本译本感谢张晓的自愿贡献。 IGF 对他们表示感谢。不代表该组织的任何立场。

利勒斯特罗姆 IGF 信息

第 **20 届互联网治理论坛年会于 2025 年 6 月 23 日至 27 日**由挪威王国在利勒斯特罗姆主办。

利勒斯特伦 IGF 信息为决策者提供了关于当前互联网治理和数字政策关键议题的高级别概述。这些信息直接来源于 2025 年 IGF 期间举行的 262 场会议。会议组织者受邀在会议结束时自行总结关键要点和行动号召，作为这些信息的输入。这些信息还参考了国家级、地区级和青年 IGF 倡议的报告。

由 IGF 秘书处策划的一系列信息草案于 6 月 27 日发布，供社群审议，截止日期为 7 月 14 日。IGF 2025 信息最终稿是年度会议成果的一部分。

论坛的主题是“***共建数字治理***”。会议围绕四大主题展开：

- **[构建] 数字信任与韧性**
- **[建设] 可持续和负责任的创新**
- **[建设] 普遍接入和数字版权**
- **[建设] 数字化合作**

本文档中的信息按照上述结构构建。

免责声明：本文件中表达的观点和意见不一定反映联合国秘书处的观点和意见。所使用的名称和术语可能不符合联合国的惯例，且不代表本组织的任何意见。

目录

利勒斯特伦 IGF 信息及其他 IGF 成果

利勒斯特伦 IGF 信息汇集了 IGF 会议期间多利益相关方社群表达的观点。这些信息的报告可访问 https://intgovforum.org/en/content/igf-2025-outputs 获取。

利勒斯特伦 IGF 信息是对其他轨道汇编的输出和观察结果的补充；这些列于 https://intgovforum.org/en/content/igf-2025-outputs 。

[构建] 数字信任与韧性

主题

GDC 3、4、5 - WSIS C5、C9、C10 - SDGs 9、16、12、17；网络安全与信任、数据治理、人工智能、媒体与内容、权利与自由 [能力建设]

面对日益增长的网络威胁和数字基础设施的破坏，一个具有韧性、可互操作且值得信赖的互联网对于确保通信基础设施、服务和数据交换的稳定和安全至关重要。虚假信息、虚假信息、黑客数据、仇恨言论、个人信息滥用、带有偏见的人工智能响应以及其他令人困惑且不准确的信息元素，都是我们日常使用和享受的互联网面临的常见挑战。

IGF 利勒斯特罗姆信息

数字基础设施

- 随着对数字服务的依赖日益加深，对网络中断的容忍度也随之下降。对等互联和传输对于实现稳健的互联至关重要，能够实现更快、更可靠的互联网。政府与私营基础设施所有者之间的密切合作对于确保网络韧性、加强和扩展数字基础设施至关重要。

- 有必要梳理联合国系统内外不同的危机应对模式和机制，并分析如何将其推广用于应对冲突和危机地区通信中断、关键互联网基础设施遭受攻击的情况。建立多利益相关方机制，以确保资金、政治承诺和其他因素，从而能够在国际人权保护和人道主义援助法框架内，有效、及时地做出应对。

- 多利益相关方社群致力于建设开放互操作的互联网，在冲突和危机环境下，为确保平民访问互联网并确保核心互联网基础设施安全，具有巨大的行动潜力。然而，它也面临着巨大的局限性。同样，包括国际人道主义法和人权法在内的规范和监管框架虽然提供了重要的工具，但也存在自身的局限性。互联网治理论坛 (IGF) 及其最佳实践论坛应成为一个平台，让各方能够相互联系、互动交流、相互促进，以应对这些关键挑战。

- 全球海底电缆网络的韧性取决于主动规划、内置冗余以及快速响应事件的能力。由于海底电缆基础设施面临的威胁跨越国界，区域和国际合作至关重要，同时还要为资源有限的国家提供支持。

- 各国应采取切实步骤，落实联合国负责任国家行为框架，使其成为一个切实可行的框架。应在国家、区域和全球层面与所有相关利益相关方进行协调和转化。支持能力建设（包括模拟演习、加强社群紧急响应小组 (CERT) 之间的合作）、分享最佳实践，以及探讨如何改进关键基础设施的保护，是实施工作的重要组成部分。

- 更具韧性、更加多样化且自主的云基础设施或许能够减少对少数几家全球主导供应商的依赖。它能够支持本地创新，确保监管清晰，并增强信任。它还能赋能各国和各社群，使其能够根据自身情况塑造数字基础设施。

- 推广负责任的互联网基础设施实践需要建立一个值得信赖的多利益相关方流程，以促进在有害活动和审查等挑战上开展合作。该流程应优先考虑开放沟通而非僵化的标准制定，并强调透明度而非限制访问。它必须支持相互问责和互操作性，以建立信任并促进有效合作。

- 需要进行全面的政策和法律分析，以识别和澄清监管方面的模糊之处，审查法律框架之间的冲突，评估商业影响，并解决阻碍负责任的互联网治理的司法管辖权不一致问题。应制定协调一致的倡导策略，以促进相关司法管辖区制定协调一致、透明且可执行的指导方针。

- 对互联网基础设施（包括其域名系统 (DNS)）的信任至关重要。必须避免与区块链标识符发生冲突。多利益相关方就负责任地整合区块链标识符进行讨论，为互联网社群提供了一个机会，使其能够继续推进构建安全、可靠和值得信赖的互联网的共同目标。

- 关于自主武器系统 (AWS) 及其技术、法律、伦理、安全和发展影响的讨论应包容透明，不应局限于封闭的专门论坛。正如联合国秘书长和红十字国际委员会所强调的那样，迫切需要国际合作，他们呼吁在 2026 年前就 AWS 谈判达成一项具有法律约束力的文书。整体解决方案需要政府、民间社会、学术界、技术界和产业界的积极参与。致命自主武器系统政府专家组 (GGE on LAWS)、奥地利主导的联合国大会决议、荷兰和韩国的“军事领域负责任人工智能全球委员会”(GC REAIM) 倡议以及互联网治理论坛 (IGF) 等多利益相关方平台在推进集体行动和提高公众意识方面发挥着至关重要的作用。

网络安全 / 信息完整性/儿童安全

- 全球数字契约的愿景是构建一个包容、开放、安全的数字空间，这不仅仅是一个愿景，更是一个指导我们日常工作的实用框架。无论是协调选举诚信工作、制定儿童保护指南，还是建立多利益相关方伙伴关系，我们都在积极地为这一全球愿景做出贡献。

- 政府、科学家、媒体、广告商、意见领袖和其他相关专业人士参与的举措，能够更有效、更可持续地应对信息诚信威胁。这些举措不应关注孤立的行为体，而应关注整个信息生态系统，将其导向可靠的、基于科学的内容，以提升公众意识并促进知情决策。在此背景下，重要的是要实施基于证据的监管措施，为研究目的访问大型平台上的算法和内容流提供便利。

- 信任超越技术，源于人性和社会。有效的网络安全依赖于嵌入透明度、包容性社群参与和公民数字素养，以增强公众信心，并抵制诸如隐私洗白之类的行为。这需要通过适当的政策工具实施安全设计授权，启动以人为本的信任建设和数字素养倡议，并建立区域和国际互操作性框架。

- 有效打击网络滥用，包括欺诈和域名系统 (DNS) 滥用，需要协调、跨部门合作和数据驱动的行动。任何单一行为体或部门都无法独自应对这些挑战。互联网社群应与其他行业（例如支付行业、托管和云服务提供商）合作，以制定有针对性的应对措施。通过全球信号交换 (Global Signal Exchange) 和网络信标 (Net Beacon) 等举措，构建一个能

够实现稳健信息共享的生态系统至关重要。这项工作必须是跨部门的，并且需要多利益相关方共同参与。

- 加密争论常常会变得根深蒂固、充满对抗，两极化的立场阻碍了有意义的进展。为了推动进展，利益相关者应该专注于那些有可能且迫切需要妥协的特定领域，而不是让意识形态僵局阻碍行动。IGF 社群应在促进有针对性的讨论中发挥关键作用，探索和试行既能维护强加密又能合法访问的技术和政策解决方案，尤其是在儿童保护等领域。

- 不同地区、不同背景的国家都在努力应对为儿童提供安全且赋能的数字环境的挑战。构建一个尊重儿童权利、包容的数字未来，远非传统科技公司和网络平台所能及。从品牌到投资者，其他行业参与者也应发挥关键作用，包括利用自身对生态系统其他参与者的影响力。

- 平台应采取以儿童权利为基础的方法，维护儿童的尊严、隐私和最佳利益。缺乏强有力、标准化且全球适用的机制来保护数字环境中的儿童，仍然是一个关键的差距。以儿童为中心且透明的方法对于构建安全的网络空间至关重要。保护儿童的网络安全必须超越透明度报告和统计数据，需要持续、有意义的承诺。便捷、儿童友好的举报机制对于赋能儿童发声至关重要。他们必须知道如何以及在哪里举报受到的伤害，并在举报时感到安全、得到支持和自信。

- 受性别暴力和网络平台快速演变的动态影响，深度伪造和性伪造问题在全球范围内日益严重。法律、教育和技术系统难以跟上步伐。解决这一问题需要多方协调合作，但目前的努力仍然分散且不足。为了加强预防和问责，需要对本地化检测数据集和不可篡改图像技术进行有针对性的投资。同时，需要开展全面的数字素养项目，以教育年轻人和决策者。 制造商了解使用和滥用此类技术所带来的风险、危害和责任。

- 造成人身伤害或情感冲击的网络犯罪与以经济动机为目的的网络犯罪同样需要应对。在打击网络犯罪和网络伤害的工作中，应纳入性别敏感的应对措施，因为这些犯罪和伤害对妇女和女童的影响尤为严重。健全的法律框架和立法文书至关重要，但必须同时为整个刑事司法系统（从执法人员到检察官和法官）提供全面的培训，使其了解如何有效地支持受害者。

[建设] 可持续和负责任的创新

主题

GDC 1、2、4、5 - WSIS C1、C6、C7、C10、C11 - SDG 7、8、9、13、14、15、16、17；环境可持续性和气候变化、经济问题和发展、新兴技术和创新、人工智能、技术和运营主题

人工智能、量子计算、区块链、物联网及其他领域的进步有潜力提高效率、去中心化和可访问性，从而推动经济增长、数字包容性和社会发展。然而，这些技术的发展和应用也蕴含着风险，包括负面的环境后果和广泛的社会经济影响。随着这些技术在社会中的作用日益增强，道德监督和包容性治理变得越来越重要。数字平台和新兴技术需要在创新、责任和可持续性之间取得平衡。

IGF 利勒斯特罗姆信息

数字公共产品

- 数字公共产品（DPG）对于创建一个包容性社会至关重要，在这个社会中，每个人都可以参与并实现自己的愿望。DPG 对于实现可持续发展目标至关重要。
- 任何国家都无法独自引领技术转型。我们需要更有效地利用资源，通过全球伙伴关系、知识共享和协同发展，开展合作并共享技术。

人工智能、工作和技能

- 人工智能正在渗透到各个领域。人工智能革命的范畴远不止取代现有工作岗位，它还将从根本上改变价值创造的方式以及受益者。那些懂得如何运用人工智能的人将会供不应求，而那些缺乏培训或工具的人则有可能被淘汰。
- 我们可以通过政策和选择来设定未来劳动世界的方向；技术本身并不能决定未来。我们需要确保劳动者获得赋权，而不是被边缘化，以避免数字鸿沟扩大。投资于数字素养至关重要，尤其是针对女性、年轻人和非正规经济从业人员，并促进工作场所的透明度、问责制和公平性。
- 投资公民的数字技能不仅有助于提升竞争力，还能让人们有机会从数字技术和服务中受益。教育体系应该帮助人们了解何时质疑人工智能系统，并赋能人们利用自身数据。
- 国家战略应优先考虑包容性教育和人工智能素养，以使社会能够拥有具有气候意识的数字化未来，并将环境素养和绿色人工智能原则纳入人工智能课程。

虚假信息、内容审核、人工智能和媒体/新闻

- 大型语言模型 (LLM) 已成为内容审核的新工具，但它们也存在强化系统性歧视、审查和监控的风险。大多数平台只对少数几个基础模型进行微调，而不是开发自己的模型，这导致内容审核权力集中，因为 LLM 训练阶段做出的决策会逐级传递到各个平台。

- 人工智能内容审核在实施和风险缓解方面缺乏足够的透明度，因为人工智能的炒作常常掩盖了已记录的人权损害。我们需要投资于人工智能内容透明度工具，并促进多利益相关方产品共同设计，让政策专家、用户、民间社会和代表性不足的群体参与早期的产品构思和测试。人工智能的出现从根本上改变了打击虚假信息的斗争，人工智能生成的回复通常与原始来源脱节，使得可靠来源难以识别。

- 需要加强跨部门合作，并在媒体参与者（包括数字版权和媒体发展组织）之间建立联盟，以理解人工智能的影响，并将负责任且合乎道德的人工智能应用纳入媒体主流。需要积极倾听来自全球南方国家的独立媒体和公益媒体的声音。

- 关于道德人工智能的宣言很重要，但我们还需要监督其在实践中的转化并评估其影响，以确保在日常媒体工作中道德地使用人工智能。

基础设施

- 建设下一代基础设施对于全球数字包容至关重要。数据机构对于公平包容的数字未来至关重要，这应体现在国际融资机制、能力建设和标准制定中。通过数据机构赋能全球南方用户，有助于支持本地创新，促进数字市场的竞争性参与，并减少对中心化平台的依赖。

- 连接技术创新与公共政策至关重要。建设者、投资者、政策制定者和民间社会行为体必须更紧密地合作，确保下一代基础设施既反映市场现实，又体现公共价值。多边和国家数字发展战略应优先考虑通过设计赋能用户的基础设施。

- 公共利益、平等、互操作性和包容性对数字公共基础设施 (DPI) 至关重要。确保 DPI 以包容和安全的方式开发和使用，是全球数字合作的重要基础。迫切需要政府能力建设、在可行的情况下推行开源政策以及建立全面的数字治理框架，以建立信任并确保 DPI 的安全应用。

- 数字公共基础设施（DPI）具有天然的垄断特性，特别是在基础身份、支付和健康平台方面，这带来了公私合作伙伴关系可能赋予现有企业过多的运营控制权的风险，使它们能够以最小的社会回报将公共数据货币化。

- 我们需要设计合同安排，将数字公共基础设施（DPI）维护为共享的公共基础设施，同时通过私营部门合作促进创新。我们应为参与式数据治理方法建立监管沙盒，投资于公共部门官员、数据保护机构、民间社会组织和社群领袖的能力建设，以确保政策决策以本地知识为依据，从而防止市场集中并确保数据使用的竞争性。

连接性

- 全球约有 26 亿人尚未接入互联网。加快国际合作对于弥合数字鸿沟至关重要。互联网的可及性和连通性是一项权利。利益相关方必须合作制定包容性政策和连通模式，以支持开放性和可负担性。

- 我们需要增强农村互联网用户的能力，为他们提供社群网络可持续发展所需的数字技能。

环境与健康

- 可扩展、节能的模型已投入运营，并可在气候脆弱和资源匮乏的环境中实现低成本、低功耗的人工智能部署。开源人工智能可以显著减少重复、成本和能源消耗，同时促进全球合作。

- 在整个人工智能生命周期中嵌入透明度，以确保能源和资源的使用得到衡量、披露和最小化，是公平人工智能治理的关键要素。政府和行业应优先考虑并激励节能型人工智能创新，并要求开发者和部署者通过可持续性标准、审计框架和生命周期披露要求，衡量和报告人工智能系统对能源、排放和水资源的影响。

- 数字数据的质量和粒度对于建立可靠的环境和健康风险模型仍然至关重要。为了解决对可访问性、标准化和互操作性的担忧，我们需要投资于公共卫生的数字素养和能力建设，尤其是在发展中国家。

- 数字解决方案应以价值驱动的设计为基础，并通过包容性框架进行治理。我们需要从参与驱动转向目标驱动的数字生态系统，尤其对于服务匮乏的社群而言。

人工智能公平差距、人工智能伦理与小型人工智能参与者

- 全球人工智能公平差距正在扩大，使发展中国家面临越来越大的被排斥风险。以本地为导向、包容且以人为本的人工智能方法对于产生有意义的影响至关重要。我们需要通过有意识地投资于培训、基础设施和语言包容性来提升本地能力。

- 政策制定者应制定既能保护公共价值又能促进创新的人工智能法规。伦理考量不应被视作新兴技术发展后才考虑的因素。伦理必须成为所有利益相关者的核心竞争力，开发者应在每个阶段平衡技术成功与伦理和可持续性视角。

- 规模较小的国家和初创企业可以通过利用开源工具、领域专业知识和战略合作伙伴关系，在人工智能领域保持竞争力，尤其是在敏捷性、深厚的领域专业知识和情境信任比规模更重要的领域。他们不应等待被邀请，而应将自己定位为数字化未来的共同创造者。

- 大型科技公司应致力于与小型企业进行真正的合作，投资开放生态系统、支持轻量级人工智能开发以及共同开发反映不同背景和约束的工具。

[建设] 普遍接入和数字版权

主题

GDC 1、2、3、4 - WSIS C2、C3、C4、C7、C8、C10 - SDG 1、2、3、4、5、8、10、11、16；权利与自由、普遍接入和有意义的连通性、经济问题与发展

有效数字接入方面的差距和不平等，对世界各地的社群构成了深刻的挑战。如果不认识到普遍接入与人权之间的根本联系，就无法解决此类数字鸿沟：一个包容、开放、可持续、公平、安全、有保障的数字未来，只有在线上线下都尊重人权，才能实现。

IGF 利勒斯特罗姆信息

人权与数字危害

- 我们需要加强数字权利保护，并对数字危害（包括一切形式的国家和非国家数字监控及数据隐私侵犯）追责。追责需要多方利益相关方共同行动，并制定更强有力的国内法律，以遏制间谍软件滥用，保护公民社会。

- 利益相关方应倡导政治承诺，推动对国际法进行渐进式解读，保护个人和社群免受数字空间的人权侵犯。法律学者和法律从业者应汇聚专业知识，协调人权与国际法原则，确保两者在数字和网络活动中均得到维护。

- 国家监控法律必须透明化并进行改革，包括司法监督、公开举报以及禁止不受约束的国家入侵。需要通过法律援助、设备取证测试和跨境团结等方式，为受害者和民间社会提供支持，以打击间谍软件滥用并获得赔偿。数字权利条款应平等适用于所有人。

- 成功的数字政策在制定过程中应听取多元化的声音。科技公司、政府和监管机构应投资建立充分的保障措施和问责机制，并将全球多数群体日益加剧的数字不平等纳入考量。全球框架需要放大南方国家的声音，以确保政策着眼于区域现实，而不仅仅是北方国家的优先事项。

- 侵犯人权的行为可能源于行动，也可能源于未能采取行动并阻止不法行为的发生。国家和企业都有责任，但目前国家和企业问责之间的界限模糊。解决这一问题的努力正在进行中，但需要进一步发展。

- 联合国指导原则明确规定了人权尽职调查的责任，但企业问责应成为平台问责，建立一种反映人权尽职调查在数字环境下含义的应用方法。

- 数字威胁影响着每个人。然而，随着现实生活中不平等和压迫的模式在数字空间中重现并加深，一些群体变得更加脆弱。妇女和女童是受影响最严重的群体之一，她们遭受网络恐吓或暴力威胁的记录更高，尤其是在参与维权活动或人权倡议活动之后。

- 在数字治理过程中，务必以最易遭受数字伤害和排斥的人群和社群的观点为中心，以确保这些进程以权利为基础、多利益相关方参与、透明且民主。数字技术应服务于人权和社会福祉，而非将少数人的利益置于所有人的福祉之上。

人工智能伦理

- 人工智能伦理准则的实施至关重要。制定准则时应考虑多方面因素，包括隐私和保密性、知情同意、偏见和公平性、融入人工监督、持续改进、遵循伦理准则进行编码以及对社群驱动/本地解决方案的支持。

- 如果没有道德准则，人工智能模型的开发、实施和部署可能会导致传播错误信息和有害刻板印象、缺乏实时事实核查、违反道德和隐私问题、对复杂人类情感的理解有限以及延续偏见和歧视。

- 有必要将心理健康和自杀意识纳入互联网和人工智能发展的政策对话、指南和标准中。利益相关者应合作，促进以社群为中心的框架建设，优先保障用户对个人心理健康数据和信

息的控制权。

有意义的访问

- 数字连通性不仅仅意味着互联网接入；它是包容性的基础。差距是由基础设施、经济、政策和社会文化障碍等多种因素造成的。发展中地区存在着深刻的数字鸿沟，新技术往往会加剧线下差距。尽管各经济体都在积极应对新兴技术，但在连通性和有效接入方面仍然存在持续的挑战。

- 数字包容需要一种基于权利的全社会参与的方法，包括灵活构建适应国家或地区需求的数字系统。任何单一实体都无法独自弥合数字鸿沟：政府、私营部门、非政府组织和社群必须共同努力，通过包容性政策制定和公私伙伴关系实现长期影响。多利益相关方伙伴为协助、激励、促进和衡量有意义的数字获取所做的努力应当是持久的。

- 对于生活在移动网络覆盖地区的大量未联网人群而言，数字不平等的主要障碍已不再是基础设施覆盖。相反，主要障碍在于可负担性（尤其是设备成本）、数字素养和有效使用技能。满足这些需求需要采取综合措施，包括基础设施投资、可负担性、数字素养和本地参与。

- 我们需要确保人们能够以自己的语言获得实用且有意义的服务。互联网及其相关技术可以成为保护和使用濒危土著语言的有力工具。教育工作者、研究人员和行业专家可以下载开源代码，以促进和扩大这些语言的复兴。与私营部门合作并使用当地语言将增强数字素养项目的影响力。

- 利益相关方应设计并支持可扩展的解决方案，例如社区网络和公共 Wi-Fi 计划，以满足服务欠缺地区的独特需求。此外，还有必要为边缘群体提供数字设备和网络连接补贴，并开展使用当地语言的本地能力建设。互联网治理论坛已通过闭会期间活动开发了一些工具，以鼓励成功且有意义的项目复制、扩展和本地化。

- 多元化的供应商生态系统对于“最后一英里”接入至关重要。传统的模式仅仅依赖大型移动运营商，不足以覆盖边缘化社区。这些社区包括社区网络、地方图书馆、邮局以及其他能够提供文化相关且价格合理的解决方案的中介机构。监管框架需要鼓励这种多元化，而不是设置只有利于大型传统运营商的壁垒。

数字公共基础设施

- 所有地区都寻求建设包容、有韧性、以人为本的数字公共基础设施 (DPI) 。基于公地的 DPI 治理方法可以统一这些努力，避免使其同质化，尊重地方自主权，并促进全球协调。此外，治理可以“融入规范”。DPI 系统的构建必须从一开始就体现问责制、隐私和公平等原则。

- 政策应旨在促进公平、安全地获取数字技术。政策应确保优先考虑传统上被边缘化和受压迫群体的权利和需求。为了支持包容性数字解决方案的开发和部署，必须采用多样化的融资模式，并引导资助方和融资方的行动。

[建设] 数字化合作

主题

GDC 3、4、5 - WSIS C1、C2、C3、C4、C6、C10、C11 - SDG 9、10、11、16；数字合作、新兴技术与创新、人工智能、可持续多利益相关方治理

2025 年是多利益相关方持续努力完善和发展数字世界治理与协调的关键一年。互联网治理论坛（IGF）是这项工作的关键平台，它将与众多利益相关方和相关进程进行互动，包括 WSIS+20 审查、近期达成的《全球数字契约》以及正在进行的人工智能治理全球对话，以应对日益增多的挑战。

IGF 利勒斯特罗姆信息

- 随着人工智能等新兴技术的快速发展，数字不平等的风险日益加剧，尤其是在发展中国家。高昂的部署成本和有限的数字技能阻碍了许多社区，尤其是发展中国家，充分受益于数字化进步。
- 必须加强全球南方国家和公民社会在全球数字对话中的参与。不仅要加强对共同目标的沟通，还要加深对当地需求和现实的理解。
- 互联网并非无主，权力日益集中以及对大型科技公司日益增长的依赖，引发了人们对社会维护健康信息空间、言论自由和信息获取能力的严重担忧。为了确保信息技术服务于民主和道德价值观，并支持开放信息社会的可持续性，或许有必要从放松管制、不干预和企业整合转向负责任的集体治理和监管，并将透明度和问责制置于首位。
- 需要探索可持续的商业模式，以确保广泛接入。应加强或建立国际法律或机构机制，防止私营卫星宽带提供商对外国司法管辖区的互联网接入和连接施加不成比例或不受监管的影响。
- 加强多边和多利益相关方合作至关重要，这有助于确保数字化转型的成果得到广泛分享，不让任何人掉队。
- 技术标准可能对现实世界的人权产生重大影响，影响关键服务的获取，并增加被监视或排斥的风险。因此，技术标准制定的包容性至关重要。这需要建立支持机制和能力建设工作，以促进包括民间社会和非工程师在内的不同群体的有效参与，并在标准制定的各个阶段纳入国际人权框架，以确保取得符合伦理道德且具有包容性的成果。
- 互联网治理论坛 (IGF) 应成为进一步讨论互联网碎片化问题的信心和能力建设平台，尤其是在当前各利益相关方群体在解决碎片化问题上缺乏协调的情况下。鉴于全球数字环境面临日益加剧的地域化、基于主权的手段日益盛行以及网络控制常态化，所有利益相关方群体的包容性意见至关重要。

- 应推动发展包容创新的数字治理模式，以解决造成数字不平等的结构性障碍。应优先投资于数字能力建设，尤其是在服务欠缺和发展中地区，以确保公平地获取新兴技术。

IGF、全球数字契约和 WSIS

- 国际社会应避免联合国系统内职责重叠或碎片化。应利用互联网治理论坛等现有平台和空间，提升合作能力，并进一步努力吸纳多元化行为体，加强多部门对话。

- 在互联网治理论坛内，应进一步努力加强服务不足社区和各代利益相关者的参与，加强与国家和地区互联网治理论坛倡议之间的联系。

- 为了进一步开展数字合作，有必要加强承诺和现有机制，特别关注全球南方国家和边缘化群体。

- 信息社会世界峰会 (WSIS) 应改革其多利益相关方框架，以应对数字主权、平台整合和新兴技术等当代挑战。这需要加强机构问责机制，扩大全球南方国家的参与，加强区域协调，并赋能互联网治理论坛 (IGF) 。

- 各方普遍认为，WSIS 行动方针的制定范围广泛且技术中立，以便能够适应并应用于持续的技术创新。WSIS 框架内部及其不同组成部分（例如互联网治理论坛 (IGF) 和 WSIS 论坛）之间的主要差距在于缺乏协调，无论是在程序方面，还是在各个论坛讨论的主题方面。

- 为加强 IGF，需要开展一些工作，包括（i）需要与其他数字治理空间进行协调；（ii）重新考虑程序方面，包括 MAG 的运作（例如，为了创建稳固和永久的机构知识）；（iii）获得更充足的资金；（iv）建立更长或永久的授权，以便持续改进；（v）改进 IGF 成果分享机制，以便覆盖更多的人和受众，包括决策者；（vi）加强全球治理与地方和区域治理之间的协调，例如加强与国家和区域互联网治理论坛间的互动。

- 应建立 WSIS 论坛与 IGF 之间的整合与协调机制，促进 WSIS 行动路线与可持续发展目标更加契合。

- 像互联网治理论坛 (IGF) 这样的多利益相关方平台应该得到维护和加强。所有利益相关方，包括政府、企业、技术社群和民间社会，都应在政治和运营层面积极支持互联网治理论坛，将其作为一项全球公共产品。

- IGF 是一个宝贵的全球跨境跨领域合作平台，它帮助大小国家赋能，共同塑造数字化未来。 跨越世代、行业和利益。

- 即将举行的 WSIS+20 审查会议为重新评估全球治理结构、更好地整合法律和技术方法提供了重要契机。它促使我们反思多利益相关方进程的进展，以及在哪些方面可以加强与国际法的衔接。

- 尽管过去二十年技术变革和新问题层出不穷，但由互联网治理工作组制定并在突尼斯会议上通过的“广义”互联网治理定义仍然适用。互联网治理工作组展示了在联合国框架下真正多利益相关方决策的价值和可行性。其模式可以用于解决其他政府尚不确定或陷入僵局、需要新方法的问题领域，例如数据和人工智能治理。

- WSIS 审查应促进真正的多利益相关方参与（包括利益相关方和政府之间的参与），并为未来的后续行动和实施工作建立更强有力的多利益相关方安排。

- IGF 需要继续作为就互联网技术层面治理进行有效对话的场所，同时也为多方利益相关方参与应对新兴的数字治理挑战创造空间。

全球人工智能合作

- 多利益相关方和跨部门合作对于确保人工智能促进可持续发展目标(SDG)至关重要。人工智能必须以人权为核心进行治理。人工智能系统应支持可持续发展，促进性别平等，并体现文化多样性。

- 人工智能治理的包容性、多利益相关方方法应该涉及民间社会、独立专家和代表性不足的社群，以确保治理模式不受专制或纯粹商业利益的主导。

- 本地人工智能生态系统将有助于赋能多元化社群，使其能够塑造科技的未来。全球努力必须优先发展本地语言的人工智能和文化相关的数据集，以赋能代表性不足的社群，塑造国际人工智能治理框架。

- 应加强多利益相关方伙伴关系，以提高数字技能并开发值得信赖的人工智能系统，从而促进在全球不同背景下的包容性采用。