联合国最新资讯：网络相关事务的发展

联合国最新资讯：信息和通信技术安全和使用问题不限成员名额工作组 (OEWG)、为拟订关于打击出于犯罪目的使用信息和通信技术行为的全面国际公约而设立的特设专家委员会 (AHC)、《全球数字契约》(GDC) 以及其他联合国相关讨论中网络相关事务的发展

GE-014
2023 年 12 月 15 日

ICANN

目录

简介

联合国大会 (United Nations General Assembly, UNGA) 设有专门讨论网络相关事务的议事程序，本文件提供了这些议事程序的最新进展情况。本文件涵盖了第二届不限成员名额工作组 (Open-Ended Working Group, OEWG)[1] 和特设专家委员会 (Ad Hoc Committee of Experts, AHC)[2] 在 2021 年 6 月 4 日至 2023 年 9 月 2 日期间开展的审议工作的最新进展，以及 2023 年就《全球数字契约》(Global Digital Compact, GDC) 及相关事务进行的讨论的最新动态。

作为定期发布的系列报告之一，本文件概述了联合国开展的与互联网生态系统以及互联网名称与数字地址分配机构 (Internet Corporation for Assigned Names and Numbers, ICANN) 使命相关的活动。[3]对这些活动进行监测，体现了 ICANN 组织（简称“组织”）政府和国际政府间组织合作 (Government and Intergovernmental Organization Engagement, GE) 团队的承诺与责任，让更广泛的 ICANN 社群了解对全球、统一、互用的互联网及其唯一标识符系统至关重要的问题。[4]

[1]信息和通信技术安全和使用问题不限成员名额工作组 (OEWG)，https://meetings.unoda.org/meeting/57871/statements

[2]为拟订关于打击出于犯罪目的使用信息和通信技术行为的全面国际公约而设立的特设专家委员会 (AHC)，https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

[3]请在此处查看 GE 以前的报告：https://www.icann.org/zh/government-engagement/publications。这个 URL 以及脚注和附录中的所有其他 URL 均于 2023 年 8 月 [插入日期] 进行检索。

[4] “ICANN 运营和财务规划”，第 47 页，ICANN 组织，2020 年 12 月，https://www.icann.org/en/system/files/files/draft-op-financial-plan-fy21-25-opplan-fy21-20dec19-en.pdf

OEWG 最新动态

第一次实质性会议[5]

2021 年 12 月 9 日

中国：“当前关键互联网资源的分配和管理体系不均衡、不公正。”[...]“各国应平等参与国际互联网资源的管理和分配，构建多边、民主、透明的全球互联网治理体系。”[6]

2021 年 12 月 12 日

中国：“各国有权根据公认的国际法原则和规则，对本国境外与本国有真正和实质性联系的特定信息和通信技术 (Information and Communication Technology, ICT) 活动，以及与 ICT 有关的设施、主体、数据和信息，行使必要且合理的属人、属地和保护性管辖权。为了行使管辖权，一国可以本着自我克制、礼让和互惠的精神，寻求其他国家和地区的援助。”
[...]
“主权在物理层的体现。各国对于其境内的物理基础设施和基本 ICT 服务拥有管辖权。各国有权根据国内法和国际法采取必要措施，维护物理基础设施的安全。各国有权参与全球互联网基础设施的管理和国际合作。”[...]“主权在逻辑层的体现。各国可以独立制定或采用相关的技术法规或标准，同时根据国际法规定的义务，保持互联网的互用性。”[7]

背景信息：在中华人民共和国国务院新闻办公室近期发布的一份白皮书中，以下关于治理和关键互联网资源的要点值得引用：

“第三章第三节：（三）积极参与网络空间治理
中国积极参与全球互联网组织事务。积极参与互联网名称与数字地址分配机构等平台或组织活动。支持互联网名称与数字地址分配机构治理机制改革，增强发展中国家代表性，推进互联网基础资源管理国际化进程。积极参与国际互联网协会、互联网工程任务组、互联网架构委员会活动，促进社群交流，推进产品研发和应用实践，深度参与相关标准、规则制定，发挥建设性作用。”
[...]

“第四章第五节：（五）维护互联网基础资源管理体系安全稳定
互联网基础资源管理体系是互联网运行的基石。应确保承载互联网核心资源管理体系的机构运作更加可信，不因任何一国的司法管辖而对其他国家的顶级域名构成威胁。中国主张，保障各国使用互联网基础资源的可用性和可靠性，推动国际社会共同管理和公平分配互联网基础资源，让包括域名系统在内的互联网核心资源技术系统更加安全、稳定和富有韧性，确保其不因任何政治或

[5]有关 OEWG 和 AHC 会议的引文包括书面和口头声明
[6]中国关于将主权原则应用于网络空间的看法，2021 年 12 月 9 日，第 1 页，https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-International-Rules-making-in-Cyberspace-ENG.pdf
[7]中国关于将主权原则应用于网络空间的看法，2021 年 12 月 12 日，第 1 页和第 4 页，https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-the-Application-of-the-Principle-of-Sovereignty-ENG.pdf

人为因素而导致服务中断或终止。中国倡导各国政府、行业组织、企业等共同努力，加快推广和普及 IPv6 技术和应用。” [8]

[8]新华网，中国发布《携手构建网络空间命运共同体》白皮书，2022 年 11 月 7 日，https://english.www.gov.cn/archive/whitepaper/202211/07/content_WS636894aac6d0a757729e2973.html

2021 年 12 月 14 日

葡萄牙：“在尊重人权、遵守国际法和遵循最高基准的前提下，开展强有力的国际合作，让所有联合国成员国的国家关键基础设施以及使其融为一体的互联网核心变得更富有韧性，这对于阻止武装冲突门槛以下的网络攻击至关重要。”[9]

中国：“互联网的未来不应也不可能由少数国家操控。以意识形态划线构建排他的‘小圈子’、执着于维持 ICT 垄断和网络霸权，只会阻碍国际社会促进网络安全的多边努力。个别国家试图建立所谓‘未来互联网联盟’，这是出于地缘政治目的，分裂互联网、谋求技术垄断和网络霸权、打压别国科技发展的又一例证。他们口口声声要打造‘开放’的互联网，实际上做的却是制造对抗、割裂互联网的行径，这同和平、安全、开放、合作的互联网精神完全背道而驰，也违背了国际社会的共同利益。”[10]

“与此同时，我们应根据 ICT 特点和形势发展需要，讨论制定新的准则。数据安全是各国面临的突出新挑战。各方应遵照决议授权，深入讨论数据跨境流动、供应链安全、个人信息保护等问题，研究应对之策。中方《全球数据安全倡议》可作为讨论的初步基础。”[11]

背景信息：在该意见声明中，中国代表对个别国家的倡议提出批评，同时提议中方倡导的“数据安全倡议”可作为“讨论的初步基础”。

西班牙：“如果我们不能在联合国内部达成共识、制定统一的全球法规，那么当前的地缘政治紧张局势可能会导致网络空间分裂成不同的影响领域，催生出互不兼容的标准认证和技术规范。”[12]

中国：“网络空间面临分裂风险。在今年的联合国大会上，联合国秘书长古特雷斯 (Gutierrez) 警告称，世界面临‘一分为二’的风险，有可能分裂成奉行不同标准的两大阵营。网络空间亦是如此。”[13]

伊朗伊斯兰共和国：“这需要在信息安全领域采取更加全面的威胁应对方法，不仅要解决数字基础设施问题，还要解决内容和信息本身的问题。各国面临着一些紧迫严峻的现有威胁和潜在威胁，包括：(1) 互联网治理存在垄断和霸权…”[14]

---

[9]联合国网络电视，第 3 次全体会议，2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组 – 第一次实质性会议，2021 年 12 月 14 日，https://media.un.org/en/asset/k11/k11eljcg88（从 1:14:20 开始）

[10]联合国网络电视，第 3 次全体会议，2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组 – 第一次实质性会议，2021 年 12 月 14 日，https://media.un.org/en/asset/k11/k11eljcg88（从 1:50:40 开始）

[11]中国代表团团长吴剑剑 (Wu Jianjian) 参赞在信息和通信技术安全和使用问题不限成员名额工作组首次实质性会议一般性辩论中的意见声明，2021 年 12 月 14 日，https://documents.unoda.org/wp-content/uploads/2021/12/Statement-of-China_ICT-OEWG-3rd-plenary-meeting_General-Exchange-of-Views_DEC-14-AM_ENG.pdf

[12]联合国网络电视，第 4 次全体会议，2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组 – 第一次实质性会议，2021 年 12 月 14 日，https://media.un.org/en/asset/k1b/k1b55qgp81（从 04:30 开始）

[13]联合国网络电视，第 4 次全体会议，2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组 – 第一次实质性会议，2021 年 12 月 14 日，https://media.un.org/en/asset/k1b/k1b55qgp81（从 1:56:42 开始）

[14]联合国网络电视，第 4 次全体会议，2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组 – 第一次实质性会议，2021 年 12 月 14 日，https://media.un.org/en/asset/k1b/k1b55qgp81（从 2:35:20 开始）

背景信息：没有证据表明互联网治理存在任何“垄断和霸权”。互联网治理在信息社会世界峰会 (World Summit on the Information Society, WSIS) 和联合国大会的 WSIS+10 谈判期间得到了广泛讨论；而且，在 WSIS《突尼斯议程》或 WSIS+10 成果文件中，均未得出这样的结论。

2021 年 12 月 15 日

荷兰：“全球社群面临一些现有挑战和潜在威胁，包括旨在损害欧盟现行法规中定义的互联网完整性、功能性和可用性的网络行动。在之前的 OEWG 和 GGE 报告（规范 13f）中，对互联网的一般可用性或完整性至关重要的技术基础设施或公共核心称为关键基础设施。另外，对互联网的基本功能性至关重要的技术基础设施也需要加以保护，从而阻止企图通过操控这一基础设施来损害互联网完整性或可用性的行径。抱有这种企图的行为者为数不少。特别是，绝不能让基于多利益相关方治理的互联网治理模型遭到破坏。互联网的正常运行，离不开私营部门、公民社会、技术社群及其他利益相关方的共同努力。”[15]

伊朗伊斯兰共和国：“我们认为，对当前互联网治理进行重大改革，各国公开、公平、非歧视地获取 ICT 技术，建立可靠的网络安全供应链，是各国在 ICT 环境中负责任行为的基本要求”。[16]

背景信息：对于互联网治理，联合国互联网治理工作组 (Working Group on Internet Governance, WGIG) 给出的定义为：“互联网治理是政府、私营部门和公民社会按照各自的角色制定和应用共同的原则、规范、规则、决策程序和方案，这些原则、规范、规则、程序和方案影响着互联网的发展和使用。”[17] 因此，它与声明中的问题无关。互联网治理论坛 (Internet Governance Forum, IGF) 每年都会讨论互联网治理现状，该论坛是进行此类讨论的合适场所，因为它面向所有人开放。关于互联网治理的未来发展，将于 2025 年在联合国大会的 WSIS+20 期间进行讨论。

印度：“我们需要讨论不进行和不故意允许对互联网公共核心进行攻击的义务。互联网的公共核心包括：数据包路由和转发元素；命名和编号系统；安全和身份的加密机制；传输媒体、软件和数据中心。”[18]

2021 年 12 月 16 日

哥斯达黎加：“CERT 一直在引导各社群建立信任关系，通过交流信息来应对 ICT 事件，因此我们也可以从技术社群汲取一些最佳做法和经验教训。具体而言，我们要深切意识到除了在目录中列出域名之外，更重要的是召开会议或开展演练，以在网络空间中建立信任、增进关系。”[19]

---

[15]联合国网络电视，第 5 次全体会议，2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组 – 第一次实质性会议，2021 年 12 月 15 日，https://media.un.org/en/asset/k1r/k1royetcr4（从 39:42 开始）；另请参阅：荷兰安全政策和网络事务巡回大使娜塔莉 • 雅苏玛 (Nathalie Jaarsma) 的意见声明，2021 年 12 月 15 日，https://documents.unoda.org/wp-content/uploads/2021/12/21.12.15-Netherlands-Statement-on-Threats-OEWG-in-the-Field-of-Information-and-Telecommunications-in-the-Context-of-Internat.pdf

[16]联合国网络电视，第 6 次全体会议，2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组 – 第一次实质性会议，2021 年 12 月 15 日，https://media.un.org/en/asset/k1r/k1rnexulnt（从 50:35 开始）

[17]联合国互联网治理工作组报告，2005 年 6 月，第 10 点，https://www.wgig.org/docs/WGIGREPORT.pdf

[18]联合国网络电视，第 6 次全体会议，2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组 – 第一次实质性会议，2021 年 12 月 15 日，https://media.un.org/en/asset/k1r/k1rnexulnt（从 01:48:55 开始）

[19]联合国网络电视，第 8 次全体会议，2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组 – 第一次实质性会议，2021 年 12 月 16 日，https://media.un.org/en/asset/k1y/k1yzr8yhb1（从 57:20 开始）；另请参阅：哥斯达黎加常驻联合国代表团的意见声明，2021 年 12 月 16 日，https://documents.unoda.org/wp-content/uploads/2021/12/Final-Costa-Rica-CBMs-1612021-SP-EN.pdf

2021 年 12 月 17 日

伊朗伊斯兰共和国：“OEWG 应着力解决致使 ICT 环境缺乏信任的主要根源，具体包括：互联网治理垄断、匿名现象、充满攻击性的网络战略、敌对形象的塑造、引发单方面强制措施的仇外心理、私营公司和平台及民族国家对境外活动缺乏责任感等。各国应朝着同一个目标出发，即实现多边、公平、透明的互联网治理。”[20]

背景信息：没有证据表明“互联网治理存在垄断”。互联网治理的定义是通过 WSIS《突尼斯议程》确定的，包括各国政府在内的所有利益相关方都参与互联网治理。而且，也没有证据表明所有相关方已就新的多边互联网治理模型达成共识。德国在 2022 年 3 月 28 日的意见声明中提到了这一点（见下述引文）。

[20]伊朗伊斯兰共和国针对第一次实质性会议提交的文件，2022 年 12 月 17 日，第 8-9 页，https://documents.unoda.org/wp-content/uploads/2021/12/Irans-submission-to-first-substantive-session_13-17-Dec-21.pdf

第二次实质性会议

2022 年 3 月 28 日

联合国副秘书长中满泉 (Izumi Nakamitsu)：“众所周知，在 ICT 安全领域，多利益相关方的参与至关重要，因为私营行为者拥有并管理着许多相关基础设施。”[21]

美国：“今天在这里开展的 [OEWG] 流程 [...] 面向每一个竭力维护网络空间稳定的成员国开放，凡是想要建立由所有人共享的开放、可互用、安全、可靠的互联网并从中受益的利益相关方都可以参与进来...”[22]

德国：“互联网不归任何国家所有，也不由任何国家控制。互联网是一个公共领域，由代表各行业、公民社会和政府的一系列相关方通过高度复杂但十分高效的合作模式来进行管理和推进。为此，这个不限成员名额工作组的参与人员构成应充分反映这一事实。”[23]

西班牙：“我们看到，网络空间的分裂威胁是切实存在的，这种威胁可能会影响技术规范，最终导致技术规范之间完全不兼容。我们绝不能允许这种情况发生，因为这将直接影响到所有国家。”[24]

2022 年 3 月 29 日

俄罗斯联邦：“例如，完全切断一个国家和地区与国际通信系统的连接是完全有可能的，特别是切断与互联网的连接，或者是切断与用于传输信息和进行支付的银行同业系统 SWIFT 的连接。这种威胁并不只是在理论上存在；实际上，俄罗斯正面临这种威胁。从以往经验来看，技术能够帮助实施这种威胁，因为这些系统由一个国家和地区或少量国家和地区构成的小团体管理。以互联网为例，管理互联网的是负责管理域名和 IP 地址的 ICANN 机构。ICANN 是一个非营利性国际组织，但事实上完全由美国控制。正因如此，这样一个掌管大权的国家所做的政治决策能够轻而易举地影响任何其他国家和地区。”[25]

背景信息：ICANN 无权“切断”（停止、关闭等）任何国家和地区与互联网的连接。在 2022 年 3 月 2 日 ICANN 总裁兼首席执行官致乌克兰副总理的信函中，非常清楚地表达了这一点。[26] 作

---

[21]联合国网络电视，（第 1 次会议）2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组，第二次实质性会议，2022 年 3 月 29 日，https://media.un.org/en/asset/k1h/k1hhzc7i5z（从 6:27 开始）

[22]联合国网络电视，（第 1 次会议）2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组，第二次实质性会议，2022 年 3 月 29 日，https://media.un.org/en/asset/k1h/k1hhzc7i5z（从 35:00 开始）

[23]联合国网络电视，（第 1 次会议）2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组，第二次实质性会议，2022 年 3 月 29 日，https://media.un.org/en/asset/k1h/k1hhzc7i5z（从 1:13:55 开始）；另请参阅：德国在 3 月份 OEWG 第 3 项议程中的意见声明，2022 年 4 月 22 日，第 3 页，https://documents.unoda.org/wp-content/uploads/2022/04/German-Statement-at-the-March-2022-OEWG-Agenda-Item-3.pdf

[24]联合国网络电视，（第 1 次会议）2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组，第二次实质性会议，2022 年 3 月 29 日，https://media.un.org/en/asset/k1h/k1hhzc7i5z（从 1:52:38 开始）

[25]联合国网络电视，（第 3 次会议）2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组，第二次实质性会议，2022 年 3 月 29 日，https://media.un.org/en/asset/k1l/k1l7rcax4f（从 51:05 开始）

[26]互联网名称与数字地址分配机构 (ICANN) 总裁兼首席执行官马跃然 (Göran Marby) 致乌克兰副总理兼数字化转型部长米哈伊洛 • 费多罗夫 (Mykhailo Fedorov) 的信函，2022 年 3 月 2 日，https://www.icann.org/en/system/files/correspondence/marby-to-fedorov-02mar22-en.pdf

为欧洲、中东和部分中亚地区的互联网注册管理机构，欧洲网络协调中心 (RIPE Network Coordination Center, RIPE NCC) 在 2022 年 3 月 10 日公开表达了类似立场。[27] 另外，2022 年 4 月 5 日，菲奥娜 • 亚历山大 (Fiona Alexander)[28] 女士指出：“与在联合国体系中相比，俄罗斯联邦在多利益相关方模型中得到了更好的保护。因此，尽管乌克兰副总理请求 RIPE 和 ICANN 移除俄罗斯的互联网资源，这两个组织都“拒绝”了。[29] 不过，在 2022 年 3 月举行的 ITU 世界电信标准化全会上，应乌克兰的请求，剥夺了俄罗斯政府在研究组中的领导职位。[30] 虽然俄罗斯联邦加入了 ICANN，但它盼望着 ITU 接管或取代 ICANN。而讽刺的是，多利益相关方模型实际上比联合国体系更好地保护了俄罗斯人民和互联网，因为俄罗斯政府在联合国体系中的席位已被剥夺。”[31] 2022 年 4 月 6 日，白宫发布了一份关于美国、七国集团和欧盟针对俄罗斯的制裁措施简报，这份简报中表示限制互联网访问不是制裁的目标。[32]

马来西亚：“在这方面，[我们] 可以考虑由托管提供商、执法机构、互联网服务提供商和域名注册服务机构采取迅速而有效的措施，在托管提供商层面阻止和关停需要重点关注的恶意网站，特别是那些影响关键信息基础设施的网站。”[33]

荷兰：“一些举措会破坏对互联网一般可用性或完整性至关重要的技术基础设施，也称为互联网的公共核心，包括：针对互联网核心物理和逻辑基础设施的网络行动；针对负责全球路由、命名和编号事务的核心组织的网络行动，例如针对地区互联网注册管理机构、ICANN 和大型互联网交换中心的网络行动。另外，还包括引入有损互联网开放性和互用性的互联网标准及协议。为从技术层面进一步加深对公共核心的理解，荷兰将开展相关活动，帮助这个不限成员名额工作组社群在技术层面深入了解公共核心。”[34]

伊朗伊斯兰共和国：“互联网治理目前存在垄断，这种垄断会带来风险，需要一种新体系架构来加以解决，但是自 2005 年在突尼斯举行信息社会世界峰会 (WSIS) 以来，这一问题一直未在联合国体系内得到有效讨论（《信息社会突尼斯议程》第 29 条至第 82 条）。遗憾的是，互联网治理论坛 (IGF) 拒绝讨论这一问题并将它交给 OEWG，而 OEWG 认为讨论互联网治理超出了其职

[27] RIPE NCC，RIPE NCC 对乌克兰政府请求的回复，2022 年 4 月 10 日，https://www.ripe.net/publications/news/announcements/ripe-ncc-response-to-request-from-ukrainian-government

[28] 菲奥娜 • 亚历山大目前是美利坚大学国际服务学院的杰出驻院政策战略分析师，也是美利坚大学互联网治理研究室的杰出研究员。菲奥娜曾在美国商务部下属的美国国家电信和信息管理局 (National Telecommunications and Information Administration, NTIA) 任职近 20 年，她曾在 NTIA 任国际事务副署长。

[29] RIPE NCC 对乌克兰政府请求的回复：乌克兰副总理致 RIPE NCC 的信函 (PDF)，及 RIPE NCC 总经理的回复函 (PDF)，阿姆斯特丹，2022 年 3 月 10 日，https://www.ripe.net/publications/news/announcements/ripe-ncc-response-to-request-from-ukrainian-government

[30] 乌克兰常驻联合国日内瓦办事处代表团的官方 Twitter 帐户，2022 年 3 月 9 日，https://twitter.com/UKRinUNOG/status/1501658319932600326；捷克共和国常驻联合国日内瓦办事处代表团的网站，2022 年 3 月 9 日，https://www.mzv.cz/mission.geneva/en/specialized_agencies/international_telecommunication_union/russia_s_military_aggression_against.html

[31] 菲奥娜 • 亚历山大，ITIF 网络研讨会，“战争和冲突时期的互联网治理”，2022 年 4 月 5 日，（从 58:57 开始），https://itif.org/events/2022/04/05/internet-governance-during-times-war-and-conflict

[32] 美国白宫，简报室，“简报：美国、七国集团和欧盟将对俄罗斯施加严格的直接经济制裁”，2022 年 4 月 6 日，https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/06/factsheet-united-states-g7-and-eu-impose-severe-and-immediate-costs-on-russia/

[33] 联合国网络电视，（第 3 次会议）2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组，第二次实质性会议，2022 年 3 月 29 日，https://media.un.org/en/asset/k1l/k1l7rcax4f（从 1:18:48 开始）

[34] 联合国网络电视，（第 3 次会议）2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组，第二次实质性会议，2022 年 3 月 29 日，https://media.un.org/en/asset/k1l/k1l7rcax4f（从 1:26:20 开始）

权范围，又将此问题交还给 IGF。因此，国际社会一直无法就全球互联网治理达成共识，进而无法消除互联网治理目前存在的垄断。鉴于此，国际社会必须尽快在 OEWG 内部制定更为有效的互联网治理解决方案，以保障 ICT 环境的稳定和安全。”[35]

背景信息：再次声明，伊朗在该周早些时候就声称“互联网治理存在垄断”，但这一观点没有事实做支撑。此外，伊朗表示需要“新的体系架构”，但是至于这个“新的体系架构”是什么，目前尚不清楚。不过，联合国秘书长在“数字合作路线图”中阐述了如何改进数字合作架构的问题。2022 年，联合国秘书长组建了 IGF 高层领导小组，这是一个旨在支持和加强 IGF 的多利益相关方团体。[36]而且，自 2003 年以来，联合国就一直通过 WSIS 和 WSIS+10 审核来讨论与联网治理有关的各种问题，还多次通过 IGF 讨论这些问题。伊朗称 IGF“拒绝讨论这一问题”，但实际上 IGF 会积极讨论参与者以提案形式提出的任何问题，只要这些提案被 IGF 多利益相关方咨询团体接受。互联网治理是一个全球问题，相关 WSIS 文件对互联网治理进行了详尽阐述和说明。[37]

法国：“我国代表团想要提醒工作组，开放自由、可互用的网络空间现在面临重重威胁。关注国际形势，我们可以看到，网络空间的孤岛化趋势日益加重 [...]，甚至是最底层也面临孤岛化风险。[...]目前从未发生过通过限制访问深层互联网对国家进行制裁的行径。但是，随着对这种制裁行径的讨论越来越多，巨大风险也随之逼近。网络空间的分裂不仅会给人权、信息自由流通和经济增长带来风险，而且也会日益对国际稳定构成威胁。事实上，如果我们有多个不同的互联网，一些国家可能会借由保护不稳定的互联网，以及在这些互联网之外再建立一个网络来从事恶意活动。工作组应该考虑到这一点，引导各国加倍努力，维护自由、统一、开放、稳定、安全且普遍可访问的网络空间架构。”[38]

2022 年 3 月 30 日

荷兰：“对荷兰而言，要保护互联网的公共核心，不仅要遵循多利益相关方互联网治理模型，还要防止引入有损互联网开放性和互用性的标准及协议。鉴于此，作为对昨日提议的回应，我想强调的是，ICANN 和地区互联网注册管理机构等多利益相关方组织的作用是确保协调互联网技术，并努力维护全球统一、可互用的互联网，以便互联网持续运行，并且可供所有人访问…”[39]

俄罗斯联邦：“各国应平等参与国际互联网治理，并在互联网治理中承担同等责任。”[40]

---

[35]联合国网络电视，（第 3 次会议）2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组，第二次实质性会议，2022 年 3 月 29 日，https://media.un.org/en/asset/k1l/k1l7rcax4f（从 1:35:05 开始）；另请参阅：伊朗伊斯兰共和国代表团在信息和通信技术安全和使用问题不限成员名额工作组第二次实质性会议上的意见声明，2022 年 3 月 29 日，第 3 页，https://documents.unoda.org/wp-content/uploads/2022/03/1-Introductory-Remarks-Existing-and-Potential-Threats.pdf

[36]另请参阅联合国秘书长组建的数字合作高层专家小组，https://www.un.org/en/sg-digital-cooperation-panel

[37]领导小组和多利益相关方咨询团体致 GDC 联合协调员的联名信函，“联合国互联网治理论坛随时准备承担由《全球数字契约》定期多利益相关方审核与跟进所产生的职责”，2023 年 10 月 16 日，https://www.intgovforum.org/en/filedepot_download/24/26649

[38]联合国网络电视，（第 3 次会议）2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组，第二次实质性会议，第 3 次会议，2022 年 3 月 29 日，https://media.un.org/en/asset/k1l/k1l7rcax4f（从 15:07 开始）

[39]联合国网络电视，（第 5 次会议）2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组，第二次实质性会议，2022 年 3 月 30 日，https://media.un.org/en/asset/k1g/k1gu15nuh2（从 1:00:07 开始）

[40]联合国网络电视，（第 5 次会议）2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组，第二次实质性会议，2022 年 3 月 30 日，https://media.un.org/en/asset/k1g/k1gu15nuh2（从 1:10:18 开始）；另请参阅：俄罗斯

背景信息：尚无证据表明各国没能“平等参与国际互联网治理”，也无证据表明各国没有在互联网治理中“承担同等责任”。

中国：“我们认为，各国对其境内 ICT 基础设施和资源及活动拥有管辖权。任何国家都不得利用 ICT 侵害他国的关键基础设施，也不得破坏和窃取此类基础设施的重要数据。 各国应完善立法，加强对关键信息基础设施的保护”[...]“中国自 2021 年 9 月 1 日起正式施行《关键信息基础设施安全保护条例》。按照该《条例》，关键信息基础设施是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。中国期待，OEWG 基于主权原则深入探讨关于关键基础设施的定义和保护措施。”[41]

葡萄牙：“在针对互联网核心的攻击中，或者在意图破坏选举过程公正性的攻击中，IP 操纵也可能发挥至关重要的作用。”[42]

新加坡：“对互联网的一般可用性或完整性至关重要的技术基础设施便属于一种关键基础设施。”[43]

俄罗斯联邦：“在当前的 ICT 发展阶段，如果不对规范全球通信网络运行的既有协议进行深入变革，并组织各国之间开展必要合作，似乎就不可能准确无误地识别危害行为的根源。鉴于此，需要建立明确的合作机制，促进具备相应权限的国家机构之间开展合作，正如 CERT 与 CERT 之间的合作，这一点至关重要。”[44]

背景信息：没有证据表明，需要通过“[互联网] 深入变革”才能达到上述目的。从世界各地大量的刑事案件来看，执法机构能够成功确定危害行为的根源。[45]

2022 年 3 月 31 日

加拿大：“具体而言，在欧洲安全与合作组织，我们携手哈萨克斯坦，共同倡导支持 CBM 4。CBM 4 旨在促进各国之间相互分享保障互联网开放性、安全性和互用性的有效方法。这项工作有

联邦代表团团长弗拉基米尔 • 申 (V. Shin) 的意见声明，2022 年 3 月 30 日，第 3 页，https://documents.unoda.org/wp-content/uploads/2022/03/Russia-OEWG-statement-3-30.03.2022-Eng.pdf

[41]联合国网络电视，（第 5 次会议）2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组，第二次实质性会议，2022 年 3 月 30 日，https://media.un.org/en/asset/k1g/k1gu15nuh2（从 1:57:29 开始）

[42]联合国网络电视，（第 5 次会议）2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组，第二次实质性会议，2022 年 3 月 30 日，https://media.un.org/en/asset/k1g/k1gu15nuh2（从 2:06:50 开始）

[43]联合国网络电视，（第 5 次会议）2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组，第二次实质性会议，2022 年 3 月 30 日，https://media.un.org/en/asset/k1g/k1gu15nuh2（从 2:36:05 开始）

[44]联合国网络电视，（第 6 次会议）2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组，第二次实质性会议，2022 年 3 月 30 日，https://media.un.org/en/asset/k1j/k1jpaw8mgf（从 34:40 开始）

[45]请参阅俄罗斯联邦内务部 (MVD) 关于 2022 年 1 月至 11 月期间俄罗斯犯罪状况的报告，第 3 页，第 9 点，https://d-russia.ru/wp-content/uploads/2022/12/mvd_22_11_.pdf；2022 年美国联邦调查局互联网犯罪报告，第 8 页，https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf；印度犯罪情况报告，印度内政部下属国家犯罪记录局，表 9A.2 网络犯罪 -《信息技术法案》相关案件（按犯罪类型细分以及按邦/联邦属地细分）- 2021 年，https://ncrb.gov.in/uploads/nationalcrimerecordsbureau/post/1679661922TABLE9A2.pdf

望帮助维护互联网的一般可用性和完整性，这是荷兰和其他国家代表在本周的发言中所提及的共同目标。”[46]

伊朗伊斯兰共和国：“我们应将在网络空间建立信任的措施 (Trust and Confidence-Building Measures, TCBM) 引入 ICT 环境，以解决致使 ICT 环境缺乏信任的主要根源，具体包括：互联网治理垄断、匿名机制、充满攻击性的网络策略和政策、敌对形象塑造和仇外心理、单方面强制措施、私营公司和平台及民族国家对境外活动缺乏责任感等。

我们坚信，各国应朝着同一个目标出发，即实现多边、公平、透明的互联网治理。在我们看来，管理上的垄断以及主客体的匿名性是导致互联网空间缺乏信任的主要根源，因此有必要制定相应的建立信任措施。当务之急是要解决当前互联网治理体系的弊端和缺陷，唯有如此，才能实现期待已久的公平公正的互联网治理。”[47]

第三次实质性会议

2022 年 7 月 25 日

副秘书长中满泉：“欢迎各利益相关方开展更多、更深入的互动交流，共同探讨如何加强关键基础设施和关键信息基础设施保护，并提出相应建议。这是为了响应秘书长的号召，将制定措施加强保护包括医疗卫生部门在内的关键基础设施作为重中之重。”[48]

以及：“鉴于 ICT 的特殊性质，以及非政府实体在管理众多 ICT 资源方面所起到的核心作用，我一再强调，必须要开放包容，持续推动各利益相关方参与其中。”[49]

欧盟： “关键基础设施清单中也包含有争议的元素。首先，从我们的经验来看，关于就关键基础设施术语和清单达成一致的提案，很难通过磋商在各国之间达成共识。根据以往的多边磋商和区域谈判经验，磋商通常是充满分歧、十分耗时的过程，就关键基础设施清单而言，这可能意味着有争议的元素是可以接受的。”[50]

中国：“事实上，我相信在座的其他同事也意识到，ICT 环境日渐呈现分化趋势。联合国秘书长古特雷斯在连续两届联合国大会一般性辩论中提醒国际社会，ICT 环境和网络空间面临的分裂风险在逐步上升。因此，ICT 环境分化是我们必须要直面和商议的一项重大议题。如果网络世界分裂或割裂成不同的阵营，那么将没有一套统一的适用规则。如此一来，我们将无法就国际规则的

[46]联合国网络电视，（第 7 次会议）2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组，第二次实质性会议，2022 年 3 月 31 日，https://media.un.org/en/asset/k1i/k1iykegjsm（从 22:40 开始）
[47]联合国网络电视，（第 7 次会议）2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组，第二次实质性会议，2022 年 3 月 31 日，https://media.un.org/en/asset/k1i/k1iykegjsm（从 31:50 开始）；另请参阅：伊朗伊斯兰共和国常驻联合国代表团一等参赞海达尔 • 阿里 • 巴鲁吉 (Heidar Ali Balouji) 的意见声明，2022 年 3 月 31 日，第 1 页，https://documents.unoda.org/wp-content/uploads/2022/03/4-CBMs.pdf
[48]联合国网络电视，（第 1 次会议）2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组，第三次实质性会议，2022 年 7 月 25 日，https://media.un.org/en/asset/k1u/k1uo46thhm（从 5:53 开始）
[49]联合国网络电视，（第 1 次会议）2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组，第三次实质性会议，2022 年 7 月 25 日，https://media.un.org/en/asset/k1u/k1uo46thhm（从 7:54 开始）
[50]联合国网络电视，（第 1 次会议）2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组，第三次实质性会议，2022 年 7 月 25 日，https://media.un.org/en/asset/k1u/k1uo46thhm（从 2:07:34 开始）

实施或适用范围达成共识，更不可能构建网络空间的建立信任措施。我希望，我们能够重视部分现有威胁和潜在威胁，并着手商议如何解决 ICT 环境目前存在的最重要、最突出的问题。”[51]

西班牙：“关于网络威胁，我们建议通过报告来介绍网络空间中存在的种种威胁，以及这些威胁对数字社会运行、公民个人以及国家机构运作所产生的影响；我们还建议，应通过制定技术规范和标准，来确保个人数据和知识产权在跨境和国际交流过程中得到有效保护。欧洲《通用数据保护条例》针对数据交换设定了高标准的稳定性和安全性要求。安全保障越大，保护力度就越高，公民和企业交换数据的意愿也就越高。”[52]

巴西：“最后，该报告在谈及互联网碎片化风险时，也提到了互联网治理轨道的相关讨论，强调确保互联网可用性和完整性。我们欢迎报告提出这一关切，但需要注意的是，这不是讨论更广泛的互联网治理问题的适当场合。”[53]

俄罗斯联邦：“报告预稿有必要包含关于确保互联网可访问以及安全稳定运行的措施，并强调各国在各自国家信息空间中享有主权。另外，还需强调，应确保各国平等参与互联网管理。”[54]

背景信息：互联网治理涉及到的国家参与问题一直在 WSIS 期间进行讨论和解决。全球互联网由数以千计的互联网络组成，这些网络由不同实体独立拥有和管理，其中一些由政府拥有和管理。没有证据表明各国无权“平等参与…互联网管理。”

俄罗斯联邦：“在加强与 ICT 安全领域中非政府主体的互动方面，我们认为，听取对保护关键基础设施（包括关键信息基础设施）负有直接责任的相关各方的意见大有裨益。开展这种互动交流的前提是，应了解各国政府在保护关键基础设施方面所起到的主要作用。”[55]

喀麦隆：“我们认为，有必要支持各国竭尽所能，全力填补漏洞并解决 IP 地址问题。”[56]

荷兰：“我们支持提及‘互联网的一般可用性和完整性’这一概念。但我方有一条修改建议，这一概念的表述应与 2021 年 OEWG 和 GGE 报告相一致。在这些报告中，这一概念表述为：‘对互联网的一般可用性或完整性至关重要的技术基础设施’。”[57]

---

[51]联合国网络电视，（第 1 次会议）2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组，第三次实质性会议，2022 年 7 月 25 日，https://media.un.org/en/asset/k1u/k1uo46thhm（从 2:26:14 开始）
[52]联合国网络电视，（第 1 次会议）2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组，第三次实质性会议，2022 年 7 月 25 日，https://media.un.org/en/asset/k1u/k1uo46thhm（从 2:41:52 开始）
[53]联合国网络电视，（第 2 次会议）2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组，第三次实质性会议，2022 年 7 月 25 日，https://media.un.org/en/asset/k1a/k1a978izhq（从 7:52 开始）；另请参阅：巴西代表团关于进展报告草案（章节：简介、威胁、规范）的意见声明，2022 年 7 月 27 日，第 2 页，https://documents.unoda.org/wp-content/uploads/2022/07/Brazil-part-1.pdf
[54]联合国网络电视，（第 2 次会议）2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组，第三次实质性会议，2022 年 7 月 25 日，https://media.un.org/en/asset/k1a/k1a978izhq（从 27:10 开始）
[55]联合国网络电视，（第 2 次会议）2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组，第三次实质性会议，2022 年 7 月 25 日，https://media.un.org/en/asset/k1a/k1a978izhq（从 27:45 开始）
[56]联合国网络电视，（第 2 次会议）2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组，第三次实质性会议，2022 年 7 月 25 日，https://media.un.org/en/asset/k1a/k1a978izhq（从 43:42 开始）
[57]联合国网络电视，（第 2 次会议）2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组，第三次实质性会议，2022 年 7 月 25 日，https://media.un.org/en/asset/k1a/k1a978izhq（从 1:31:53 开始）

2022 年 7 月 27 日

巴基斯坦：“巴基斯坦强烈支持‘建立信任措施’这一想法，也支持实施建议的后续措施，以此推动各成员国计算机紧急事件响应小组之间加强合作，处理好事件调查或互联网协议请求，并解决网络归属方面的技术障碍。”[58]

2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组第一份年度进展报告

OEWG 的第一份年度进展报告总结了各代表团在 2021-2022 年 OEWG 会议上开展的讨论以及提出的意见和建议。因此，这是一份记录了共识意见的文件，为 2023 年的讨论奠定了基础。[59]

2022 年 8 月 8 日

OEWG 第一份年度进展报告：“尤为令人关切的是，恶意 ICT 活动影响到关键信息基础设施、向公众提供基本服务的基础设施、对互联网的一般可用性或完整性至关重要的技术基础设施以及医疗领域实体。”

背景信息：上述文字摘自 2021 年联合国政府专家组 (Group of Governmental Experts, GGE) 报告。[60]

OEWG 第一份年度进展报告：“各国可以加强彼此之间，以及与企业、非政府组织和学术界等各利益相关方之间的协作与合作。各国已注意到，各利益相关方已通过与各国建立合作关系，在培训、研究以及促进互联网和数字服务访问方面发挥着重要作用。”[61] [62]

[58]联合国网络电视，（第 5 次会议）2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组，第三次实质性会议，2022 年 7 月 27 日，https://media.un.org/en/asset/k10/k100qzajqy（从 8:35 开始）

[59] 2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组报告，2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组，最终报告，2022 年 8 月 22 日，https://meetings.unoda.org/meeting/57871/documents?f%5B0%5D=document_type_meeting%3AFinal%20reports

[60]2021 年 GGE 报告，A/76/135，联合国大会第 76/19 号共识决议，2021 年 7 月 14 日，第 10 段，https://documents.un.org/prod/ods.nsf/xpSearchResultsM.xsp

[61]2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组第一份年度进展报告，2022 年 8 月 8 日，第 13 页，https://documents-dds-ny.un.org/doc/UNDOC/GEN/N22/454/03/PDF/N2245403.pdf?OpenElement

[62]俄罗斯联邦和乌克兰代表反对一些非政府实体参与 OEWG 工作。按照各成员国之前就非政府实体参与方式达成的共识意见，共有 32 个非政府实体被排除在 OEWG 会议拟定认证名单之外。该共识意见明确指出，未经联合国经济及社会理事会认证的实体必须在无异议的情况下，才能参与 OEWG 工作。乌克兰反对 5 个来自俄罗斯的组织参与 OEWG 工作。俄罗斯反对的组织包括：10 个来自美国的组织，4 个来自英国的组织，3 个国际组织，2 个来自德国的组织，以及其他 8 个组织，分别来自澳大利亚、芬兰、法国、爱尔兰、尼日利亚、西班牙、瑞士和乌干达。

非正式磋商

OEWG 主席在闭会期间召开了几次非正式磋商会议。以下引文摘自 OEWG 网站上发布的材料。

2022 年 12 月 7 日，俄罗斯在 OEWG 非正式磋商中提交了以下意见声明：“在当前的 ICT 发展阶段，如果不从根本上变革全球通信网络协议，并组织各国之间开展必要合作，就不可能稳妥可靠、准确无误地识别恶意活动的根源。鉴于此，建立明确的互动交流机制，促进具备有效管辖权的国家机构之间开展合作，变得尤为重要。”[63]

背景信息：俄罗斯联邦表示需要“从根本上变革互联网协议”以达成上述目的，但未提供任何证据来支撑这一观点。目前有一些常用的互联网协议，如传输控制协议/互联网协议 (Transmission Control Protocol/Internet Protocol, TCP/IP)，正是有了这些协议，设备之间才能进行通信。TCP/IP 协议族由互联网工程任务组 (IETF) 负责管理维护。任何关于 TCP/IP 协议族的变更均由 IETF 处理，而 IETF 是一个完全开放的组织。

在这份意见声明中，俄罗斯还表示：“在打击出于恐怖主义和犯罪目的使用 ICT、制止非法内容和虚假信息传播，以及推进互联网治理国际化进程方面，尚无获得公认的统一行动规范。”[64]

背景信息：如前所述，WSIS《突尼斯议程》和 WSIS+10 成果文件是国际公认的纲领性文件，其中不仅阐述了互联网治理多利益相关方模式，还明确声明这一模式是国际社会精诚合作的结果。

第四次实质性会议[65]

2023 年 3 月 7 日，新加坡表示：“我们还回顾了‘主席总结’附录中关于保护对互联网一般可用性或完整性至关重要的技术基础设施的建议。这类技术基础设施包括 DNS（域名系统）或互联网交换点等，对发达国家和发展中国家都很重要，因为所有国家都越来越依赖基于 ICT 的技术。我们支持在 OEWG 内进一步探讨有助于保障互联网可用性或完整性的可行措施。”[66]

[63]俄罗斯联邦代表在 2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组闭会期间非正式会议上发表的意见声明，纽约，2022 年 12 月 7 日，第 1 页，https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Russia_-_statement_on_international_law_-_OEWG_intersessionals_07.12.2022.pdf

[64]俄罗斯联邦代表在 2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组闭会期间非正式会议上发表的意见声明，纽约，2022 年 12 月 7 日，第 2 页，https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Russia_-_statement_on_international_law_-_OEWG_intersessionals_07.12.2022.pdf

[65]在 OEWG 第四次实质性会议期间发表的一些意见声明中，有些声明内容与本最新资讯报告前文已引用的声明内容重复。

[66]联合国网络电视，（第 3 次会议）信息和通信技术 (ICT) 不限成员名额工作组 - 第四次实质性会议，2023 年 3 月 7 日，（从 2:11:30 开始），https://media.un.org/en/asset/k1a/k1ah2cv3gr

第五次实质性会议

2023 年 7 月 27 日，葡萄牙代表团还谈及未列入 OEWG 年度报告的四项内容：“…3.重申应务必确保基础服务和关键基础设施免遭恶意网络攻击；4.承认包括技术平台在内的所有利益相关方对于…关键基础设施保护框架内的每个支柱都起着重要作用…”[67]

2023 年 7 月 28 日，俄罗斯代表团引用俄非峰会关于 ICT 主题的宣言[68]，发表了以下意见声明：“我们注意到，有必要促进俄罗斯联邦与非洲各国在联合国体系下的国际组织中，以及在 ITU 中就邮政服务问题加强协调，特别是在制定有关 ICT 发展方面的文件时。我们开展行动的事实依据是，《信息社会突尼斯议程》应该与时俱进，不断发展。该议程于 2005 年在 WSIS 论坛上获准通过。我们支持在联合国的带领下，建立一个更加公平均衡的国际互联网治理体系，避免任何单方面的政治权利限制或商业利益倾斜，确保全球网络关键信息基础设施的安全与稳定。”[69]

背景信息：没有证据表明，当前体系存在任何限制，并因此威胁“全球网络关键信息基础设施的安全与稳定”。此外，没有证据表明现有的国际互联网治理体系不均衡，也无证据表明需要将现有体系转变为由包括联合国在内的国际政府间组织来主导。事实上，在现有体系下，俄罗斯联邦正是以 ICANN 政府咨询委员会成员的身份参与互联网治理工作。[70]

2023 年 7 月 28 日，OEWG 通过了第二份年度进展报告草案。[71]该报告包含以下内容：

“另外，各国还着重指出，针对关键基础设施和关键信息基础设施的恶意 ICT 活动，破坏了人们对政治和选举进程、公共机构的信任和信心，或影响了互联网的一般可用性或完整性，是一个真实存在且日益严重的问题。各国表示，旨在干涉他国内政的恶意 ICT 活动尤其令人担忧。”[72]

“各国强调保护关键基础设施 (Critical Infrastructure, CI) 和关键信息基础设施 (Critical Information Infrastructure, CII) 的重要性。他们着重指出，恶意 ICT 活动旨在破坏 CI 或 CII，或者以其他方式阻止使用和运行 CI 或 CII 来向公众提供服务，可能会在国家、地区和全球层面产生级联影响。这类活动对公众造成危害的风险有所增加，并且可能进一步升级。因此，各国强调需要继续增强保护措施，保障所有 CI 和 CII 免受 ICT 威胁侵害，并建议增进关于最佳 CI 和 CII 保护措施的互动交流，包括分享国家政策，以及发生涉及 CI 和 CII 的 ICT 事件后可采取的恢复措施。在这方面，各国重谈联合国大会第 58/199 号决议，即“创建全球网络安全文化以及保护关

[67]联合国网络电视，（第 8 次会议）信息和通信技术 (ICT) 不限成员名额工作组 - 第五次实质性会议，2023 年 7 月 27 日，（从 2:11:52 开始），https://media.un.org/en/asset/k1n/k1ngmoogyi
[68]第二届俄非峰会关于国际信息安全领域合作的宣言，2023 年 7 月 28 日，第 7 段，http://en.kremlin.ru/supplement/5975
[69]联合国网络电视，（第 10 次会议）信息和通信技术 (ICT) 不限成员名额工作组 - 第五次实质性会议，2023 年 7 月 28 日，（从 11:00 开始），https://media.un.org/en/asset/k1s/k1san5j55u
[70]ICANN | GAC，政府咨询委员会，https://gac.icann.org/
[71]2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组报告，2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组，最终报告，2023 年 8 月 1 日，https://meetings.unoda.org/meeting/57871/documents?f%5B0%5D=document_type_meeting%3AFinal%20reports
[72]2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组第五次实质性会议，纽约，2023 年 7 月 24 日 - 28 日，第二份年度进展报告，第 6 页，https://documents-dds-ny.un.org/doc/UNDOC/LTD/N23/227/59/PDF/N2322759.pdf?OpenElement

键信息基础设施”，以及该决议的附录。另外，各国还建议，在发展中国家和小国请求帮助确定其国内的 CI 和 CII 时，应给予相应支持。”[73]

该年度进展报告还包含以下建议：“在 OEWG 第六次、第七次和第八次会议上，各国还应重点讨论以下事项：(a) 增强保护措施，保障 CI 和 CII 免受 ICT 威胁侵害，包括分享关于 ICT 安全事件检测、防御或应对以及恢复的最佳做法；在发展中国家和小国请求帮助识别其国内的 CI 和 CII 时，给予相应支持；(b) 进一步加强合作与援助，保障供应链完整性，防止有害的隐藏功能得到使用。”[74]

[73]同上，第 8 页
[74]同上，第 9 页

联合国为拟订关于打击出于犯罪目的使用信息和通信技术行为的全面国际公约而设立的特设专家委员会 (AHC)[75]

第一次会议（与 AHC 第一次会议相关的提交文件）[76]

2021 年 6 月 29 日

俄罗斯联邦：“‘关键信息基础设施’是指各种关键信息基础设施以及用于连接这些关键信息基础设施的电信网络的集合；n)‘关键基础设施’是指公共权威机构使用的信息系统及信息和通信网络，以及在国防、医疗、教育、交通、通信、能源、银行和金融部门、核能及对国家和社会生活至关重要的其他行业运行的信息系统和自动化过程控制系统”。[77]

2021 年 11 月 8 日

国际刑警组织：“在当前监管环境中，执法机构对关键域名注册信息（即 WHOIS 数据）的访问权限受到限制。为帮助全球执法机构应对这一重大挑战，国际刑警组织设计并推出了一个设有限制门槛的新门户系统，这个系统旨在为经过审查的执法机构自动提供对域名注册信息的访问权限，目前处于试点测试阶段。在该系统成功渡过试点阶段后，国际刑警组织会将这一解决方案纳入其全球警务能力，并签订必要的法律协议，以扩大参与的私营运营商库，并向各成员国开放该系统。”[78]

第二次会议（与 AHC 第二次会议相关的提交文件）[79]

2022 年 4 月 7 日

俄罗斯联邦（代表白俄罗斯、布隆迪、中国、尼加拉瓜和塔吉克斯坦）：“各缔约国应采取必要的立法和其他措施，授权其主管机关下令：[...] (b) 在该缔约国境内提供其服务的服务提供商提交该服务提供商拥有或控制的订阅者信息。”[...]“就本条款而言，‘订阅者信息’一词是指服务提

[75]本章包含来自六次 AHC 会议的发言内容。从章节结构上看，首先是第一次和第二次会议中的发言内容。来自 AHC 第三次会议的发言内容还包括现场讨论录音。第四次和第五次会议的最终成果是发布了一份题为“合并谈判文件”的文本草案，而第六次会议的成果是“公约文本草案”。本章引用了这两份草案文件中的相关内容。请参阅：为拟订关于打击出于犯罪目的使用信息和通信技术行为的全面国际公约而设立的特设专家委员会，特设专家委员会会议：会议，https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

[76]特设专家委员会第一次会议，纽约，2022 年 2 月 28 日至 3 月 11 日，各成员国提交的与特设专家委员会第一次会议相关的文件，https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-first-session.html

[77]关于打击出于犯罪目的使用信息和通信技术行为的联合国公约，草案，非官方译文，俄罗斯联邦提交的与特设专家委员会第一次会议相关的文件，2021 年 6 月 29 日，第 6 页，https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_E.pdf

[78]国际刑警组织为拟订关于打击出于犯罪目的使用信息和通信技术行为的全面国际公约而提交的贡献提案，国际刑警组织提交的与特设专家委员会第一次会议相关的文件，2021 年 11 月 8 日，第 6 页，https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/IGOs/21COM1175-SRIUN_UseInformation_CriminalPurposes_complet.pdf

[79] 特设专家委员会的第二次会议，维也纳，2022 年 5 月 30 日至 6 月 10 日，与特设专家委员会第二次会议相关的提交文件，https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-second-session.html

供商除流量数据或内容数据之外所掌握的与其服务订阅者有关的所有信息，根据这些信息可以确定：”“b) 服务协议或安排中提供的订阅者身份、邮政地址或其他地址、电话和其他联系号码，其中包括 IP 地址以及账单和付款信息；(c) 与对服务协议或安排产生影响的信息和电信设备的位置相关的信息。”[80]

2022 年 4 月 8 日

巴西：“(i)‘订阅者数据’是指服务提供商在正常的经营活动中收集的所有计算机数据，涉及姓名、出生日期、邮政地址或地理地址、账单和付款数据、设备标识符、电话号码或电子邮件地址，或者任何其他信息，例如创建帐户时使用的 IP 地址，这些信息可用于识别订阅者或客户，以及所提供服务的类型和与服务提供商签订合同的期限，但流量数据或内容数据除外。”[81]

伊朗伊斯兰共和国：“公约应明确指出和规定私营部门、服务提供商及其他类似实体与执法机构合作的义务和法规，特别是在国际级别开展全球性或实质性外展活动的部门和提供商。”[82]

日本：“本公约不应涉及网络安全和互联网治理问题。例如，以下措施将对合法的经济活动产生寒蝉效应，阻碍技术发展，并将超出特设专家委员会的职权范围：

- 根据本公约制定安全标准；
- 对法人和个人强加遵守此类标准的义务，或对违反此类标准施加惩罚；或
- 追究法人、其代表或软件创建者在不知情的情况下无意中参与其他行为者实施的网络犯罪的责任。”[83]

2022 年 4 月 9 日

加拿大：建议将“计算机数据”定义为“适合在计算机系统中处理的事实、信息或概念的任何表现形式，包括适合让计算机系统执行某项功能的程序”。该定义包括所有类型的数据：内容数据（实际信息）、计算机程序、流量数据、订阅者信息、密码和连接代码。根据同一贡献提案，“流量数据”是指“任何计算机数据，可用于识别、激活或配置与通过计算机系统创建、传输或接收通信相关的设备，这些数据由构成通信链一部分的计算机系统生成，表示通信的起始地、目的地或终点、路由、时间、日期、大小、持续时间或基础服务类型。对于电话和互联网服务而言，该定义包括用于拨号、路由和寻址或发送信号所需的数据，例如：电话号码、通话的日期和时间（以及通话数据日志中的其他元素）、信息的来源和目的地（例如通信起始地、目的地或终

[80] 俄罗斯联邦（同时代表白俄罗斯、布隆迪、中国、尼加拉瓜和塔吉克斯坦）提交的与特设专家委员会第二次会议相关的文件，2022 年 4 月 7 日，第 13 页，
https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Russia_Contribution_E.pdf
[81] 巴西关于《联合国网络犯罪公约》最初章节的提案，巴西提交的与特设专家委员会第二次会议相关的文件，2022 年 4 月 8 日，第 2 页，
https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Brazil_Contribution_E.pdf
[82] 伊朗伊斯兰共和国提交的与特设专家委员会第二次会议相关的文件，2022 年 4 月 8 日，第 4 页，
https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Islamic_Republic_of_Iran_contribution.pdf
[83] 日本，关于刑事定罪、一般规定、程序性措施和执法的贡献提案，日本提交的与特设专家委员会第二次会议相关的文件，2022 年 4 月 8 日，第 5-6 页，
https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Japan_Contribution.pdf

点、路由、时间、日期、大小、持续时间或基础服务类型，电子邮件或文本信息），以及 IP 地址和与所用协议相关的数据。”[84]

2022 年 4 月 12 日

越南：建议将网络空间定义为“信息技术 (Information Technology, IT) 基础设施网络，包括电信网络、互联网、计算机网络、通信系统、信息处理和控制系统、数据库。”[85]

2022 年 4 月 13 日

墨西哥：“墨西哥认为必须就以下问题添加其他一般条款：[...] 承认互联网的公共核心以及网络中立方法对于公约宗旨的相关性。”[86]

2022 年 4 月 14 日

南非：“各缔约国应根据本国法律的基本原则，对其司法管辖范围内的所有域名注册服务机构、加密资产交易商和加密资产的可标识信息进行注册，并向主管机关提供此类信息，以用于调查和取证。”[87]

第三次会议（与 AHC 第三次会议相关的提交文件）[88]

2022 年 8 月 29 日

伊朗伊斯兰共和国：“私营实体（例如服务提供商，包括域名领域的服务提供商）在打击通过 ICT 执行的犯罪方面发挥着特别重要的作用。鉴于滥用所提供服务的犯罪活动猖獗，此类实体与执法机构的合作及其在这一领域开展的尽职调查仍然至关重要，特别是在国际级别开展大量外展和活动的实体。在这方面，公约应该针对这些实体与执法机构的有效合作规定相关法规和义务。这些实体还应尊重各国的经济、社会、法律和文化特点。”[89]

中国：“各国不得违反数据存储地国家的法律，通过批准网络安全保护措施，从企业或个人或者利用技术手段直接收集存储在国外的数据。”[90]

---

[84]加拿大，针对在特设专家委员会第二次会议期间将审查的特定章节和条款提交的文本草案和贡献提案，即关于刑事定罪、一般规定、程序性措施和执法的贡献提案，2022 年 4 月 9 日，第 1 页，https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Canada_Contribution.pdf

[85] 越南提交的与特设专家委员会第二次会议相关的文件，2022 年 4 月 12 日，第 1 页，https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Vietnam_Contribution.pdf

[86] 墨西哥政府提交的供特设专家委员会在其第二次实质性会议上审议的贡献提案，2022 年 4 月 13 日，第 3 页，https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Mexico_Contribution.pdf

[87] 南非针对刑事定罪条款、一般条款以及程序性措施和执法条款的贡献提案，2022 年 4 月 14 日，第 13 页，https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/South_Africas_contribution.pdf

[88] 特设专家委员会的第三次会议，2022 年 8 月 29 日至 9 月 9 日，纽约，与特设专家委员会第三次会议相关的提交文件，https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_third_session/main.html

[89] 联合国网络电视，（第 1 次会议）为打击出于犯罪目的使用 ICT 的行为而设立的特设专家委员会第三次会议，2022 年 8 月 29 日，（从 1:08:56 开始），https://media.un.org/en/asset/k1x/k1xh926qrt

[90] 联合国网络电视，（第 1 次会议）为打击出于犯罪目的使用 ICT 的行为而设立的特设专家委员会第三次会议，2022 年 8 月 29 日，（从 2:13:22 开始），https://media.un.org/en/asset/k1x/k1xh926qrt

加拿大：“尽管加拿大不反对将第 32 条纳入《布达佩斯公约》，但我们认为，鉴于我们对该公约开展工作的时间紧迫，而且该条款是经过长时间讨论的结果，因此要就这样一个条款达成共识可能很困难。”[91]

背景信息：《布达佩斯网络犯罪公约》关于经同意或在可公开获取的情况下跨境访问存储的计算机数据的第 32 条内容如下：

“缔约国一方可不经另一方缔约国的授权：

a. 访问公众能够获得的（开源）存储于计算机中的数据，而不论该数据存储在何处；或

在该缔约国一方已从合法权利人处取得合法且自愿许可，允许通过电脑系统向其披露数据的前提下，通过其境内的计算机系统，访问或接收位于另一方缔约国的存储计算机数据。”[92]

智利：“但是除了证据之外，还需要所有犯罪行为的基本证据，这包括互联网或与网络相关的任何其他程序，或者可能被用来支持或不支持犯罪的其他程序。”[93]

2022 年 9 月 1 日

厄瓜多尔：“在这方面，厄瓜多尔确定了几项需求。这些问题太多，现在无法一一列举，但我可以举例说明当前互联网服务提供商的问题，因为他们不想要使用 IPv4 地址，因此他们不得不使用 CGNET 这样的协议，这使得成千上万的用户可以使用同一 IP 公共地址。这就很难确定实施网络犯罪的主体。在这方面，我们要求在未来的公约中增加一项条款，要求各缔约国制定内部规范，从而要求互联网服务提供商在合理的时间内将 IPv4 全部迁移到 IPv6。这样就有可能在调查网络犯罪方面取得有利成果，从而满足这个领域的技术援助要求。”[94]

主席就这一问题发表了评论：“与大家所见相同，IP 地址存在着各种差异，这给了我们很大的进步空间，让我们看到在技术理解层面存在着巨大差异。”[95]

阿曼：“我赞同厄瓜多尔代表关于交流工作机制以及从第 4 版协议转向第 6 版协议的重要性所做的发言。在打击网络犯罪方面，这将对 [...] 产生积极影响。如果公司或服务提供商更改他们所使用的协议，我指的是改为使用第 6 版协议，这将对打击网络犯罪产生更大的影响。”[96]

---

[91] 联合国网络电视，（第 2 次会议）为打击出于犯罪目的使用 ICT 的行为而设立的特设专家委员会第三次会议，2022 年 8 月 29 日，（从 1:43:42 开始），https://media.un.org/en/asset/k1j/k1jbh2v1z7

[92]欧洲理事会，《欧洲条约汇编》第 185 条，《网络犯罪公约》，布达佩斯，2001 年 11 月 23 日，第 17 页，https://rm.coe.int/1680081561

[93] 联合国网络电视，（第 2 次会议）为打击出于犯罪目的使用 ICT 的行为而设立的特设专家委员会第三次会议，2022 年 8 月 29 日，（从 2:37:05 开始），https://media.un.org/en/asset/k1j/k1jbh2v1z7

[94] 联合国网络电视，（第 8 次会议）为打击出于犯罪目的使用 ICT 的行为而设立的特设专家委员会第三次会议，2022 年 9 月 1 日，（从 1:54:12 开始），https://media.un.org/en/asset/k1o/k1o39wyquf

[95] 联合国网络电视，（第 8 次会议）为打击出于犯罪目的使用 ICT 的行为而设立的特设专家委员会第三次会议，2022 年 9 月 1 日，（从 1:58:09 开始），https://media.un.org/en/asset/k1o/k1o39wyquf

[96] 联合国网络电视，（第 8 次会议）为打击出于犯罪目的使用 ICT 的行为而设立的特设专家委员会第三次会议，2022 年 9 月 1 日，（从 02:06:20 开始），https://media.un.org/en/asset/k1o/k1o39wyquf

2022 年 9 月 7 日

巴基斯坦：“巴基斯坦一贯支持有关信心建立措施 (CBM) 的意见，并进一步提出以下建议行动，呼吁加强各成员国的计算机紧急事件响应小组 (Computer Emergency Response Team, CERT) 之间的合作，以处理互联网协议的调查/回溯请求，并解决网络归属方面的技术障碍。”[97]

俄罗斯：“俄罗斯联邦建议在文件（报告）中添加以下段落：[...]各国指出，务必要采取相应措施，在考虑到各国对信息空间主权的情况下，保障互联网的一般可用、安全和稳定运行，以及确保各国平等参与这一网络的治理。”[98]

背景信息：与在 OEWG 会议上的发言一样，俄罗斯并没有提供证据表明各国在参与互联网治理方面存在不平等现象。如上所述，俄罗斯联邦是 ICANN GAC 的成员之一，因此可以与所有其他 GAC 成员一起平等参与 ICANN 的工作。

AHC 的第四次会议[99]和第五次会议[100]

合并的 AHC 谈判文件：

在 AHC 的第五次会议之后，发布了状态为“截至 2023 年 4 月 21 日”的合并谈判文件。谈判文件载有特设专家委员会主席编写的《联合国网络犯罪公约》文本草案。各代表团并未接受所有建议，公约草案的文本还增加了更多内容。不过，我们在此引用了这段文字，因为它具有相关性。

2023 年 4 月 21 日

合并的谈判文件：

印度、巴基斯坦、美国、中国、新西兰、埃及、肯尼亚、苏丹、澳大利亚、俄罗斯、哥伦比亚、挪威、加拿大、坦桑尼亚、阿拉伯叙利亚共和国、阿尔及利亚、布基纳法索、新加坡、南非、尼加拉瓜、中国澳门、汤加、欧盟及其成员国和斐济声明，他们希望从关于序言、关于国际合作、预防措施、技术协助和实施机制条款以及关于打击出于犯罪目的使用信息和通信技术行为的全面国际公约最终条款的合并谈判文件中删除第 72 条“经同意或在可公开获得的情况下跨境获取所存储的 [计算机数据] [电子/数字信息]”草案。厄瓜多尔和委内瑞拉这两个国家赞同在编辑后保留此条款的文本。[101]条款全文如下：

---

[97] A/77/275 中所载关于解释采纳不限成员名额工作组进度报告的立场声明汇编，附录，2022 年 9 月 7 日，第 26 页，https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg-II/documents/compendium_2022.pdf

[98] A/77/275 中所载关于解释采纳不限成员名额工作组进度报告的立场声明汇编，附录，2022 年 9 月 7 日，第 37 页，https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg-II/documents/compendium_2022.pdf

[99] 本章并未引用特设专家委员会第四次会议中的任何内容。有关参考，请参阅特设专家委员会的第四次会议，2023 年 1 月 9 日至 20 日，维也纳，https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_fourth_session/main.html

[100] 特设专家委员会的第五次会议，2023 年 4 月 11 日至 21 日，维也纳，https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_fifth_session/main

[101] 为拟订关于打击出于犯罪目的使用信息和通信技术行为的全面国际公约而设立的特设专家委员会，第五次会议，2023 年 4 月 11 日至 21 日，关于序言、关于国际合作、预防措施、技术协助和实施机制条款以及

“缔约国一方可不经另一方缔约国的授权：
(a) 访问公众能够获得的（开源）存储于 [计算机中的数据] [电子/数字信息]，而不论该 [数据] [信息] 存储在何处；或
(b) 在该缔约国一方已从合法权利人处取得合法且自愿许可，允许通过相关计算机系统，向其披露 [数据] [信息]，从而访问或接收相关 [数据] [信息] 的前提下，通过其境内的 [计算机系统] [信息和通信技术系统/设备] 访问或接收位于另一方缔约国的存储 [计算机数据] [电子/数字信息]。”[102]

马来西亚、安哥拉和纳米比亚选择仅排除该条款草案的“b)”部分。

备注：为 AHC 第六次会议编写的公约文本草案后续试行本不包含类似于《布达佩斯网络犯罪公约》第 32 条的以下条款草案：“第 72 条‘经同意或在可公开获得的情况下跨境获取所存储的 [计算机数据] [电子/数字信息]”。[103]

AHC 的第六次会议[104]

AHC 第六次会议的工作于 2023 年 9 月 1 日结束。

公约文本草案（截至 2023 年 9 月 2 日的版本）

AHC 第六次会议编制了长达 80 页的《网络犯罪公约》草案文本。我们希望提请大家注意此文本的以下条款以及关于这些条款的备注。

“第 2 条：术语的使用。

[...]

(c)‘流量数据’是指服务提供商收集的与以下方面相关的所有 [计算机数据] [数字信息]，但不包括内容数据：(i) 所提供服务的类型及其持续时间，其中涉及技术数据，用于识别订阅者或客户使用或向其提供的相关技术措施或接口的数据，以及与验证服务的使用有关的数据，不包括由用户提供或应用户请求创建的密码或代替密码的其他认证方式；(ii) 服务的用户访问会话的开始和终止数据，例如使用的日期和时间，或者登录或注销服务的日期和时间；以及 (iii) 在电子通信网络中为传输、分发或交换内容数据而处理的通信元数据，其中包括用于追踪和识别通信来源和目的地

关于打击出于犯罪目的使用信息和通信技术行为的全面国际公约最终条款的合并谈判文件，第 38 页，2023 年 4 月 21 日，https://www.unodc.org/documents/Cybercrime/AdHocCommittee/5th_session/Documents/CND_2_-_21.04.2023.pdf

[102] 同上

[103] 为拟订关于打击出于犯罪目的使用信息和通信技术行为的全面国际公约而设立的特设专家委员会，第六次会议，2023 年 8 月 21 日至 9 月 1 日，公约草案（试行本），https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Pre-session-docs/A_AC_291_22_Advance_Copy.pdf

[104] 特设专家委员会的第六次会议，2023 年 8 月 21 日至 9 月 1 日，纽约，https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_sixth_session/main

的数据，关于提供通信服务时使用的终端设备位置的数据，以及通信的日期、时间、持续时间和类型；”[105]

备注：这与《布达佩斯网络犯罪公约》中提供的定义不同。根据《布达佩斯公约》：“流量数据是指与通过计算机系统进行的通信有关的任何计算机数据，这些数据由构成通信链一部分的计算机系统生成，指示通信的起始地、目的地、路由、时间、日期、大小、持续时间或基础服务类型。”[106]

《布达佩斯网络犯罪公约》针对“服务提供商”和“订阅者信息”提供了相同的定义[107]，但没有提供“内容数据”的定义。《联合国公约》草案对此作了定义。[108]

[...]

多米尼加共和国将该条款草案添加到“第 2 条：术语的使用”中。他们希望定义谁是“相关利益相关方”[109]。

俄罗斯联邦、伊朗、白俄罗斯、布基纳法索、委内瑞拉和埃及引入了：“第 10 条之二：非法干扰关键信息基础设施。
1.各缔约国应采取必要的立法和其他措施，根据本国法律将下列行为规定为犯罪：故意制作、传播和/或使用旨在非法干扰关键信息基础设施的软件或其他数字信息，包括用于破坏、阻止、修改、复制其中所含信息或使安全功能失效的软件或其他数字信息。2.各缔约国应采取必要的立法和其他措施，根据本国法律将下列行为规定为犯罪：违反为存储、处理和传输关键信息基础设施或信息系统或者属于关键信息基础设施的信息和通信网络中所载的受保护数字信息而设计的媒体运营规则，或违反访问这些媒体的规则（如果这种违反行为损害了关键信息基础设施）。”[110]

备注：澳大利亚、美国、欧盟及其成员国、新西兰、格鲁吉亚、挪威、英国、列支敦士登、加拿大、智利、日本和墨西哥反对将该条款纳入公约，并要求删除该条款。

中国、伊朗、俄罗斯联邦、委内瑞拉和埃及引入了：
“第 10 条之三：非法提供服务。

---

[105]为拟订关于打击出于犯罪目的使用信息和通信技术行为的全面国际公约而设立的特设专家委员会，第六次会议，2023 年 8 月 21 日至 9 月 1 日，公约文本草案（截至 2023 年 9 月 2 日的状态，其中包括各成员国的最新动态），第 3 页，https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/DTC/DTC_rolling_text_02.09.2023.pdf

[106] 欧洲理事会，《网络犯罪公约》，布达佩斯，11 月 23 日，第 3 页，https://rm.coe.int/1680081561

[107] 欧洲理事会，《欧洲条约汇编》第 185 条，《网络犯罪公约》，布达佩斯，2001 年 11 月 23 日，第 3 页和第 9 页，https://rm.coe.int/1680081561

[108] “(d)‘内容数据’是指与通过 [计算机系统] [信息和通信技术设备] 进行的通信有关的所有 [计算机数据] [数字信息]，涉及该通信的实质内容或主旨，如文本、语音信息、录音、录像和其他类型的信息。”《欧洲关于个人数据自动化处理的个人保护公约》针对“个人数据”进行了定义，这一术语在《联合国公约》草案文本中也有类似的表述：“个人数据”是指与确定的或可识别的自然人有关的数据。为拟订关于打击出于犯罪目的使用信息和通信技术行为的全面国际公约而设立的特设专家委员会，第六次会议，2023 年 8 月 21 日至 9 月 1 日，公约文本草案（截至 2023 年 9 月 2 日的状态，其中包括各成员国的最新动态），第 3-4 页，https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/DTC/DTC_rolling_text_02.09.2023.pdf

[109]同上，第 4 页

[110] 同上，第 9 页

各缔约国应采取必要的立法和其他措施，根据本国法律将下列在无权的情况下故意实施的行为规定为刑事犯罪：
(a) 提供服务或技术支持，其中包括互联网访问、服务器托管、在线存储、通信传输或类似服务；或
(b) 创建网站、通信网络，

意图将其服务或技术支持用于实施本公约所确立的任何犯罪。”[111]

备注：澳大利亚、美国、欧盟及其成员国、新西兰、格鲁吉亚、挪威、英国、列支敦士登、加拿大、日本和墨西哥反对将该条款纳入公约，并要求删除该条款。

俄罗斯联邦、马里、白俄罗斯、尼加拉瓜、布基纳法索、厄立特里亚、委内瑞拉、苏丹、古巴、尼日利亚、布隆迪、朝鲜、埃及、土耳其和塞拉利昂提交了：“第 15 条之七：与恐怖主义有关的犯罪。
各缔约国应采取必要的立法和其他措施，将下列利用信息和通信技术实施的行为规定为刑事犯罪：实施恐怖主义行为，煽动、招募或以其他方式参与恐怖活动，鼓吹恐怖主义并为其辩护，为实施恐怖主义行为筹集或提供资金，为实施恐怖主义行为提供培训，为恐怖主义组织及其成员之间的通信提供便利，包括建立、发布或使用网站，或为恐怖主义行为的实施者提供后勤支持，传播爆炸物的制造方法（特别是在实施恐怖主义行为中使用的制造方法），以及散布纷争、煽动叛乱、宣扬仇恨或种族主义。”[112]

备注：加拿大、美国、新西兰、多米尼加共和国、危地马拉、挪威、格鲁吉亚、澳大利亚、欧盟及其成员国、以色列、英国、黎巴嫩、列支敦士登、智利、日本和墨西哥反对将该条款纳入公约，并要求删除该条款。

阿尔及利亚、加拿大和俄罗斯联邦建议保留以下条款的原文：
第 21 条：起诉、裁决和制裁
[...]
“各缔约国可根据本国法律采取必要的立法和其他措施，规定根据本公约第 6 条至第 9 条确立的犯罪的加重处罚情形，包括影响关键信息基础设施的情形。”[113]

备注：列支敦士登、新西兰、挪威、坦桑尼亚、美国、欧盟及其成员国、瑞士、尼日利亚、以色列、菲律宾、澳大利亚、格鲁吉亚、挪威和加勒比海地区社群反对将该条款纳入公约，并要求删除该条款。

“第 26 条：流量数据的快速存留和部分披露
各缔约国应采取必要的立法和其他措施，就根据有关存储的 [计算机数据] [数字信息] 快速存留条款进行存留的流量数据，进行如下规定：[...](b) 确保快速向该缔约国的主管机关或该主管机关指定的人员披露足够数量的流量数据，使该缔约国能够确定通信或所显示信息所经过的服务提供商和传输路径。”[114]

[111] 同上，第 9 页
[112] 同上，第 19 页
[113] 同上，第 25 页
[114]为拟订关于打击出于犯罪目的使用信息和通信技术行为的全面国际公约而设立的特设专家委员会，第六次会议，2023 年 8 月 21 日至 9 月 1 日，公约草案（试行本），第 13 页，

“第 27 条：生产令
各缔约国应采取必要的立法和其他措施，授权其主管机关下令：[...](b) 要求该缔约国境内提供其服务的服务提供商，提交其拥有或控制的与此类服务有关的订阅者信息。”[115]

俄罗斯联邦、阿根廷、委内瑞拉、埃及和南非赞成保留以下条款的文本：
“第 29 条：实时收集流量数据[116] 1.各缔约国应采取必要的立法和其他措施，授权其主管机关：(a) 通过在该缔约国境内应用技术手段，收集或记录；以及 (b) 在其现有技术能力范围内，强制服务提供商：(i) 通过在该缔约国境内应用技术手段，收集或记录；或 (ii) 配合和协助主管机关，收集或记录：与其境内通过 [计算机系统] [信息和通信技术设备] 传输的特定通信有关的实时流量数据。2.如果缔约国由于其国内法律制度的原则而不能采取第 1 段 (a) 项所述措施，则可采取必要的立法和其他措施，以确保通过在其境内应用技术手段，实时收集或记录与在其境内传输的特定通信有关的流量数据。3.各缔约国应采取必要的立法和其他措施，责成服务提供者对执行本条规定的任何权力的事实以及与此有关的任何信息保密。”[117]

备注： 新加坡、瑞士、马来西亚和越南反对将该条款纳入公约，并要求删除该条款。

“第 36 条：保护个人数据。
1.缔约国依据本公约传输个人数据时，应该遵守该缔约国本国法律和适用的国际法。如果不能按照缔约国有关保护个人数据的适用法律提供个人数据，则不要求缔约国根据本公约传输个人数据。缔约国亦可根据此类适用法律寻求施加条件，以实现合规，从而对个人数据请求做出回应。鼓励缔约国建立双边或多边安排，以促进传输个人数据。”[118]

加勒比海地区社群、欧盟及其成员国、瓦努阿图、新西兰、阿尔巴尼亚、格鲁吉亚、美国、英国、中国、挪威、佛得角、坦桑尼亚、黎巴嫩、哥伦比亚、厄瓜多尔、巴基斯坦、瑞士、汤加和澳大利亚支持将以下条款纳入第 36 条：“第 1 条之二：在无法按照第 1 段的规定传输个人数据的情况下，缔约国可以寻求施加适当条件（遵守其关于保护个人数据的适用法律 [...]）以实现合规，从而对获取个人数据的请求做出积极回应。”[119]

备注：印度建议删除上述补充条款。

俄罗斯联邦提议将其添加到以下条款中：

---

https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Pre-session-docs/A_AC_291_22_Advance_Copy.pdf
[115]同上
[116] 2023 年 9 月 1 日，AHC 小组主席讨论了第 29 条和第 30 条（分别为“实时收集流量数据”和“截取内容数据”），并指出：“然而，关于第 29 条和第 30 条，一些代表团向协调员请求提出修订案的保留意见，并期望在委员会第 7 次会议上进一步讨论。”联合国网络电视，（第 23 次会议）为拟订关于打击出于犯罪目的使用信息和通信技术行为的全面国际公约而设立的特设专家委员会第六次会议，2023 年 9 月 1 日，（从 02:01:23 开始），https://media.un.org/en/asset/k17/k17lzfhyyp
[117] 为拟订关于打击出于犯罪目的使用信息和通信技术行为的全面国际公约而设立的特设专家委员会，第六次会议，2023 年 8 月 21 日至 9 月 1 日，公约文本草案（截至 2023 年 9 月 2 日的状态，其中包括成员国的最新动态），第 33 页，https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/DTC/DTC_rolling_text_02.09.2023.pdf
[118] 同上，第 38 页
[119] 同上

“第 40 条：与司法互助相关的一般原则和程序。[...]3.可针对下列任何目的请求依照本条规定提供司法互助：[...]（第 I 条之二）删除用于实施犯罪活动的域名。”[120]

“第 43 条：快速披露保留的流量数据
1.在执行根据第 42 条提出的保留有关特定通信的流量数据请求时，如果被请求的缔约国发现另一缔约国的服务提供商参与了该通信的传输，则被请求的缔约国应快速向提出请求的缔约国披露足够数量的流量数据，以查明该服务提供商和通信的传输路径。”[121]

第 45 条：实时收集流量数据的司法互助
1.各缔约国应相互提供司法协助，实时收集与本国境内通过 [计算机系统] [信息和通信技术设备] 传输的特定通信有关的流量数据。在不违反第 2 段条款的情况下，此类协助应遵循国内法规定的条件和程序”。

[...]

“3.根据本条款第 1 段提出的请求应具体说明：(c) 需要收集流量数据的 [计算机数据] [数字信息] 及其与犯罪行为或其他非法行为的关系；(d) 可识别数据所有者或使用者或者 [计算机系统] [信息和通信技术设备] 位置的任何可用数据；”[122]

背景信息：在第六次会议和 2024 年 1 月至 2 月举行的最后一次会议之间的闭会期间，AHC 一直在进行非正式谈判。未邀请多利益相关方参与这些谈判，这些谈判只面向政府。主席的目标是在 2023 年 11 月底之前制定一份经过删减的公约文本草案“简洁版”。

[120] 同上，第 47 页
[121] 对于这一规定，各缔约国一致同意“留待进一步审核”，同上，第 26 页
[122] 同上

《全球数字契约》和未来峰会

简介/背景

2020 年，秘书长古特雷斯的报告《我们的共同议程》提议举办一次未来峰会，通过技术轨道达成《全球数字契约》(GDC)：“此外，在数字合作路线图（参阅 A/74/821）建议的基础上，联合国、各国政府、私营部门和公民社会可以作为一个多利益相关方数字技术轨道联合起来，为未来峰会做好准备，就《全球数字契约》达成一致。这将勾勒出为所有人创造开放、自由和安全数字未来的共同原则。”[123]

《全球数字契约》

2023 年 4 月 25 日，联合国秘书长发布了第 5 号政策简报，其中特别包含联合国秘书长关于未来 GDC 框架参数的言辞。请参阅 ICANN 博文，其背景信息中引用了 GDC 的一些内容。[124]

各成员国、联盟和超国家组织针对 GDC 提交的书面文件摘录

背景信息：联合国技术事务特使办公室于 2023 年春季和夏季针对与 GDC 相关的问题组织了一系列的深入讨论。ICANN 的 GE 工作人员出席了这些演讲会，但审议过程未正式记录，GE 无法提供这些讨论的内容。不过，一些书面材料反映了各国代表团在审议期间的口头发言。

2023 年 4 月

2023 年 4 月 13 日，欧盟表示：“欧盟认为，[…] 互联网必须保持开放、全球化、自由、可互用和分散化。我们强烈支持采用多利益相关方方法来治理互联网，以确保包括各国政府、私营部门、公民社会和技术社群在内的所有行为者都能参与塑造互联网的未来。”
[…]
“关于推进多利益相关方方法的一个正面示例是，2016 年向 ICANN 成功移交了 IANA 管理权。欢迎包括各国政府在内的所有利益相关方积极参与 ICANN，帮助提高全球域名系统 (DNS) 的安全性与稳定性。”[125]

伊朗伊斯兰共和国表示：“在互联网治理生态系统管理机构、 IP 和管理系统监管机构，以及各国执法机构和司法机关之间，建立有效的合作框架，以预防和打击网络犯罪。”[126]

---

[123]《纪念联合国成立 75 周年宣言》，联合国大会于 2020 年 9 月 21 日通过的决议，A/RES/75/1，2020 年 9 月 28 日，https://documents.un.org/prod/ods.nsf/xpSearchResultsE.xsp
[124] ICANN 博文，2023 年 6 月 13 日，https://www.icann.org/zh/blogs/details/un-secretary-general-policy-report-considerations-for-the-icann-community-13-06-2023-zh
[125] 欧盟驻纽约联合国代表团，欧盟声明 --《全球数字契约》：深入探讨互联网治理，2023 年 4 月 13 日，https://www.eeas.europa.eu/delegations/un-new-york/eu-statement-global-digital-compact-deep-dive-internet-governance_en?s=63
[126] 伊朗伊斯兰共和国针对《全球数字契约》的贡献提案，2023 年 4 月，上次修改日期：2023 年 5 月 2 日，第 20 页，https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-submission_Islamic-Republic-Iran.pdf

荷兰表示：“《全球数字契约》应致力于避免互联网的技术基础设施碎片化，避免妨碍系统的互用能力，以及避免威胁互联网核心基础设施的总体完整性和可用性。这包括数据包路由和转发、命名和编号系统、加密 [技术]，以及底层物理基础设施。”[127]

G77 和中国表示：“《全球数字契约》应建立在推进数字合作的关键文件和论坛基础之上，其中包括信息社会世界峰会 (WSIS)，尤其是《突尼斯议程》和《日内瓦行动计划》、互联网治理论坛，并且还应将秘书长的数字合作路线图考虑在内。”
[…]
“77 国集团强调，WSIS 的成果应作为国际数字合作和互联网治理的指南予以保留，因为它是建立在有利于发展的原则基础之上。”
“《突尼斯议程》、《日内瓦原则宣言》和《日内瓦行动计划》将为建立包括 GDC 在内的任何新数字合作机制确定指导原则。”

[...]
“我们认识到，不应允许单个国家和地区或利益相关方，或者其中的某个小团体垄断或控制互联网核心基础设施。”
“在包括互联网在内的 ICT 环境中拥有垄断和支配地位的国家不得利用 ICT 的进步作为遏制和压制其他国家合法经济和技术发展的工具。”
“《全球数字契约》应重申，互联网应是开放、安全、包容、可访问和可互用的。”
[...]
“应在联合国系统的支持下，通过所有国家的广泛参与，并采用 WSIS 成果中规定的多利益相关方方法，在全球范围内解决互联网治理问题。”
[…]
“必须维护互联网的可靠性、安全性和稳定性，而不损害为实现可持续发展所做的努力。通过加强该领域的多边主义来开展国际合作，这一点非常重要。”[128]

萨尔瓦多重申“…务必要继续采用 2003 年日内瓦峰会和 2005 年《突尼斯议程》中所述的多利益相关方方法。”[129]

法国写道：“建议采取的行动：[…] 还需要在协议方面开展工作，以保持互联网的统一、中立和弹性。”[130]

中华人民共和国表示：“各国均有权平等参与国际互联网基础资源的管理和分配，不得利用互联网资源和技术损害其他国家接入互联网的合法权利，从而危及全球互联网的安全、稳定和连接。”[131]

---

[127] 荷兰王国提交的《全球数字契约》，2023 年 4 月 28 日，第 7 页，https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-submission-Kingdom-of-the-Netherlands.pdf
[128] G77 和中国针对《全球数字契约》讨论的意见，2023 年 4 月 28 日，https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-submission_G77-and-China.pdf
[129]萨尔瓦多关于《全球数字契约》拟定主题领域的国家提交文件，上次修改日期：2023 年 5 月 1 日，第 3 页，https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-submission_El-Salvador.pdf
[130] 法国对《全球数字契约》的贡献提案 – 译文，上次修改日期：2023 年 5 月 8 日，第 5 页，https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-submission_France.pdf
[131] 中国在全球数字治理问题上的立场（针对《全球数字契约》的贡献提案），上次修改日期：2023 年 5 月 24 日，第 5 页，https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-submission_China.pdf

[...]
“各国应营造一个和平、安全、开放、合作和有序的网络空间，反对互联网分裂和碎片化。各国应在联合国的带领下，通过各成员国的广泛参与，制定全球互用的网络空间共同规则和标准，并坚持致力于建立以多边主义、民主和透明为特征的国际互联网治理体系。”[132]

非正式会议发布《我们的共同议程》第 5 号政策简报《全球数字契约》— 面向所有人的开放、自由和安全的数字未来[133]

2023 年 6 月 5 日，在联合国总部举行的一次非正式会议上，秘书长安东尼奥 • 古特雷斯 (António Guterres) 发布了第 5 号政策简报。古特雷斯先生在其介绍性发言中表示，“简报提议举办一个数字合作论坛，评估数字治理方面的进展并强调存在的差距。这将是旨在把所有利益相关方聚集在一起，推动在数字技术方面采取一致行动的第一个全球框架。它将与区域性机构和多利益相关方网络合作，并支持互联网治理论坛等现有机构之间的交流。它将吸引广泛的参与者，让那些开发数字技术的人员参与进来，以了解潜力并推广其负责的应用程序。”[134]

部分联合国成员国代表的回复：

欧盟（代表其 27 个成员国）：“支持和加强互联网治理论坛、ITU、UNESCO 等既有机构可能有助于避免工作重复和分散。”[…]“多利益相关方方法是支持 GDC 的关键”[135]

加拿大（同时代表澳大利亚和新西兰，也称为 CANZ）：“我们各国完全致力于与其他国家和地区合作，确保在全球范围内继续提供一个自由、开放、可互用、可靠和安全的互联网。”[…]“我们还大力支持互联网治理的多利益相关方模型，这是保持互联网开放、弹性和稳定的基础。多利益相关方方法认识到，如何管理互联网与每个人都息息相关。我们必须承认，现有多利益相关方组织在互联网发展和运营方面成功地发挥了作用。我们钦佩政策简报中各项提案的雄心壮志，但我们强烈呼吁，任何潜在的新举措都必须首先以加强和补充联合国在全球数字合作方面的现有成功努力为目标。”[136]

立陶宛：“我要特别强调，务必让 ITU 等专门机构参与进来，使他们在促进实现契约目标方面发挥更加明确的作用。”[137]

巴基斯坦：“我们更希望看到的是，需要确定一个国际政府间流程，引导契约朝着一个更具发展性的方向而不是监管性方向发展，这应当与《突尼斯议程》相符，在该议程中，与互联网相关的公共政策是各国的职权范围和主权权利。当然，我们也正在考虑我们想要举办的这个数字合作论

[132] 同上，第 13 页
[133] 请查看 ICANN 博文页面，了解有关该政策简报的详细信息：https://www.icann.org/zh/blogs/details/un-secretary-general-policy-report-considerations-for-the-icann-community-13-06-2023-zh
[134] 秘书长发布的《我们的共同议程》政策简报，未来峰会（由秘书长办公厅 (Executive Office of the Secretary-General, EOSG) 组织）的《我们的共同议程》政策简报，联合国网络电视，2023 年 5 月 7 日，（从 19:35 开始），https://media.un.org/en/asset/k1n/k1nugz7a7n。
[135] 同上，（从 20:30 开始）
[136] 同上，（从 30:33 开始）
[137] 同上，（从 34:00 开始）

坛，以及这个论坛将如何与互联网治理论坛、WSIS 论坛以及 ICT 安全和使用问题不限成员名额工作组协同增效。”[138]

美国：“关于《全球数字契约》，为确保透明度、包容性以及所有利益相关方积极、有意义地参与 GDC 流程，我们鼓励联合国为利益相关方社群提供机会，使他们也能就 GDC 政策简报提供反馈。”[139]“从纽约来指导数字合作的尝试并没有反映这样一个事实，即多利益相关方、多部门和分散化方法为利用数字技术帮助实现可持续发展目标提供了更有效的手段。”[140]

瑞士：“组建新数字合作论坛的提案可能会给契约的实施造成不必要的负担。它非但不能创造真正的附加价值，反而有可能使现有合作数字机构中已经开展的工作重复。特别是，在多利益相关方针对契约所涉及问题采取后续行动方面，互联网治理论坛展示了其效力。”[141]

爱沙尼亚：“正如我们在《突尼斯议程》中已经商定的那样，我们需要依靠共同的价值观和原则，开展多利益相关方合作，从而实现普遍和有意义的连接。”[142]

中国：“关于 GDC，中国支持联合国发挥关键作用，协调各种利益相关方共同努力，加强数字合作，缩小数字鸿沟，完善数字治理，让数字技术造福全人类。起草流程应以问题为导向…”[143]

印度尼西亚：“关于 GDC，我们注意到 GDC 的一些理念与 2023 年互联网治理论坛的主题有相似之处。在这方面，我们希望听取进一步的意见，了解如何确保 GDC（特别是全球数字合作论坛举措）能够补充现有流程，避免重复工作并增强 IGF？”[144]

英国：“所有新举措应是对联合国已经开展的现有数字合作工作的补充。英国承认，现有多利益相关方组织是构建开放、弹性和稳定的互联网的基石。”[145]

印度：“我们应当避免重复工作或建立并行流程，从而提高工作效率。”[146]

在结束语中，联合国秘书长表示：“但我们需要区分国际政府间流程的范围，因为它涉及各成员国的主权，同时确定适合所有人共同参与的具体范围和领域，以便让事情朝着积极的方向发展。[…] 我很期待大家提出关于论坛[147]的问题，因为我们也在团队中开展了相关讨论。同样，这并不是信仰的问题。这就是我们的提议，如果各成员国同意，很好，就算各成员国不同意，那也无妨。但话虽如此，我认为这并不是工作重复的问题。而是在何处整合这几项工作，使其协同增效的问题。因为我们已经开展了几项相关工作。我们举行了互联网治理论坛，制定了 ITU 机制，还有 UNESCO 机制，但这些都是相互分开的。我认为，我们需要在纽约，在靠近联合国大会的地

[138]同上，（从 39:38 开始）
[139]同上，（从 1:06:50 开始）
[140] 同上，（从 1:08:15 开始）
[141] 同上，（从 1:10:17 开始）
[142] 同上，（从 1:12:46 开始）
[143] 同上，（从 1:18:24 开始）
[144] 同上，（从 1:19:40 开始）
[145] 同上，（从 1:24:30 开始）
[146] 同上，（从 1:34:32 开始）
[147] 此处为 - 数字合作论坛

方，能够找到将这些工作整合起来的方法。[…] 这不是一种重复工作的逻辑，而是一种将所有这些工作有效整合在一起的逻辑。这也是这项建议被提出来的唯一原因。”[148]

未来峰会的部长级筹备会议 - 联合国大会，第 78 届会议

2023 年 9 月 21 日，就《全球数字契约》和互联网治理问题发表了若干部长级和高层声明，其中包括：

卢旺达：“全球数字合作将是 GDC 的关键，[它] 提供了这样一个数字合作框架。”[149]

挪威：“我们还必须共同努力，实现公正的全球数字转型和《全球数字契约》。”[150]

俄罗斯：“我们支持将技术和创新问题纳入峰会议程，在严格遵守各国的国家主权前提下，克服数字不平等的情况，并实现互联网治理和 AI 监管的民主化。”[151]

保加利亚：“我们必须维护的最佳成果是，保护多利益相关方方法和互联网的完整性。”[152]

墨西哥：“我们完全致力于《全球数字契约》。”[153]

ITU：“这些挑战要求所有利益相关方共同努力。信息社会世界峰会及其后续流程（例如 IGF 和 WSIS 论坛）可以发挥重要作用，这一点已得到《全球数字契约》共同协调人的认可。”[154]

印度：“我们欢迎 SoTF 致力于提供《全球数字契约》，以最大限度地减小任何数字鸿沟。”[155]

津巴布韦：“鉴于技术的快速发展及其伴随的相关威胁和风险，我们需要找到一个更为全面的多边技术治理方法。我们亟需制定一份《全球数字契约》。”[156]

芬兰：“未来峰会的一项重点工作领域是就《全球数字契约》达成一致。该契约应当带来切实价值，指导我们就共同的数字优先事项开展合作，鼓励提出实现可持续发展目标的解决方案，以及保障数字空间的人权（包括隐私和言论自由）。”[157]

---

[148] 秘书长发布的《我们的共同议程》政策简报，未来峰会（由秘书长办公厅 (EOSG) 组织）的《我们的共同议程》政策简报，联合国网络电视，2023 年 5 月 7 日，（从 1:55:11 开始），https://media.un.org/en/asset/k1n/k1nugz7a7n。

[149] 联合国网络电视，（开幕式、全体会议、闭幕式）未来峰会的部长级筹备会议 - 联合国大会，第 78 届会议，2023 年 9 月 21 日，（从 42:52 开始），https://media.un.org/en/asset/k1z/k1zzbbnqaq

[150] 同上，（从 1:39:10 开始）

[151] 同上，（从 2:55:05 开始）

[152] 同上，请参阅法语原文（从 3:24:40 开始）

[153] 同上，（从 4:05:19 开始）

[154] 同上，（从 5:15:40 开始）

[155] 同上，（从 6:36:55 开始）

[156] 同上，（从 7:10:40 开始）

[157] 同上，（从 7:48:55 开始）

其他联合国举措

联合国大会第 77 届会议的官方文件

2023 年 5 月 15 日，俄罗斯、白俄罗斯、朝鲜、尼加拉瓜和叙利亚（作为共同提案国）提交了一份关于保障国际信息安全的联合国公约概念文件，作为联合国大会第 77 届会议的官方文件。[158] 除其他外，共同提案国提出了以下原则和建议，“可作为《公约》规定国家活动的基础，并界定各国在信息和通信技术的安全使用领域促进国家能力建设方面的权利和义务：[...] 根据全球通信网络的中立原则，促进开发和使用安全的信息和通信技术，其中包括逐步改革协议和信息传输方法，以消除将该网络用于实施犯罪行为的可能性；”[159]

背景信息：俄罗斯以及公约草案的共同提案国坚持提出，应在 OEWG 2023 年年度进展报告中，提及公约概念文件草案。俄罗斯声称，中国和伊朗也支持在 OEWG 年度进展报告中提及公约草案。[160]

秘书长技术事务特使（联合国技术事务特使）的发言

2022 年 10 月 13 日，联合国技术事务特使阿曼迪普 • 辛格 • 吉尔 (Amandeep Singh Gill) 表示：“在国际社会重振多边主义，更好地应对未来挑战方面，2024 年未来峰会将是一次契机。

这次峰会是联合国大会根据联合国秘书长应邀提交的一份报告决定召开的。这份报告称为《我们的共同议程》，而《全球数字契约》(GDC) 则是这份报告中的一项提案。这项提案将在未来峰会上通过。”[161]

2022 年 10 月 24 日，吉尔特使表示：“毫不犹豫地说，我们对多利益相关方方法所做出的承诺是极为坚定的。事实上，秘书长在联合国大会上发言时明确表示，我们要么通过多利益相关方流程制定 GDC，要么根本无法制定 GDC。这是在纽约发表的非常明确、非常强烈的声明。我们正在通过这些磋商和许多其他磋商，通过与 IGF 以及其他论坛，还有 ICANN 开展有力合作，履行这一承诺。”[162]他继续说道：“你们现在提出的问题是，我们如何才能超过多利益相关方方法的本质要求，以及如何才能解决以下问题，即这是国际政府间多边主义，还是多利益相关方方法，这最终将成为协商性的有趣讨论，但实施的途径是什么？我们努力解决这个问题，但坦率地说，没有人真正破解过它。”[163]

“我在纽约听到过，WSIS 突尼斯方案是一个多利益相关方参与的良好方案。 你们知道，这是在我们的职责和权限范围内提出的方案。我没有想出确切的措辞，但对于一些人来说，这一方案不够深入，而对于另外一些人来说，又过于深入。 所以，我们来看看最终的成果，这也是一个良好

[158] 俄罗斯联邦外交部，关于国际信息安全联合国公约概念的新闻稿，2023 年 5 月 16 日，https://mid.ru/ru/foreign_policy/news/1870609/?lang=en

[159] 关于保障国际信息安全的国际公约概念更新文件，2023 年 5 月 15 日，第 8 页，https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Concept_of_UN_Convention__on_International_Information_Security_Proposal_of_the_Russian__Federation.pdf

[160] 联合国网络电视，（第 8 次会议）信息和通信技术 (ICT) 不限成员名额工作组 - 第五次实质性会议，2023 年 7 月 27 日，（从 13:50 开始），https://media.un.org/en/asset/k1n/k1ngmoogyi

[161] ITU 新闻，建立《全球数字契约》：对阿曼迪普 • 辛格 • 吉尔的简短访谈，2023 年 10 月 13 日，https://www.itu.int/hub/2022/10/establishing-the-global-digital-compact-qa-with-amandeep-singh-gill/

[162] IGF，与联合国秘书长技术事务特使的市民大会，2022 年 10 月 24 日，（从 49:53 开始），https://youtu.be/NEmXNzQzsCk?t=2991

[163]同上，（从 51:31 开始），https://youtu.be/NEmXNzQzsCk?t=3091

示例。我提到过最近的两项经验，其他相对积极的经验：网络犯罪讨论以及 ITU 讨论。因此，我们也许可以提出一种*“独具一格”*的方案，
让所有人[164]对这方面都感到满意。”[165]

2023 年 6 月 23 日，联合国技术事务特使表示：“我想让大家看看，这份 [联合国秘书长] 政策简报的最后一部分与定期评估契约实施情况以跟上技术发展步伐的想法有关。我想再次强调的一点是，这里特别要提及这个专家组中的先前发言，即这是一个多利益相关方论坛。因此，准备工作 – 三方，这些词被明确用于公民社会，其中包括来自技术社群、学术界的所有参与者，还有科学、独立科学专业知识的价值，特别是在 AI 方面的价值，如今你们也清楚地认识到，这也包括私营部门和各国政府。”[166]

2023 年反恐周会外活动

2023 年 6 月 22 日，联合国反恐怖主义委员会执行局 (U.N. Counter-Terrorism Executive Directorate, UN CTED)支持的“科技反恐”倡议呼吁各国“考虑如何改进机制，以删除恐怖分子运营的网站，包括帮助我们对域名注册服务机构、内容分发网络和托管服务提供商进行干预。”[167]

结语

联合国当前以 OEWG 形式进行的持续讨论将于 2025 年结束，如果报告以协商一致的方式获得通过，它将成为这些讨论的成果。AHC 审议工作计划于 2024 年 2 月结束，届时将以协商一致的方式通过网络犯罪公约，如果无法达成一致，则应由出席的国家代表通过表决获得三分之二多数投票通过。尽管 GE 职能部门认为这两个流程的结果可能对 ICANN 使命产生极微小的影响，但它仍将跟踪这两个流程并就此提出报告。

针对 GDC 的谈判将于 2024 年 1 月开始，最后阶段计划于 2024 年 9 月 20 日至 23 日在未来峰会期间举行，届时该契约有望在协商一致的基础上获得通过。目前，这一流程给组织带来了太多未知因素。GE 将密切关注有关 GDC 的所有审议工作，并随着谈判的逐步进行，向 ICANN 社群报告进展情况和发展动态。

[164] 在这里，联合国技术事务特使提到了加拿大代表和 MAG 成员就 WSIS 进程和技术社群的职责向他提出的问题。
[165] 同上，（从 1:06:13 开始），https://youtu.be/NEmXNzQzsCk?t=3973
[166] YouTube 视频，2023 年欧洲互联网治理对话 (EuroDIG) • 前期 05 | 让我们共同推动欧洲数字治理与合作的愿景，2023 年 6 月 23 日，（从 1:36:42 开始），https://youtu.be/RctcgFscohU?t=5802
[167] 联合国网络电视，防止和打击出于恐怖主义目的使用新技术和新兴技术：全方位多边应对措施的前进方向（2023 年反恐周会外活动），2023 年 6 月 22 日，（从 1:08:27 开始），https://media.un.org/en/asset/k1i/k1iy7ltzvt

同一个世界，同一个互联网

请访问我们的网站 **icann.org**

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin.com/company/icann

soundcloud.com/icann

instagram.com/icannorg