论和建议之一是，会员国应通过颁布具有技术上中立的措辞的法律，确保其立法规定在未来技术发展方面经受住时间的考验，并将被视为非法的活动而不是所使用的手段定为刑事犯罪。[10]这一点特别重要，因为我们试图起草一项持久的文书，以能够充分处理明天的技术，并满足执法人员现在和未来的需要。

铭记这些原则，全球打击网络犯罪文书应包括将以下行为定位刑事犯罪：

(a) 非法访问，即未经授权访问计算机或计算机系统；

(b) 非法拦截，即实时非法拦截通信内容或与通信有关的流量数据；

(c) 干扰数据或系统，即恶意软件、拒绝服务攻击、勒索软件以及删除或修改数据；

(d) 滥用设备，即贩运或使用允许获取资源的信用卡数据、密码和个人信息；

(e) 与儿童性虐待材料有关的犯罪；

(f) 与计算机辅助诈骗有关的犯罪，即操纵计算机系统或数据用于诈骗目的，如网络钓鱼、损害营商电子邮件和拍卖诈骗；

(g) 与侵犯著作权及相关权利有关的犯罪；以及

(h) 关于未遂、协助和教唆以及阴谋的规定。

此外，对网络犯罪所得的洗钱行为也应定为刑事犯罪。最后，如果法人参与该文书禁止的网络犯罪，应受到刑事或民事和行政制裁。

收集和分享电子证据的程序权威

除了将实质性犯罪定为刑事犯罪外，全球打击网络犯罪文书还应满足国内法律当局按照适当程序和保护人权和基本自由保全、收集和分享电子证据的需

[10] 见全面研究网络犯罪问题专家组 2021 年 4 月 6 日至 8 日在维也纳举行的会议报告（UNODC/CCPCJ/EG.4/2021/2）。

要。一些会员国指出，根据其本国法律，传统的程序权威来源可能不适用于无形数据，也可能不授权足够迅速地收集不稳定的电子证据。与以往一样，过时的法律将不足以应对电子犯罪调查的许多挑战，包括处理广泛的加密和云计算服务等新技术。因此，收集电子证据的程序权威的专门来源至关重要。在起草这些法律时应考虑到适用的技术概念以及刑事调查人员的实际需要。更具体地说，这些程序权威来源应允许：

(a) 快速保全存储的计算机数据；

(b) 计算机数据提供令；

(c) 搜查和扣押存储的计算机数据；

(d) 实时收集计算机流量数据；以及

(e) 在严重犯罪案件中实时收集内容数据。

此外，新文书应允许开展合作，以收集和获取任何类型犯罪的电子证据，而不仅仅是网络犯罪的电子证据。几乎所有重大刑事犯罪都涉及与侦查和起诉犯罪有关的电子证据，无论是移动电话数据、电子邮件、交易数据还是其他数据。作为一个国内事项，会员国需要一个现代法律证据框架，其中允许在刑事调查和起诉中采纳电子证据，包括与国际执法伙伴分享电子证据。

国际合作

除了国内法之外，打击网络犯罪的有效国际合作既依赖于正式的、基于条约的合作，如司法协助，也依赖于其他手段，如传统的、经授权的警方对警方合作。新的打击网络犯罪文书应借鉴现有条约中加强国际合作的有效工具，并确保其不会破坏全球打击网络犯罪方面的现有文书和正在进行的国际合作。打击网络犯罪文书中与国际合作有关的规定，包括司法协助、引渡、移交起诉、没收包括虚拟货币在内的所得和将没收的资产返还被害人、双重犯罪和执法合作，应严格遵守《有组织犯罪公约》和《反腐败公约》的规定，包括其中的适当保障措施和保护措施，绝大多数会员国已成功地实施了这些措施。此外，关于司法协助的规定应规定广泛协助获取与刑事犯罪有关的电子证据，无论刑事犯罪的实施是否涉及计算机系统。

技术援助和能力建设

毒品和犯罪问题办公室的研究报告指出，75%以上的国家在现有执法组织内设有专门处理网络犯罪相关问题的单位，约 15%的国家设有专门处理网络犯罪问题的专门机构。这突出了网络犯罪调查的专业性，包括需要进行专门培训。此外，网络犯罪和传统犯罪的电子或数字要素的复杂性大大增加，这对培训和维持高技能的调查人员和技术专家产生更多的需求。

国内能力不足是各国可能无法有效开展国际合作的最常见原因。对大多数国家来说，国际合作的失败不是因为缺乏意愿，而是因为国内法或执法机构专门知识的限制。许多会员国在执法机关打击网络犯罪或处理电子证据的能力方面资源不足。例如，鉴于现有的国家优先事项，一些会员国在培养和留住受过

培训的调查员和法证检查员以及处理计算机设备和软件短缺问题方面面临挑战。因此，已有一个广泛的国际共识是，对执法机构，包括调查人员、检察官和法官，进行技术援助和能力建设仍然是国际社会有效应对网络犯罪的最紧迫要求。此外，由于电子证据成为几乎每一类犯罪的组成部分，即使是非专业的执法人员也需要对与计算机有关的调查有一些基本了解。

网络犯罪文书中与技术援助和能力有关的规定应包括：

(a) 会员国为其负责预防和打击网络犯罪的人员启动、制定或改进培训方案而采取的措施；

(b) 会员国考虑根据能力，在各自打击网络犯罪的计划和方案中相互提供最广泛的技术援助，特别是为发展中国家和可能不成比例地面临网络犯罪威胁的国家提供技术援助；

(c) 建立各种机制，使会员国的自愿财政捐款能够支持实施一项网络犯罪文书；

(d) 会员国考虑向毒品和犯罪问题办公室网络犯罪问题全球方案及其相关的刑事司法能力建设努力提供自愿捐款。

社会、实体和组织的参与

鉴于网络犯罪问题的复杂性和多面性，打击网络犯罪不能是一项孤立的努力。一项打击网络犯罪的文书应考虑到个人以及如非政府组织、民间社会组织、学术机构和私营部门等团体积极参与预防网络犯罪的重要性，同时适当考虑到性别平等。这种参与可以提高公众对网络犯罪威胁的认识，确保会员国以透明的方式开展工作，并处理与隐私、公民自由和人权有关的实质性事项。此外，一项有效的文书取决于在网络犯罪领域拥有专门知识的个人和实体的贡献。为了实施一项切实有效的打击网络犯罪文书，该领域专家的强力参与至关重要。

执行机制

对于确定是否需要一个单独的进程来审查该文书今后的执行情况，如果需要，应采取何种形式，这在现阶段还为时过早。有各种成功的模式可以考虑。鉴于可用于技术援助的资源短缺，应考虑采用依靠预算友好型备选办法来最大限度地增加捐助者对技术援助的捐款的方法。其中一种方法是授权经济及社会理事会第 1992/1 号决议所设预防犯罪和刑事司法委员会审议与该网络犯罪文书的目标有关的所有事项。与负责监督三项国际药物管制条约的麻醉药品委员会有关的这种监督有一个成功的先例。如关于社会、实体和组织的参与的上一节所概述，在执行文书产生的任何工作流程时，必须考虑到公共社会、实体和组织的强力参与。然而，关于执行机制的讨论应予保留，直到文书的范围得到进一步界定为止。