注意：感谢杨晓波和李娜的自愿贡献，因此可以提供此翻译。 IGF 对他们表示感谢。

2022 年联合国互联网治理论坛
亚的斯亚贝巴 IGF 关键信息

本文件[1]是 2022 年 11 月 28 日至 12 月 2 日在亚的斯亚贝巴举行的第十七届联合国互联网治理论坛年会期间提出的要点摘要。

本文所表达的观点和意见并不代表联合国秘书处。文中所使用的名称和术语可能不符合联合国的惯例，也不代表本组织的任何立场。

2022 年 IGF 集中讨论了全球数字契约（GDC）中明确的五个关键主题。GDC 由联合国秘书长在关于联合国成立 75 周年的报告《我们的共同议程》中提出，并将在 2023 年的联合国大会上进行审议。这将成为拟于 2024 年举行的未来峰会发展的组成部分。

IGF 讨论的主题包括：

- **连接所有人并保障人权**
- **避免互联网碎片化**
- **数据治理和隐私保护**
- **实现安全、安保和问责制**
- **处理包括人工智能（AI）在内的前沿技术问题**

IGF 的多利益相关方社群对秘书长关于全球数字契约的提议表示支持。本文件所载信息代表了 IGF 对该契约发展的贡献。IGF 动态联盟已经在处理与全球数字契约主题相关的具体挑战和机遇，同时也表示愿意在联合国关于全球数字契约的筹备和执行阶段中做出贡献。

[1] 这些信息来自第十七届联合国互联网治理论坛年会。文件曾公开征求意见，并将收集到的公众反馈内容纳入到本最终版本中。

连接所有人并保障人权

主题

联合国秘书长提出全球数字契约（GDC）的首要原则是“让所有人连接到互联网，包括所有学校”。此契约承认互联网连接和接入已成为确保世界各地人民的生计、安全和教育的先决条件,同时也承认学校互联网提供了关键的接入点，使所有学生都能获得信息资源，并能从小开始培养数字素养。然而目前全球仍有 27 亿人无法上网。这对处于最不发达国家和农村社群的人们尤其不利。

有意义的连接不仅仅是互联互通，而且与保障网络人权密不可分。促进社会福祉的网络接入必须将人权置于中心地位。这包括用户自由表达自我的能力；不受限制地践行民主和参与政治；任何背景的人都能在不恐惧被骚扰或歧视的情况下体验互联网；以及儿童能在网上享有与在线下相同的权利和保护。随着我们的日常生活日益依赖互联网，线上和线下的界限正变得越来越不明显，互联网既是权利的推动者，也必须无缝地纳入到既定的人权内涵中。

关键信息

数字鸿沟

- **不同国家和地区之间的数字鸿沟仍然是影响国家和国际发展的强大因素**，包括影响可持续发展目标（SDGs）的进展，尤其是最不发达国家和小岛屿发展中国家（SIDS）。数字鸿沟远不止是互联互通方面的鸿沟。有意义的接入包括可访问性、可负担性、内容、服务、数字素养和其他能力以及连通性等问题。对许多人来说，负担能力是一个特别的问题，特别是在全球南方。

- **COVID-19 大流行展示了互联网在增强个人和经济韧性方面的作用，但也表明了那些尚未连接至互联网及未进行有意义连接的人在很大程度上处于不利地位。**这可能加剧其他不平等。理解与 COVID-19 相关的干预措施在互联网的获取，使用以及人权的全面影响尚需要时间。

- **在所有社会中，有些群体比其他群体的数字鸿沟更大，或更缺乏有意义的接入。**在许多社会中，女性的网络连接比男性少，对连接的利用也较少。弱势和被边缘化社群的数字劣势更大。许多人由于年龄、性别、族裔、语言、社会阶层等其他因素而经历多重劣势。在基础设施、设备和服务方面采取有针对性的措施可以帮助提高连接较少社会群体的接入率，但同时需要采取方法

来解决有意义的接入方面的其他问题，并应与其他举措相结合以解决劣势和歧视。

- **富有韧性和安全的数字基础设施对数字包容至关重要。各国政府应保护和促进所需的基础设施，包括电网、离网电力以及通信网络。**在非洲和其他大陆的部分地区，农村和偏远社区之间的距离遥远，这也包括小岛屿发展中国家的社区。这使得最后一英里的连接在商业上对私营部门缺少吸引力。连接、速度和可靠性是基础设施供应的重要方面。提高基础设施能力和解决区域失衡问题需要时间和投资，尤其是在农村地区。

- **利益相关方群体之间的合作对于确保和促进接入十分重要。各国政府和多利益相关方伙伴应支持建立有效的监管机构和工作框架，解决因商业上缺乏吸引力的领域所带来的挑战，以及鼓励以创新方式实现互联互通，**包括社区网络、适当的频谱分配、近地轨道卫星提供的接入和本地内容（包括本地语言内容）的可用性。

性别数字鸿沟与女性权利

- **男性上网或拥有移动网络连接的可能性明显高于女性。**在最不发达国家，性别数字差距尤其巨大。在消除这一差距之前，旨在实现普遍、负担得起的互联网接入的可持续发展目标 9c 无法实现。

- **暴力和骚扰的威胁阻碍了女性的在线参与。**网络性别暴力是推动和加剧互联网接入和使用方面性别不平等的重要因素，并导致一些女性离开网络空间。技术服务和平台在宣传基于性别的暴力方面的角色应得到承认和解决。应指导女性抵制和纠正基于性别的在线暴力，包括通过社区组织的求助热线等。应以本地语言提供有关平台的资源、社区准则和报告。

- 按照联合国妇女署的建议，**应将性别平等、包容以及女性权利和保护的概念纳入全球数字契约（GDC）。**

人权和数字发展

- **普遍接入应尊重人权，以确保互联网对所有人而言都是可接入和安全的。**数字权利包括言论和结社自由、隐私权以及国际权利协定规定的其他公民权利、政治权利、经济权利、社会权利和文化权利。互联网治理架构和数字技术设计应尊重这些权利。标准制定组织应该考虑邀请来自所有利益相关方社群的线上人权专家参与他们的工作。

- **人权方面的透明度、问责制和尽职调查是所有利益相关方群体的责任，包括政府间和国际性组织、政府、私营部门、技术社群和公民社会。**这将要求商

业实践与数字权利结合起来，并要求利益相关方开展合作，以解决虚假信息、歧视和仇恨言论等问题，特别是在政治动荡、选举和权力转移时期。

- **接入互联网为获取信息和表达途径提供了一个关键的机会。**政府应避免关闭互联网，因为这对人权和经济福利都有负面影响。社交媒体和技术公司应该支持公民就关闭互联网问题所建立的倡议工作。

- **加强对数字权利的监督和实施尤其重要。**关于在联合国系统内建立多利益相关方参与的国际监督安排，一些建议已被提出。这些建议可以补充和发展现有机制，包括与数字发展和权利有关的机制，以及气候变化等其他领域的机制。

- 作为更广泛的改善教育政策的一部分，**互联网为加强受教育权提供了机会。**由于缺乏网络连接，全球南方的教育质量受到影响，特别是在疫情大流行期间。尽管信息通信技术可以使学生获得有意义的接入，但全球和本地采用率的差异加剧了大流行前的不平等。大流行期间的经验可用于改进未来数字资源的使用。

- **应努力帮助规模较小的本地企业最大限度地利用互联网。**自 2020 年以来，中小企业对数字化工具的使用大幅增加，但微型企业在业务数字化能力方面仍面临重大挑战。

- **在线平台所带来的劳动力市场变化为创造就业和提高就业质量带来了机遇和挑战，**特别是对于大多数国家非正规部门中比男性发挥更大作用的女性而言。缺乏培训仍然是许多人最大限度发挥其就业潜力的障碍。

- **必须提高数字化能力，教学、学习和培训方法也需要调整，以适应教育和就业的新范式。**重要的是要找出并缩小行业需求与高等教育之间的差距。

避免互联网碎片化

主题

维护一个全球开放和可互操作的互联网是 IGF 的核心价值之一。这意味着整个互联网继续采用共同的技术标准和协议，以实现跨国家和地区网络间的互联互通；以及内容和服务的标准符合人权和法规。应用一个框架于互联网——其优先考虑用户的权利和自由，以及基础设施和端到端的一致性——这些呼吁都已经在全球数字契约的计划中得到了响应。

互联网碎片化的风险是真实存在的，而且还在不断增加。尽管技术和商业碎片化——互联网的运作受到各种自愿和非自愿条件以及商业实践的综合影响——需要加以解决，但是影响互联网开放性和互操作性的政府政策造成的碎片化也值得关注。

关键信息

对问题的理解

- **全球数字契约为重申一个开放连接的互联网的价值提供了机会，这有助于实现《联合国宪章》、实现可持续发展目标和行使人权。**互联网社群就一个全球完整的互联网作为人类活动平台的价值达成了广泛的共识。

- **在互联网碎片化的讨论中提出的问题是多层次的，不同的利益相关者对这个术语给出了各种不同的含义和解释。**一些人最关心互联网的技术和基础设施，而另一些人则关注公共政策问题，包括接入、权利和对用户体验的影响。IGF 政策网络所编写的关于互联网碎片化的框架草案对这些问题进行了探讨。如果我们要达成有效和协调一致的应对措施，尊重和理解不同人对碎片化的看法和体验至关重要。

- **广泛的政治、经济和技术因素都可能潜在地推动碎片化。**然而，多样性和去中心化不应被误认为碎片化。这些从根本上来说都是互联网架构和运营的积极方面。

处理碎片化的风险

- **有效的多利益相关方治理机制对于治理一个全球完整的互联网至关重要。**有必要加强对这些机制的信任，确保它们是强有力和可持续的，并在治理结构不断发展以迎接新挑战的同时促进这些结构之间的一致性。
- **有必要对新的或正在形成的碎片化风险保持警惕。**全球合作和协调对于查明早期预警迹象、了解政策和其他事态发展的影响以及准备应对这些变化至关重要。多利益相关方模式最适合于评估、评价和监督影响互联网措施的潜在意外后果，并提出有效的替代办法，以避免或减轻碎片化的风险。IGF 政策网络在针对互联网碎片化的方面就是一个积极示范。

- **互联网开放有助于促进互联网用户享有人权，促进竞争和机会平等，并保护互联网生成的对等天性。**关于网络中立和非歧视性流量管理的辩论仅仅属于这方面广泛讨论的一部分。网络中立对于保障互联网开放是必要但不足够充分的条件。基础设施和数据互操作性以及平台和设备的中立性也是必要的。

- **尽管世界各地的法律、监管和政策模式不同，但跨国际边界的积极协调对于确保碎片化措施不会威胁到互联网的全球覆盖和互操作性至关重要。**维持全球网络的完整性需要国际监管合作，并就基本原则达成共识。

- **许多不同的因素影响着不同法域的互联网体验，包括不同的社会、人口、经济、文化和政治环境以及技术和基础设施问题。**在国家层面追求某些形式的数字治理会增加互联网技术层面的碎片化风险。然而，监管框架还必须考虑不同情况下的不同要求，并跟上技术和服务的快速变化。

- **有必要加强利益相关方之间的知识和信息共享，**进一步讨论网络外交这一不断演变的现象，并考虑适当干预的范围。标准制定机构应继续加强与利益相关方的接触和互动，并增进政策和技术社群之间的理解。标准化组织应通过所有受影响的利益相关方的直接参与，讨论具有政策影响力的技术层面的决定。

数据治理和隐私保护主题

数据是全球化数字时代的关键资源。数据流动促进经济增长，同时数据分析，包括大数据分析，也一直是金融、健康、执法等各领域取得突破性创新的基础。

但数据的广泛使用、常规性跨境流动和可替代性仍然是十分敏感且亟待解决的问题。作为一种跨国商业资产，数据流动在缺乏各国间法律制度一致性的环境下运行，会给执法带来重大挑战。从数据收集到应用和存储，数据交换常会牺牲个人隐私。这会对信任和安全造成严重影响。

若想发挥数据在经济和研究方面的巨大潜力，需要围绕治理、诚信和个人隐私保护展开重新讨论。

关键信息

数据的中心性

- **在日益数字化的时代，数据已成为关键资源。**数据流动对许多领域的跨国合作至关重要，包括科学研究、执法以及国家和全球安全。数据、数据安全和数据保护是可持续发展的重要保障。在全球范围内有效使用和共享数据，有助于应对共同的挑战，如疫情、气候变化等连锁危机带来的威胁。

- **数据可以产生利润和显著的社会价值。**然而，到目前为止，数据驱动的经济利益分配不均。许多人担忧他们可能成为主要数据提供者，而非受益者。

- **数据生成者和使用者之间的关系十分重要。**数据贫困是一个重大问题，特别是在本地社区和弱势群体中。缺乏数据隐私和保护会破坏对数据管理的信任。在各级政府、教育课程和公众中建立数据素养和数据能力是重要的解决方式。

- **数据管理和治理是国家和国际治理中的复杂问题。**数据开发利用——包括大数据分析、人工智能和机器学习的创新，以及公共政策层面和可持续发展目标的创新——需要适当考虑政治、经济和社会影响，并结合细致的政策干预。政府和监管机构需要一定的基础设施和能力，以构建有效、综合的国家数据治理框架。应用程序开发人员有责任确保设计的安全性并符合道德规范。

数据隐私和数据正义

- **数据隐私并非便利或良好实践问题，而是关乎人权。**除了隐私权、平等待遇和非歧视之外，数据还影响其他方面的人权，如获得医疗、教育和公共服务的权利，以及言论自由、结社自由等民主权利。隐私法应该是实质性的、有理有据的，并且能够明确执行。受到这些影响的人应该可以清楚地理解其影响。

- **数据流动和数据交换应在不损害数据隐私的情况下进行。**在数据交换、信息收集和使用过程中，个人数据隐私经常受到侵害，对信任和安全造成有意/无意的风险。互联网接入和使用不应依赖数据跟踪：用户应该有权选择信息分享范围，包括由其在线行为产生的信息。个人数据不应被引入没有充足保证的法域。

- **政策应从数据保护延伸到数据正义，让人们可以选择如何使用个人数据，以及在何处分享由其数据集产生的创新收益和好处。**因此，隐私保护应促进更安全、更繁荣的数字经济。

- **政府和监管机构应确保个人数据得到保护**，确定不同利益相关方的不同责任，而不给个人用户施加过度的负担或责任。数据治理政策应参考多利益相关方的意见，以确保实施过程中的挑战能够被充分吸收理解。

- **隐私和数据保护对于人工智能和机器学习的治理尤为重要。**人工智能供应链中的所有利益相关方都能在维护隐私权方面发挥作用。

- **需要配备拥有适当资源的独立监督机构。**数据保护办公室应授权管理数据登记、提供指导、实施调查和解决数据主体的投诉。

数据治理

- **与数据治理有关的问题及其影响不应被孤立看待。**当前的数据治理格局是由碎片化的国家、区域和国际规则拼凑而成，涉及各国政府、私营部门和个人的责任。

- **全球要加强一致性，实现数据为人类和地球服务的平衡之道。**国家、区域和国际层面现有的立法和监管框架不足，无法跟上技术和应用的变化步伐。这些框架应确保拥有数据的企业和其他组织采用高水平的安全标准。

- **不同的背景和挑战、历史、文化、法律传统、监管架构意味着不可能形成一套针对所有人的刚性规则。**不同的个人和组织也以不同的方式诠释着大致相似的模式。尽管各国和地区必须制定符合自己的数据治理模式，但也应保持一致性和互操作性，以促进数据流动、确保公平竞争。

- **透明度、参与度和问责制是良好数据治理的重要方面。**数据治理的重要考虑因素包括（但不限于）：数据标准和分类；数据共享、交换和互操作性；数据安全和数据隐私；数据基础设施；数据和数字身份；数据正义与公平；数据可追溯性、透明度和可解释性；数据最小化和数据限制；数据准确性和质量；数据偏见、边缘化和歧视；数据生命周期、数据使用的明确性和保存时间；数据问责制和数据伦理；数据危害、数据安全和数据保护。

- 包括监管机构、研究人员、标准化组织、消费者组织和终端用户等在内的**多个多利益相关方扮演着一定角色，应运用其权力和影响力以促进有效的数据治理。**数据治理政策的制定应基于多方利益相关方社群的意见。他们在围绕隐私的法律辩论和实施有效数据隐私解决方案的“现实世界”挑战的方面具有一定的专业知识。

- **发展中经济体需要加强其制度能力的建设，以全面、客观和循证的方式治理、使用和管理数据，包括通过区域和全球合作。**这需要进一步了解政府官员和其他利益相关方的制度能力。

跨境数据流动

- **跨境数据流动对电子商务和数字贸易的许多方面至关重要。**有效的区域内贸易和供应链管理依赖于数据以及货物、服务和资本的顺畅流动。然而，这些需要考虑复杂的交叉因素：监管的趋同性，法律框架的协调，互联网治理，信息和通信技术政策改革，以及战略性区域基础设施实施。

- **目前的多边、区域和双边贸易协定不能完全适用于当前和未来的跨境数据流动。**这些都是在基本上不受监管的环境中运作，国家法律制度之间几乎没有一致性。各国采用的方式不同，且各有背景，因此造成贸易壁垒，许多国家目前没有足够的立法或执法能力。制定和协调管理跨境数据流动的措施愈发必要，以促进不同背景下的发展和经济价值创造，同时尊重国家主权和用户隐私。

实现安全、安保和问责制
主题

互联网面临的安全威胁主要有几个方面。传统的网络安全涉及保护网络、设备和数据免受未经授权的访问或被犯罪使用。持续存在的网络攻击问题也包括在内，无论这些攻击来自个人还是国家制裁，目标是公民、商业还是政府。缺乏广泛和具有约束力的网络安全协定、网络安全性不足等因素导致充分利用数字技术带来的经济效益的机会流失，特别是对发展中国家而言。

安全、安保和问责制的问题应该从多方面考虑，包括基础设施、服务、内容和互联网的其他方面。例如，现在我们对安全和安保的理解包括在线虚假信息和错误信息的持续挑战。近年来，这些因素加剧了新冠肺炎疫情的影响，并对世界各地的选举进程构成重大风险。这强调了对误导性内容建立责任制并明确标准的必要性。

考虑到“绿色”互联网和减少与数字消费相关的碳排放，“安全”的概念可能会进一步扩大到包括环境安全。解决数字化对环境的影响是 IGF 讨论中日益重要的主题。

关键信息

政策制定者的作用

- **网络安全应被视为互联网政策的核心挑战。**信任和安全方面的考虑对安全、可靠接入的发展不可或缺，包括尊重人权、政策制定的公开和透明，以及服务终端用户利益的多利益相关方模式。

- **确保网络安全和预防网络犯罪是同等重要的政策领域，需要高度重视和发展专业能力。**然而，它们目标不同，所需的方法也不同。针对一个方面有效的方法不适用于其他方面，需要进行调整和重新制定。

- **网络安全和网络犯罪问题具有跨组织、跨境等多层性质。解决这些问题需要：**
  a）**全政府和全社会通力合作**，包括强有力的伙伴关系和协调努力，涉及议会、监管机构、其他有关政府主管部门和机构、私营部门、技术社群、学术界和公民社会；以及
  b）**政府间、多边和多方利益相关方的高效和有效的区域和国际合作。**

- **各国政府、私营部门和技术社群应注意避免通过的网络犯罪法和建立的有关标准对网络安全维护者的工作产生负面影响。**他们应邀请所有利益相关方共同参与政策制定，并促进不同社群之间的互动及经验和专门知识的交流。

- **公民社会应参与网络犯罪和网络安全讨论。**为确保进行有效讨论，公民社会利益相关方应就所涉及的不同方法和问题进行自我教育，并与其他利益相关方合作，收集充分参与决策所需的信息和资源。

网络安全

- **国际社会应探索切实可行的方式，将网络安全能力建设纳入到更广泛的数字发展主流中。**数字化转型的愿望与实现有效网络安全的需求之间的紧张关系，对实现安全、可靠的在线环境和实现可持续发展目标构成了挑战。提高数字基础设施的弹性十分重要，但这还不够。将现有的国际协定转化为可行的行动势在必行。

- **实现网络安全的标准对于构建开放、安全和有弹性的互联网至关重要，这有利于促进社会进步和经济增长，特别是对保护尚未联网人们的安全也很关键。**此类标准已经制定，但大量的使用需求才能促成其充分有效地发挥作用。联合国可以通过将关键标准的推广纳入全球数字契约、支持倡议和能力建设，鼓励测试和监督部署等举措，加速关键标准在全球范围的采纳。在联网需求大且互联网仍处发展期的地区，尽早提高认识、加强标准能力建设是优先事项。

- **仍需加大力度提高国家政策制定者和其他利益相关方对网络安全、国际规范和原则带来挑战的认识。**这应包括认识可持续发展与网络安全之间的联系，加强相关能力建设，将不同的利益相关方聚集在一起，组织促成有效、可持续和包容性的国际合作以提高网络弹性。现已有许多国际举措对此进行支撑。资助机构和其他利益相关方也需要把握为网络弹性提供资金的机会。

- **网络安全规范必须影响互联网用户过去、现在和未来的体验。**在这种情况下，倾听遭受网络安全攻击的个人和组织以及第一响应者的经历非常重要，特别是当制定新规范的背景之时。

网络犯罪

- **网络犯罪对许多互联网用户构成越来越大的威胁。**打击网络犯罪的法规应当对平台规模、能力和资源足够敏感。法律义务应考虑技术部门的多样性，并认识到小企业在遵守其法律义务方面的需求和情况，例如打击恐怖和暴力极端主义分子对其服务的滥用。

- **各国政府和政策制定者应确保对犯罪和恐怖分子使用互联网的法律回应既保障法治又保障人权，**充分考虑到言论自由，并在打击网络犯罪的同时确保透明度和问责制。

内容和虚假信息

- **可以并且应该通过解决个人和社会所面临风险的机制来应对虚假信息，同时保护言论自由、多元化和民主进程。**对专业新闻和媒体的支持在解决虚假信息方面发挥着重要作用，包括对既定新闻规范的承诺。

- **媒体和数字素养技能赋权公民对所遇到的内容或信息持更具批判性的态度，这有助于识别虚假信息和错误信息，提高民主参与度。**数字素养教育有助于提高在线安全意识，尤其是对弱势的个人和社群。针对不同人口群体的需求和风险所采取的各项举措需要保持敏感度。例如，针对年轻人和老年人采取的不同方法，须对应不同的使用模式。

- **教育课程应包含帮助儿童安全上网的数字素养技能。**措施应涉及父母、教师和监护人。立法者和数字平台应承担相应责任，在儿童在线权利框架内确保儿童安全。这一框架应与包括《联合国儿童权利公约》在内的国际权利协定保持一致。

- **域名系统在这方面的技术能力有限。**持续的利益相关方对话应澄清何时以及采用何种方式来补救具体的在线内容问题，同时应加强正当程序规范。

- **加密对于构建一个开放、安全和民主的互联网至关重要，**并能帮助用户实现安全、隐私和言论自由。仍有一些问题需要解决，如执法、用户对儿童保护等领域接入的管理能力。

- **翻译造成的严重障碍会阻碍终端用户有效参与平台社区标准和准则的制定。**关键术语有时翻译不到位，导致解释不明确。与不同语言社群互动以提高翻译的准确性和关联性，包括与其交流有关概念但避免采用在不同语言中直接对等的名称，对增进平台和用户的理解至关重要。

处理包括人工智能（AI）在内的前沿技术问题

主题

先进的数字技术不断塑造我们的经济和社会，包括引领在线体验、为智能设备提供动力，同时影响我们自己的决策和他人对我们作出决策的人工智能（AI）系统，以及在制造业、医疗保健和农业等不同领域部署的机器人技术和物联网应用程序。这些技术提供了发展机遇，也带来了挑战。例如，算法决策可导致偏见、歧视、刻板印象和更广泛的社会不平等，而基于人工智能的系统会对人类安全和人权构成风险。物联网设备带来隐私和网络安全挑战。增强现实和虚拟现实技术引发了公共安全、数据保护和消费保护等问题。

把握先进技术带来的机遇，同时应对相关的挑战和风险是一项任何一方都无法独自承担的任务，需要包括政府、政府间组织、技术公司、公民社会和其他利益相关方在内的多利益相关方对话和合作，以确保技术的开发和部署以人为本、尊重人权。

关键信息

治理

- **包括人工智能在内的前沿技术的设计应尊重法治、人权、民主价值和多样性，并纳入适当的保障措施。**前沿技术应该通过推动包容性增长、可持续发展和福祉来造福人类和地球。监督和执行机制应遵循一定的原则和规则，人工智能参与者应对造成的任何损害负责。

- **技术必然促进平等的假设存在缺陷。**设计机器学习技术的人和训练人工智能应用程序的数据往往在其所在社会并没有代表性。技术会加剧不平等现象，并对弱势群体以及边缘化群体造成伤害。

- **社会需要适应人工智能对合作框架和治理模式带来的变革。**构建以人为本的智能社会需要政府、企业、社会组织和学术届通力合作。为防止算法带来不受控或不想要的结果，持续的人为控制仍然必不可少。打破工程师和政策专家之间的孤岛对于实现这一目标至关重要。

- **单一进程不能促使全球就人工智能规范达成共识。**现有规范大多是软性法律，而不是具有约束力的原则。有意义的全球标准制定需要所有国家的参与，包

括发展中国家和发达国家。同时，区域性倡议的反映和所有利益相关方的参与也十分重要。

- **能力建设对于前沿技术发展很重要。**需要制定人工智能素养、技能开发和提供少数民族语言资源的政策，以便就前沿技术制定真正的全球方案。

信任、安全和隐私

- **监管框架应包括帮助社交媒体和其他平台履行勤勉尽责义务的原则，管理可能损害民主和人权的内容。**这一框架应促进在线内容审核的全球对话，以赋权用户，包括最弱势群体和少数民族语言用户。新兴技术，例如考虑计算机如何识别、理解和模拟人类情感的情感计算技术，需要进行实质性的伦理评估。

- **算法系统运行和报告的透明度对于人权至关重要。**人工智能有助于持续观察和分析数据，以个性化和定向推送内容和广告。由此产生的个性化在线体验会产生在线信息空间碎片化的风险，限制个人接触多样化的信息。信息多样性缺乏会助长操纵和欺骗——加剧不平等，破坏民主辩论，并可能加剧数字权威主义、仇恨和暴力。

- **来自技术和非技术社群的利益相关方需要交流专业知识并共同制定通用原则，这些原则和标准在**多种环境中需要足够灵活，并能促进对人工智能系统的信任。

- **承认和尊重不同国家和社群的不同制度和文化背景很重要，**促进包容性、加强人工智能领域的国际合作也是如此。

权利和内容审核

- **在线平台的内容治理政策及其执行需要符合国际人权标准。**人工智能和机器学习技术已经被用于决定内容的发布和删除、内容的优先级和传播对象。这些工具通过影响个体和集体人权的方式明显塑造政治和公共话语，包括社会、经济和文化权利以及全球和平和安全的权利。这些工具很少或根本没有透明度、问责制或公众监督。这种现象理应得到纠正。

- **用于促进人权的技术同样可以被用于实施监视、宣扬暴力意图以及侵犯这些权利的其他行为。**在冲突和危机时期，自动化内容管理产生的意外后果尤其有害，因为它们可能压制在这一时期最关键的批评声音。

- **技术标准能够促进发展，推动数字技术及相关基础设施、服务、协议、应用程序和设备的价值，同时也可能对人权产生重大影响。**然而，标准制定组织内的技术标准制定过程没有充分考虑到人权问题。这些流程通常隐晦、复杂，

而且公民社会和其他利益相关方需要大量的资源才能系统性地访问和遵循。这个问题应该要解决。