# 中国关于全球数字治理有关问题的立场

(就制定"全球数字契约"向联合国提交的意见)

信息技术革命日新月异,数字经济蓬勃发展,深刻改变 着人类生产生活方式,对各国经济社会发展、全球治理体系、 人类文明进程影响深远。与此同时,全球数字治理赤字日益 凸显,数字领域发展不平衡、规则不健全、秩序不合理更为 突出,个别国家将科技和经贸问题政治化、工具化、武器化, 人为割裂全球互联网,危害全球数字发展与合作。

面对数字化带来的机遇和挑战,各方应坚持多边主义, 坚守公平正义,统筹发展和安全,深化对话合作,完善全球 数字治理体系,构建网络空间命运共同体。中方支持联合国 在全球数字治理和规则制定方面发挥主导作用,愿与各方一 道,就数字发展及全球数字治理的突出问题寻求解决思路, 凝聚国际共识。为此,中方愿提出以下基本原则和具体建议:

一、基本原则

一是坚持团结合作。正如联合国秘书长所警告的,网络和数字领域正出现两个市场、两套标准、两条供应链。以意识形态划线,搞集团政治和阵营对抗,只会阻碍全球发展和人类进步。各国应坚持团结而非分裂、合作而非对抗、包容而非排他,在相互尊重和广泛共识基础上,讨论制定全球可互操作性的数字规则,防止数字治理规则分裂和碎片化。

**二是聚焦促进发展**。经济数字化为各国特别是发展中国家提供重要发展机遇。各国应拓展数字合作,促进数字贸易,弥合数字鸿沟,构建普惠平衡、协调包容、合作共赢、共享繁荣的全球数字经济格局;应尊重网络主权,尊重各国根据自身国情自主选择数字发展道路;应平衡发展与安全,为数字发展营造开放、包容、公平、公正、非歧视的环境,反对泛化滥用安全问题遏制打压他国正当经济和科技发展。

**三是促进公平正义。**各国特别是发展中国家获取和发展 数字技术、产品和服务,是不可剥夺的合法权利,对于弥合 数字鸿沟、实现可持续发展目标至关重要。应推动国际合作 与援助,反对技术垄断和单边强制措施,维护全球数字技术 产品和服务的供应链开放、安全、稳定,提升全球数字发展 的公平性、有效性、普惠性;各国应努力解决数字经济给社 会弱势群体带来的挑战,确保各阶层、各群体从数字发展机 遇中均衡获益,共享数字发展红利。

**四是推动有效治理。**面对网络安全、数据安全、关键信息基础设施安全、平台监管、个人隐私、仇恨言论等各方共同关切,应以联合国为主导,在所有成员国普遍参与的基础上协商制定国际规则,推动建立多边、民主、透明的国际互联网治理体系,实现互联网基础资源公平分配、共同管理。 国际组织、信息技术企业、技术社群、民间机构等各主体可积极发挥与自身角色相匹配的作用。

- 2 -

二、具体建议

## (一) 确保所有人接入互联网

各国应进一步推动实现公平合理普遍的互联网接入、互 联网技术的普及化、互联网语言的多样性,加强数字互联互 通,确保人人共享互联网和数字技术发展成果;各国有权平 等参与国际互联网基础资源管理和分配,反对利用互联网基 础资源和技术优势,损害他国接入互联网的合法权益,危害 全球互联网安全、稳定联通。

应加强各国数字能力建设,保障发展中国家和平利用互 联网基础资源和技术的权利,支持向发展中国家提供包括资 金、技术转让、关键信息基础设施建设、人员培训等能力建 设援助,助其可负担地接入互联网;鼓励各国政府、企业、 民间机构通过投资、教育、培训、技术创新应用等,帮助老 年人、妇女、未成年人、残疾人、贫困人口等群体接入和使 用互联网,提高数字包容性;加强知识分享和发展政策交流, 鼓励青年、妇女等民间交流,为落实 2030 年议程汇聚众力。

## (二)避免互联网碎片化

应致力于维护一个和平、安全、开放、合作、有序的网 络空间,反对互联网分裂和碎片化。应以联合国为主导,在 成员国普遍参与的基础上,讨论制定一套全球可互操作性的 网络空间规则和标准,推动构建多边、民主、透明的国际互 联网治理体系。 各国应秉持发展和安全并重原则,推动信息通信基础设施互联互通,加强互联网技术和平利用、合作共享;不得泛 化国家安全概念,滥用管制工具,任意阻断全球信息通信产 品供应链,特别是在商业基础上长期合作形成的供应;支持 企业基于商业考虑作出独立选择使用信息通信技术和产品; 应坚持合作和普惠原则,充分考虑发展中国家在数字贸易领 域面临的独特机遇与挑战,推动制定开放、包容的高水平数 字贸易规则,加强各国政策协调,促进世界范围内公平自由 的贸易和投资,反对贸易壁垒和贸易保护主义,推动形成世 界数字大市场。

## (三)保护数据

应以事实为依据全面客观看待数据安全问题,促进数据 依法有序自由流动;反对利用信息技术破坏他国关键基础设 施或窃取重要数据,以及利用其从事危害他国国家安全和社 会公共利益的行为。

各国应尊重他国主权、司法管辖权和对数据的安全管理 权,未经他国法律允许不得直接向企业或个人调取位于他国 的数据;各国如因打击犯罪等执法需要跨境调取数据,应通 过司法协助渠道或其他相关多双边协议解决。国家间缔结跨 境调取数据双边协议,不得侵犯第三国司法主权和数据安全。

信息技术产品和服务供应企业不得在产品和服务中设置 后门,非法获取用户数据、控制或操纵用户系统和设备;产 品供应方应承诺及时向合作伙伴及用户告知产品的安全缺陷 或漏洞,并提出补救措施。

## (四)保护线上人权

发展权是首要的基本人权。应通过数字创新和数字发展, 弥合数字鸿沟,推动数字发展成果更多、更公平惠及全世界 人民;反对滥用单边强制措施,损害他国发展数字经济和改 善民生的能力,造成对人权的持续系统性侵犯;反对人权问 题政治化,反对以保障线上人权为名干涉别国内政、挑战别 国司法主权。

各国应致力于向本国不同人群,特别是社会弱势群体, 提供持续、稳定、普惠、开放的数字产品和服务,缩小一国 内部不同群体和地域之间的数字能力差距;应加强对老年人、 妇女、未成年人、残疾人、贫困人口等群体数字技能培训, 提升全民数字素养和技能,特别是根据老年人需求特点,提 供更多智能化适老产品和服务,不断改善老年人服务体验。 通过上述,维护和促进有关人群的发展权。

各国应尊重公民在网络空间的权利和基本自由。同时, 各国有权对境内网络信息传播实施保护、管理与指导,防范、 制止侵害公民合法权利、损害公共秩序、煽动暴力、歧视、 排外和相关不容忍行为、危害国家安全的不法行为,保障老 年人、妇女、未成年人、残疾人、贫困人口等群体合法权益。 各国应承诺采取措施防范、制止利用网络侵害个人信息 和隐私的行为,反对滥用信息技术从事针对他国的大规模监控、非法采集他国公民个人信息;应共同打击非法窃取、曝光、贩卖公民个人隐私信息、商业数据等行为;应提高企业数据安全保护意识,加强行业自律,保护网络空间个人信息和隐私。

## (五) 制定针对歧视和误导性内容的问责标准

各国应采取适当举措,包括建立健全相关法律法规、鼓 励互联网行业组织建立健全行业自律制度和行业准则、加强 对互联网企业指导监督等,防止个人和组织利用互联网发布 危害国家安全、煽动颠覆国家政权、煽动分裂国家、破坏国 家统一的信息,宣扬恐怖主义、极端主义、种族仇恨、种族 歧视言论,编造、故意传播谣言扰乱经济秩序和社会秩序, 传播暴力、淫秽色情信息,以及侮辱诽谤他人、侵害他人名 誉、隐私、知识产权和其他合法权益等;鼓励互联网企业建 立健全公众投诉、举报和用户权益保护制度,主动接受公众 监督,及时处理公众投诉、举报,并依法承担对用户权益造 成损害的赔偿责任。

## (六)加强人工智能治理

各国应在普遍参与的基础上,通过对话与合作,推动形成具有广泛共识的国际人工智能治理框架和标准规范,确保 人工智能安全、可靠、可控,更好赋能全球可持续发展。各国应坚持"以人为本"和"智能向善"理念,反对利用人工

- 6 -

智能危害他国主权和领土安全的行为,反对以意识形态划线、 构建排他性集团、恶意阻挠他国技术发展的行为,确保各国 充分享有技术发展与和平利用权利,共享人工智能技术惠益。

各国应坚持伦理先行,建立并完善人工智能伦理准则、 规范及问责机制,明确人工智能相关主体的职责和权力边界, 充分尊重并保障各群体合法权益。各国应立足自身人工智能 发展阶段及社会文化特点,逐步建立符合自身国情的科技伦 理审查和监管制度,加强人工智能安全评估和管控能力,建 立有效的风险预警机制,采取敏捷治理,分类分级管理,不 断提升风险管控和处置能力。

各国应要求研发主体加强对人工智能研发活动的自我约 束,避免使用可能产生严重消极后果的不成熟技术,确保人 工智能始终处于人类控制之下。各国应要求研发主体努力确 保人工智能研发过程的算法安全可控,不断提升透明性、可 解释性、可靠性,逐步实现可审核、可监督、可追溯、可预 测、可信赖;努力提升人工智能研发过程的数据质量,提升 数据的完整性、及时性、一致性、规范性和准确性等。各国 应要求研发主体充分考虑差异化诉求,避免可能存在的数据 采集与算法偏见,努力实现人工智能系统的普惠性、公平性和 非歧视性。

各国应禁止使用违背法律法规、伦理道德和标准规范的 人工智能技术及相关应用,强化对已使用的人工智能产品与 服务的质量监测和使用评估,研究制定应急机制和损失补偿 措施。各国应加强人工智能产品与服务使用前的论证和评估, 推动人工智能培训机制化,确保相关人员具备必要的专业素 质与技能。各国应保障人工智能产品与服务使用中的个人隐 私与数据安全,严格遵循国际或区域性规范处理个人信息, 反对非法收集利用个人信息。

## (七) 数字公共产品

国家主权原则应适用于网络和数字空间。各国对本国境 内信息通信基础设施、资源和数据及信息通信活动拥有管辖 权,有权制定本国互联网公共政策和法律法规,保障公民、 企业和社会组织等主体在网络空间的合法权益。

与此同时,提高数字产品的开放性,对于释放数字技术 潜力、推动实现可持续发展目标,特别是对中低收入国家而 言,具有积极意义。各国可在尊重各国主权、数据安全、公 民合法权益以及自愿原则的基础上,就开放数字产品的标准、 范畴、管理方式、使用规范等进行讨论,逐步凝聚共识。各 国应提升公共服务数字化水平,加强在线教育等领域国际合 作,加强可持续发展目标监测评估数据合作与共享,更有效 推动 2030 年议程落实。

# **China's Positions on Global Digital Governance**

(Contribution for the Global Digital Compact)

The phenomenal development of information technology revolution and digital economy is transforming the way of production and life of mankind, exerting far-reaching influence over social and economic development of States, global governance system and human civilization. In the meantime, the global digital governance deficit is becoming increasingly prominent, and such problems as unbalanced development, inadequate rules and inequitable order have become more evident in the digital field. Certain country has politicized science and technology as well as economic and trade issues, and used them as a weapon and tool to divide the global Internet, jeopardizing global digital development and cooperation.

In the face of both opportunities and challenges brought by digitalization, all parties should uphold multilateralism, stick to fairness and justice, take a balanced approach to development and security, step up dialogue and cooperation, and work together to improve the global digital governance system and build a community with a shared future in cyberspace. China supports the leading role of the United Nations in global digital governance and rules-making, and stands ready to join all parties in exploring solutions to the prominent issues in digital development and digital governance and building international consensus in this regard. To this end, China would like to put forward the following basic principles and proposals.

#### **Basic Principles**

Uphold unity and cooperation. As the UN Secretary-General has warned us in a similar way, two markets, two sets of standards and two supply chains are also emerging in the cyber and digital domain. Drawing ideological lines or instigating group politics and bloc confrontation will only set obstacles in the way of global development and human progress. States should adhere to unity rather than division, cooperation rather than confrontation, inclusiveness rather than exclusion, and formulate globally interoperable common rules and standards on the basis of mutual respect and broad consensus, and prevent the division and fragmentation of digital governance rules.

Focus on development. Economic digitalization has offered significant opportunities to all States, in particular the developing ones. States should expand digital cooperation, promote digital trade, bridge the digital divide, and build a global digital economic paradigm featuring benefits for all, balance, coordination, inclusiveness, win-win cooperation and common prosperity. States should respect others' cyber sovereignty as well as the right to independently choose their own paths of digital development in light of their own national conditions. States should put an equal emphasis on development and security, forge an open, inclusive, fair, just and non-discriminatory environment for digital development, and refrain from overstretching and abusing the issue of security to contain and suppress the legitimate economic and technological development of other States.

Promote fairness and justice. Access to and development of digital technologies, products and services is the inalienable legitimate right of all States and especially developing ones, and is crucial to bridge the digital divide and achieve the Sustainable Development Goals (SDGs). States should promote international assistance, stand against cooperation and technological monopoly and unilateral coercive measures, maintain an open, secure and stable supply chain of global digital products and services, and make global digital development more equitable and effective and beneficial to all. States should make efforts to address the challenges posed by digital economy to vulnerable groups, ensuring that people from all walks of life can share the benefits and dividends of digital development on an equal footing.

**Facilitate effective governance**. In the face of such issues of mutual concern as cybersecurity, data security, critical information infrastructure security, platform regulation, personal privacy and hate speech, States should formulate international rules through wide participation and extensive consultation

among all Member States under the auspices of the UN, work together to build an international Internet governance system featuring multilateralism, democracy and transparency, and ensure equitable distribution and joint management of basic Internet resources. International organizations, ICT companies, technology communities, civil organizations and other stakeholders can play their part commensurate with their roles and responsibilities.

#### **Specific Proposals**

#### 1. Connect all people to the Internet

States should further promote fair, reasonable and universal access to the Internet, facilitate the popularization of Internet technology and linguistic diversity on the Internet, and enhance digital connectivity, ensuring that the benefits of the Internet and digital technology developments are shared by all. States have the right to participate in the management and distribution of basic international Internet resources on equal footings, and should refrain from taking advantage of Internet resources and technologies to undermine the legitimate rights of other States to access the Internet, thus endangering the security, stability and connectivity of the global Internet.

States should strengthen digital capacity building, ensure developing countries' rights of peaceful use of Internet resources and technologies, and support providing developing countries with capacity building assistance including finance, technology transfer, critical information infrastructure development and personnel training, enabling those countries to have affordable access to the Internet. It is encouraged that governments, businesses and civil organizations should assist the elderly, women, minors, people with disabilities and the poor in their access to and usage of the Internet through investment, education, training, innovation and application of technologies to increase digital inclusiveness. Exchanges on knowledge and development policies should be enhanced, and people-to-people exchanges, including those among youth and women should be encouraged, in order to forge synergy for the implementation of the 2030 Agenda.

#### 2. Avoid Internet fragmentation

States should foster a cyberspace featuring peace, security, openness, cooperation and order, and stand against division and fragmentation of the Internet. States should formulate globally interoperable common rules and standards in cyberspace through broad participation of Member States under the auspices of the UN, and stay committed to building an international Internet governance system featuring multilateralism, democracy and transparency.

States should put an equal emphasis on development and security, promote information infrastructure connectivity, and ensure peaceful use, cooperation and shared benefits of the Internet technologies. States should not overstretch the concept of national security nor abuse control tools to arbitrarily block the supply chain of global ICT products, in particular those based on long-term commercial relationship, and support enterprises in making their own independent choices based on business consideration to use ICT technologies and products. States should uphold the principles of cooperation and shared benefits, take into full consideration the unique opportunities and challenges faced by developing countries in relation to digital trade, and facilitate formulation of high-level digital trade rules in an open and inclusive manner. States shall enhance policy coordination, promote fair and free trade and investment globally, and oppose trade barriers and trade protectionism to create a global digital market.

#### 3. Protect data

States should handle data security in a comprehensive, objective and evidence-based manner, and ensure free flow of data in an orderly manner and in accordance with the law. States should stand against ICT activities that impair or steal important data of other States' critical infrastructure, or use the data to conduct activities that undermine other States' national security and public interests.

States should respect the sovereignty, jurisdiction and

governance of data of other States, and shall not obtain data located in other States through companies or individuals without other States' permission. Should States need to obtain overseas data out of law enforcement requirement such as combating crimes, they should do it through judicial assistance or other relevant multilateral and bilateral agreements. Any bilateral data access agreement between two States should not infringe upon the judicial sovereignty and data security of a third State.

ICT products and services providers should not install backdoors in their products and services to illegally obtain users' data, control or manipulate users' systems and devices. Products providers should make a commitment to notifying their cooperation partners and users of serious vulnerabilities in their products in a timely fashion and offering remedies.

## 4. Apply human rights online

Right to development is the primary and basic human right. States should facilitate digital innovation and development, bridge digital divide, and enable more people around the world to share the benefits of digital development in a more equitable way. States should oppose the abuse of unilateral coercive measures that undermine other States' capabilities to develop digital economy and improve people's livelihood, or pose consistent and systemic violation of human rights. States should refrain from politicizing human rights issues, or interfering in others' domestic affairs and challenging others' judicial sovereignty under the excuse of protecting online human rights.

States should dedicate themselves to providing consistent, stable and open digital products and services that deliver benefits to all their citizens, in particular the vulnerable, and narrow down the digital capacity gap among different groups and regions. Training on digital skills should be further extended to the elderly, women, minors, people with disabilities and the poor, so that digital capacity and skills of all people could be enhanced. In particular, more smart products and services that are suited to the needs and characteristics of the elderly should be provided for them to enjoy better service experience. By taking aforementioned actions, the right to development of specific groups will be better protected and promoted.

States should respect the rights and fundamental freedoms of their citizens in cyberspace. In the meantime, States are entitled to protect, manage and regulate the transmission of Internet information, in order to prevent and stop any rights violation of their citizens, as well as any illicit acts that jeopardize the public order, incite violence, discrimination, exclusion and intolerance, or undermine national security. States should take actions to protect the legitimate rights and interests of the elderly, women, minors, people with disabilities and the poor. States should be committed to taking actions to prevent and stop acts that jeopardize personal information and privacy through the use of ICTs, and oppose mass surveillance against other States and unauthorized collection of personal information of other States with ICTs as a tool. States should make joint efforts to combat illicit stealing, exposure and trade of personal information and commercial data. States should help businesses improve their awareness of data protection, increase self-discipline, and take concrete actions to protect personal information and privacy in cyberspace.

# 5. Introduce accountability criteria for discrimination and misleading content

States should take appropriate measures, including formulating and improving the framework of laws and regulations, encouraging ICT organizations to conduct self-discipline and introduce code of conduct, and increasing regulation and supervision of ICT companies, to prevent individuals and organizations from using the Internet to engage in illicit acts. Such acts include but are not limited to publishing information that endangers national security, incites subversion and secession, and jeopardizes state unity, spreading rhetoric of terrorism, extremism, racial hatred and discrimination, fabricating and intentionally transmitting rumors that disturb the social order, economic and transmitting violent and pornographic content, and insulting and slandering others and violating others' reputation, privacy, intellectual property rights and other legitimate rights and interests. States should encourage ICT companies to establish or improve systems of handling public complaints and reports and protecting customers' rights. Relevant companies should take an initiative to receive public supervision, handle public complaints and reports in a timely manner, and offer compensation to their users for any violation of their rights and interests in accordance with law.

### 6. Promote regulation of artificial intelligence (AI)

States, on the basis of broad participation, should promote the formation of a framework and a set of standards for international AI governance with broad consensus through dialogue and cooperation, and ensure that AI is safe, reliable and controllable and better empowers global sustainable development. States should stick to a people-centered approach and the principle of AI for good, oppose moves that undermine the sovereignty and territorial security of other countries by using AI technology, refrain from drawing ideological lines or setting up exclusive groups to maliciously obstruct other countries' technological development, and ensure all countries' rights of development and peaceful use of technologies in order to share the benefits of AI technologies.

States should give priority to ethics, establish and improve rules, norms and accountability mechanisms for AI ethics, clarify responsibilities and power boundaries of AI-related entities, fully respect and protect the legitimate rights and interests of all groups. States should, in light of their own stage of AI development as well as social and cultural characteristics, gradually establish review and regulation mechanisms for ethics in science and technology suited to their national conditions, strengthen evaluation and management capacity for AI security, establish an effective early warning mechanism, apply agile governance and tiered and categorized management, and continuously improve risk management, control and settlement capacity.

States should require R&D entities to strengthen self-discipline, avoid premature use of technologies that may cause serious consequences, and ensure that AI is always under the control of humans. States should require R&D entities to strive for algorithm security and controllability throughout the AI R&D process, improve transparency, explainability and reliability and gradually make AI verifiable, regulatable, traceable, predictable and trustworthy and strive for better data quality during AI R&D, and improve the completeness, timeliness, consistency, normalization and accuracy of data. States should require R&D entities to fully consider diversified demands, avoid potential data and algorithms bias, and strive to achieve the universality, fairness and non-discrimination of AI systems.

States should prohibit using AI technologies and relevant applications which run counter to laws, regulations, ethics and standards, strengthen quality monitoring and evaluations on the use of AI products and services, and formulate emergency compensation measures. mechanisms and States should strengthen pre-use study and evaluations of AI products and services, promote institutionalized training on AI ethics, and ensure that relevant personnel acquire necessary professional expertise and skills. States should safeguard individual privacy and data security of Al products and services, strictly follow international or regional norms for handling of personal information, and oppose illegal collection and utilization of personal information.

#### 7. Digital public goods

The principle of national sovereignty should be applied in cyber and digital domain. States have jurisdiction over ICT infrastructures, resources and data as well as ICT activities within their borders, and have the right to formulate their own public policies and laws and regulations regarding the Internet, safeguarding the legitimate rights and interests of their citizens, enterprises and social organizations and other subjects in cyberspace.

Meanwhile, increasing the openness of digital products has positive implications for unlocking the potential of digital technologies and advancing the achievement of the SDGs, especially for low and middle income countries. On the basis of respecting the sovereignty, data security, legitimate rights and interests of citizens of other States and following the principle of voluntarism, States can discuss and gradually build consensus on the standards, scope, way of management and guidelines for the use of digital public goods. States should enhance the digitalization of public services, strengthen international cooperation in areas such as online education, and strengthen cooperation and sharing of data for monitoring and evaluation of the SDGs in order to promote their implementation more effectively.