网络主权：理论与实践（4.0版）

武汉大学

中国现代国际关系研究院

上海社会科学院

复旦大学

北京航空航天大学

中国社会科学院国家全球战略智库

清华大学

对外经济贸易大学

西南政法大学

北京理工大学

中国电子信息产业发展研究院

联合发起

纵观世界文明史，国家主权的含义因时而变、不断丰富。人类先后经历了农业革命、工业革命、信息革命，每一次产业技术革命，都给国家主权的内涵外延带来巨大而深刻的影响。农业时代，人类活动空间主要集中在陆地，国家主权的重点在于捍卫领土完整。工业时代，人类活动空间从陆地拓展到了海洋、天空，国家主权的范围也随之延伸扩展。进入信息时代，网络空间与人类活动的现实空间高度融合，成为了现代国家的新疆域、全球治理的新领域，网络主权由此而生。

主权国家是开展网络空间活动、维护网络空间秩序的关键行为体。《联合国宪章》确立的主权平等原则是当代国际关系的基本准则，覆盖国与国交往各个领域，其原则和精神也适用于网络空间。实践中，各国都将国家主权延伸适用于网络空间，但对在网络空间行使主权的理念和具体做法仍存在不同认识。为推动全球互联网治理朝着更加公正合理的方向迈进，构建网络空间命运共同体，国际社会应坚持以人类共同福祉为根本，秉持网络主权理念，平等协商、求同存异、积极实践。

《网络主权：理论与实践》系列文件一直致力于更好地凝聚共识，推动实践。相较于前三版的探索，4.0 版文件在既有逻辑框架的基础上承继理论探索与实践发展，进一步体

现出新变化与新需求，旨在及时反映当前全球网络空间发展的新形势、新变化，应对实践层面出现的新挑战。本版文件增加了“新形势下网络主权的突出挑战”等内容，邀请多国专家参与撰写“部分国家关于网络主权的主要实践”，对百年未有之大变局加速演进，尤其是新一轮科技革命和地缘政治变革迭加影响之下网络主权内涵与外延的持续拓展进行了梳理探讨。感谢英国谢菲尔德大学教授 Nicholas Tsagourias、俄罗斯圣彼得堡国际大学教授 Yana Leksyutina、印度尼赫鲁大学法学院教授 Swaran Singh、墨西哥阿纳瓦克大学教授 Ricardo Israel Robles Pelayo、土库曼斯坦 Ak Ussa 咨询公司首席营销官 Leonid Demidov、坦桑尼亚达累斯萨拉姆大学法学院教授 James Jesse、尼日利亚伊巴丹大学副教授 Ehizuelen Michael Mitchell Omoruyi 等为文件撰写做出的贡献。

网络主权是一个理论问题，更是一个实践问题，探索“永远在路上”。我们将以和而不同的开放心态，求同存异的务实做法，为推动网络空间走向更加和平、开放与发展的未来而努力。

目　录

一、网络主权的涵义.....1
二、行使网络主权的基本原则.....5
三、网络主权的主要体现.....6
四、网络主权的实践进程.....8
五、新形势下网络主权的突出挑战.....14
六、基于网络主权建立更具包容性的国际协作框架.....18
七、尊重网络主权，携手构建网络空间命运共同体.....20
附件：部分国家关于网络主权的主要实践.....23

一、网络主权的涵义

（一）网络主权的权利维度

网络主权是国家主权在网络空间的自然延伸，是一国基于国家主权对本国境内的网络设施、网络主体、网络行为及相关网络数据和信息等所享有的对内最高权和对外独立权。具体而言，主要包括以下权利：

1.独立权

主权国家有权自主选择网络发展道路、治理模式和公共政策，不受任何外来干涉。

2.平等权

按照《联合国宪章》的主权平等原则，主权国家有权平等参与网络空间国际治理，共同制定国际规则。

3.管辖权

立法规制权。主权国家为保障国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，有权对本国境内的网络设施、网络主体、网络行为及相关网络数据和信息等制定法律法规。

行政管理权。主权国家为维护良好的网络空间秩序，有权依法对本国境内的网络设施、网络主体、网络行为及相关网络数据和信息等加以管理。

司法管辖权。主权国家有权依法对本国境内的网络设施、网络主体、网络行为及相关网络数据和信息等进行司法

管辖。

主权国家有权基于公认的国际法原则和规则，对本国境外与本国具有真实充分联系的特定网络行为，以及与之相关的网络设施、网络主体、网络数据和信息等行使必要且合理的属人管辖权、属地管辖权和保护性管辖权等。为顺利实施此类管辖权，主权国家可以本着克制、礼让和对等的精神，寻求其他国家和地区的协助。

4.防卫权

主权国家有权开展本国的网络安全能力建设，并有权在《联合国宪章》框架下采取合法合理措施，维护本国在网络空间的正当权益不受外来侵犯。

（二）网络主权的义务维度

无论在物理世界还是网络空间，主权都意味着权利和义务的统一。各国在网络空间的互联互通和相互依存，更要求各国在享有网络主权所衍生权利的同时，应遵守国际法一般原则和基本规则，切实履行国际法所规定的相关义务。

1.不侵犯他国。各国未经许可不得进入另一国网络基础设施，或入侵另一国管辖范围内的网络系统，不得实施网络监控、窃密或破坏活动。

2.不干涉他国内政。各国不得干涉其他国家在网络空间享有的生存、安全与发展的权利，不得干涉其他国家维护其自身网络秩序、安全和发展的权利；不得支持纵容分裂势力

通过网络空间危害他国领土完整、国家安全和社会稳定。

3.审慎预防义务。各国不得蓄意允许其领土，或在政府控制下的领土或网络设施、网络数据和信息，被用于实施损害他国国家安全和利益的网络活动。

4.保障义务。各国有义务保障其管辖范围内相关网络主体的合法权益，也有义务在保障网络空间秩序、安全和发展的同时，促进网络空间开放与自由。

（三）网络主权的国际法属性

网络主权作为国家主权在网络空间的延伸，同样是一项具有法律约束力的原则和规则。各国可能对网络主权的概念有不同的界定，对侵犯网络主权的标准存在不同的理解，但这些差异并不影响网络主权作为一项独立原则和规则的法律地位。

如果一国未经许可侵犯他国基于国家主权对其境内的网络设施、网络主体、网络行为及相关网络数据和信息等享有的对内最高权和对外独立权，包括未经许可入侵他国领土或管辖范围内的网络系统，或对有关网络基础设施造成损害或破坏，或未经许可损害一国在网络空间对内对外的排他性主权权利，都违反了主权原则，构成国际不法行为。一项网络行动可能同时违反主权原则、不干涉内政原则以及禁止使用武力原则，需要在有关具体场景中进行个案分析。

（四）与网络主权相关的几个概念

基于主权原则在网络空间多元的适用场景和领域，国际社会各方近年来陆续提出“信息主权”“技术主权”“数据主权”“数字主权”等概念。

1.强调信息内容管理的“信息主权”。信息有广义与狭义之分，前者涵盖技术与内容等，如俄罗斯提出的“信息安全”。而在学界探讨的“信息主权”中，信息更多是狭义界定，主要是指利用信息通信技术与网络制造和传播的信息内容。“信息主权”的核心诉求体现为对信息内容的有效治理与规范。

2.聚焦重要技术自主能力的“技术主权”。2020 年 2 月，欧盟委员会接连发布三份重要战略文件，《塑造欧洲的数字未来》《人工智能白皮书》和《欧洲数据战略》。欧盟委员会主席乌尔苏拉·冯德莱恩称系列举措旨在重新夺回“技术主权”，重点强化欧盟在人工智能、大数据、5G 等前沿技术及应用的发展和规范方面的独立自主能力。

3.重视数据战略价值的“数据主权”。其要义在于大数据时代，数据的战略价值得到前所未有的重视。相关国家积极探索数据的有效治理，力图找到确保安全与促进发展的平衡点，例如 2020 年欧洲接连发布《欧洲数据战略》和《欧洲数据治理条例提案》等。

4.旨在提升“战略自治”的“数字主权”。2020 年 7 月欧洲议会发布的《欧洲数字主权》文件中，“数字主权”

被明确定义为“欧洲在数字世界独立行动的能力，应该从保护性机制和促进数字创新的防御性工具（包括与非欧盟公司合作）两方面来理解它”。这一概念是欧盟面对数字世界的竞争，为保持独立性、竞争力与领导力提出的，强调国家主导本国数字发展的能力。

上述概念的核心关切或侧重点有所不同，但又有所联系，相关实践探索在客观上丰富和拓展了网络主权的内涵与外延。

二、行使网络主权的基本原则

（一）平等原则

《联合国宪章》提出的主权平等原则，是各国行使网络主权时应遵循的首要原则。主权国家无论大小、强弱、贫富，在法律上是平等的，都有权平等参与网络空间国际事务，也有权受到他国的平等对待，更有义务平等对待他国。

（二）公正原则

各国应坚持网络空间的公平正义，推动互联网治理体系向公正合理的方向发展，使其反映世界大多数国家的意愿和利益，尤其是要维护好广大发展中国家的正当权益，确保网络空间的发展由各国人民共同掌握。各国不应滥用自身在网络领域的设施、技术、系统、数据优势地位，对他国行使网络主权进行干涉，或推行网络霸权、网络孤立等不公正行为。

（三）合作原则

网络空间具有全球性，任何国家都难以仅凭一己之力实现对网络空间的有效治理。基于《联合国宪章》所提倡的“善意合作”原则，各国应尊重他国的国际法主体地位，秉持共商、共建、共享的理念，坚持多边参与、多方参与，打造多领域、多层次、全方位的治理体系，致力于维护网络空间的安全与发展。

（四）和平原则

网络空间互联互通，各国利益深度交融。各国应遵守《联合国宪章》的宗旨与原则，和平利用互联网，以和平方式解决网络空间争端。各国应采取有效措施，防范利用信息通信技术从事破坏和平的行动，防止网络空间军备竞赛，预防并打击网络犯罪与网络恐怖主义，维护网络空间的和平与安全。

（五）法治原则

各国应推进网络空间国际治理法治化，共同维护国际法的权威性，反对双重标准。各国应完善国内立法，依法行使网络主权，对内保护本国公民、法人和其他组织在网络空间的合法权利，对外尊重他国网络主权，遵守国际规则和国际法原则，不得利用网络干涉他国内政，不得从事、纵容或支持损害他国国家安全和利益的网络活动。

三、网络主权的主要体现

从网络空间架构的角度来看国家主权在网络空间中的

体现，可以将网络空间划分为物理层、逻辑层、应用层和社会层，国家主权在各分层中均有所体现。

（一）在物理层的体现。包括：国家对于其境内的物理基础设施和基础电信服务可行使管辖权，并有权为维护基础设施安全而依法采取必要措施；国家有权参与国际网络基础设施的管理和国际合作。

（二）在逻辑层的体现。包括：国家可以在不违反其承担的国际法义务的前提下，在维护互联网兼容性的同时，独立地制定或采用相关的技术法规或标准。

（三）在应用层的体现。包括：国家对应用软件的开发和运营依法管理，保护合法网络数据与信息，特别是涉及国家安全的网络数据与信息不被窃取或破坏；国家依法对境内网络信息传播实施保护、管理与指导，限制侵犯合法权利或损害公共秩序的信息传播；国家遏制境外组织在本国境内捏造、歪曲事实，散播危害国家安全、公共秩序的网络信息内容；国家参与数据跨境流动、信息治理的国际协调与合作。

（四）在社会层的体现。包括：国家自主管理本国境内网络用户和互联网平台的行为，培育与网络发展相适应的社会环境；维护本国独立自主的互联网治理体制，平等参与完善互联网治理模式的国际合作；有权平等参与全球数字经济发展建设。

上述体现反映了网络主权活动的系统性与完整性，尊重

网络主权有利于促进网络空间的有序合作，维护网络空间的和谐稳定，推动网络空间的可持续发展。同时网络主权的行使应当遵循公认的国际法原则和规则，尊重网络空间“互联、互通、互动”的特性，防止互联网“碎片化”。各国不应以行使网络主权为名，将网络安全问题政治化，违反国际通行经贸规则和市场化原则，干扰正常网络基础设施及服务领域项目合作，对他国实施网络孤立等；不应凭借自身技术、经济与政治的优势，不公平分配或封锁重要网络资源，危害全球供应链安全。

四、网络主权的实践进程

（一）许多重要的国际文件已经确认了国家主权原则适用于网络空间

2003 年，联合国信息社会世界峰会通过的《日内瓦原则宣言》就提出“互联网公共政策的决策权是各国的主权”；该峰会 2005 年通过的《突尼斯议程》强调各国政府在峰会进程中的关键作用和责任。

2011 年和 2015 年，中俄等国在《信息安全国际行为准则》中，提出“重申与互联网有关的公共政策问题的决策权是各国的主权”。

2013 年、2015 年和 2021 年，联合国信息安全政府专家组在其报告中指出，“国家主权和在主权基础上衍生的国际规范及原则适用于国家进行的信息通信技术活动”“国家主

权原则是增强国家运用信息通信技术安全性的根基”“国际合作、对话以及对所有国家主权的应有尊重至关重要”。

2015 年，二十国集团领导人《安塔利亚峰会公报》中指出，“确认国际法，特别是《联合国宪章》，适用于国家行为和信息通信技术运用，并承诺所有国家应当遵守进一步确认自愿和非约束性的在使用信息通信技术方面的负责任国家行为准则”。

2016 年，金砖国家领导人《果阿宣言》重申，“在公认的包括《联合国宪章》在内的国际法原则的基础上，通过国际和地区合作，使用和开发信息通信技术。这些原则包括政治独立、领土完整、国家主权平等、以和平手段解决争端、不干涉别国内政、尊重人权和基本自由及隐私等。这对于维护和平、安全与开放的网络空间至关重要”。

2019 年，世界互联网大会发布《携手构建网络空间命运共同体》概念文件，强调“网络主权是国家主权在网络空间的自然延伸，应尊重各国自主选择发展道路、治理模式和平等参与网络空间国际治理的权利”。

2020 年，《中国-东盟关于建立数字经济合作伙伴关系的倡议》指出，“在考虑各国法律与社会实际基础上，充分尊重网络主权”“推动建立多边、民主、透明的全球网络空间命运共同体”。

2020 年，世界互联网大会发布《携手构建网络空间命

运共同体行动倡议》，再次重申了尊重网络主权的重要性。

2021 年，中非互联网发展与合作论坛发起《中非携手构建网络空间命运共同体倡议》，提出“在尊重各国网络主权、尊重各国网络政策的前提下，探索以可接受的方式扩大互联网接入和连接，让更多发展中国家和人民共享互联网带来的发展机遇”。

2022、2023 年，上海合作组织《撒马尔罕宣言》、《新德里宣言》提出：“成员国强调联合国在应对信息空间威胁方面的关键作用，主张在尊重主权和不干涉他国内政基础上，构建安全、公正、开放的信息空间。成员国认为，确保各国在管理互联网方面享有平等权利，并拥有网络主权十分重要”。

（二）相关国家在有关国际法适用于网络空间的立场文件中对网络主权问题加以宣示

近年来，一些国家陆续发表了有关国际法适用于网络空间的立场文件，就国家主权原则在网络空间的适用问题宣示了本国的立场主张。

在确认国家主权原则适用于网络空间方面，2020 年新西兰《适用于网络空间国家行动的国际法》文件表示，“领土主权作为一项独立的国际法规则适用于网络空间”。同年芬兰《关于国际法与网络空间的国家立场》主张，“主权作为一项国际法首要规则”完全适用于网络空间。2020 年伊

朗武装力量总参谋部发布的《关于国际法适用于网络空间的宣言》主张，“国家的领土主权和管辖权也延伸到网络空间的所有方面。”2022 年波兰《关于国际法在网络空间的适用立场文件》同样主张“主权原则适用于网络空间”。

在肯定网络主权原则构成有约束力的国际法原则和规则方面，2019 年荷兰《现有国际法有关规则在网络空间的适用》文件表示，主权构成一项独立的、有约束力的国际法规则，“各国有义务尊重其他国家的主权，并避免从事构成侵犯其他国家主权的活动”。2021 年德国《国际法在网络空间的适用》文件明确，“可归因于国家的侵犯另一国主权的网络行动违反国际法，国家主权本身构成一项法律规范”。同年，挪威、意大利在其立场文件中表示，主权不仅是一项原则，也是“国际法的一项初级规则”。2021 年，中国在向联合国信息与安全开放式工作组提交的关于网络主权的立场文件中主张，“网络主权是一项具有法律约束力的原则和规则”。

在确定何种行为构成对他国网络主权的侵犯方面，2019 年法国《适用于网络空间行动的国际法》文件指出，“他国未经授权进入法国系统的行为或任何通过数字载体对法国领土造成影响的行为，至少可构成对主权的侵犯”。2020 年伊朗武装力量总参谋部发布的《关于国际法适用于网络空间的宣言》强调，“任何对网络空间的利用，如果涉及对另

一国控制下的官方或私人网络系统的非法侵入，可能构成对目标国主权的侵犯”。2021 年俄罗斯《国家安全战略》指出，“利用信息通信技术干涉他国内政、破坏国家主权和领土完整的情况越来越多，这对国际和平与安全构成威胁”。同年，挪威在立场文件中声明：“通过网络手段在另一国领土上造成物理损害、导致网络基础设施功能丧失，或者干扰或篡夺他国政府固有职能的网络行动，可能构成对主权的侵犯”。巴西在立场文件中表示，“对电信的拦截，无论是否被认为已跨过干涉另一国内政的门槛，都将被视为国际不法行为，因为它们侵犯了国家主权。同样，针对另一国境内的信息系统或造成域外影响的网络行动也可能构成对主权的侵犯”。

（三）世界各国还纷纷通过立法、行政、司法等实践活动行使网络主权

在倡导和践行网络主权原则方面，中国在 2015 年第二届世界互联网大会上提出，尊重网络主权是推进全球互联网治理体系变革的一项重要原则；2016 年通过《网络安全法》，将“维护网络空间主权”作为网络空间立法的根本宗旨；2016 年发布《国家网络空间安全战略》，提出“国家主权拓展延伸到网络空间”，并将网络空间主权作为国家主权的重要组成部分；2017 年发布《网络空间国际合作战略》，将主权原则列为网络空间国际合作的基本原则之一，并将“维护主

权与安全”作为参与网络空间国际合作的首要战略目标；2021 年通过《数据安全法》，指出“维护国家主权、安全和发展利益”是立法的主要目的之一。中国还在联合国信息安全政府专家组和开放式工作组、亚非法律协商组织等多边平台明确主张主权原则适用于网络空间。

在探索互联网发展道路和网络管理模式方面，越南 2018 年出台《网络安全法》明确将“相互尊重独立、主权、领土完整、互不干涉内政、平等互利”作为网络安全合作的基本原则，并详细列举了各种网络禁止行为，包括歪曲历史、破坏民族团结、触犯宗教等侵犯国家主权、利益、安全的行为。欧盟 2020 年 2 月提出“技术主权”，强化欧盟对网络空间的技术、规则和价值的控制力和主导权。

在保护本国网络免受威胁、干扰、攻击和破坏方面，俄罗斯 2019 年 5 月出台《稳定俄罗斯网络法案》，旨在确保俄罗斯互联网资源的自主性与可靠性，在无法连接国外服务器情况下仍能保障俄罗斯网络正常运行。巴基斯坦 2021 年首次制定《国家网络安全政策》，确认对巴基斯坦关键信息基础设施的网络攻击“可被视为对国家主权的侵犯，将据此采取适当的应对措施”。

在保障本国公民在网络空间权益和数字经济发展方面，欧盟 2018 年 5 月实施《通用数据保护条例》，对个人数据的跨境流动予以严格管制，并通过个人数据处理活动的域外

管辖权拓展其主权边界。欧盟2021年发布《2030数字指南针：欧洲数字十年之路》，旨在引领欧盟构建可持续的数字化社会，加强欧盟的数字主权，以确保欧盟成为世界上数字经济最发达的地区之一。法国2021年发布《网络安全国家战略》，提出要在未来5年内使法国掌握维护网络主权的技术，促进网络安全产业的发展。

五、新形势下网络主权面临的突出挑战及其应对

当前，世界之变、时代之变、历史之变正以前所未有的方式展开，以大数据、人工智能为代表的新一轮科技革命和产业变革深入发展，国际力量对比深刻调整。个别国家搞“小圈子”“脱钩断链”制造网络空间的分裂与对抗，发展进攻性网络军事力量，扩散进攻性网络技术，公然对他国开展进攻性网络行动，将关键基础设施列入战时网络攻击目标。各国在网络空间的主权、安全和发展利益面临着前所未有的挑战。

（一）关于人工智能

近年来，人工智能技术取得许多突破性进展，被广泛应用于工业、医疗、交通、信息内容等领域，给人类带来巨大机遇，也给网络主权带来许多新挑战。人工智能技术的误用和滥用，将导致虚假信息的大规模扩散，侵害公民合法权益，给国家维护公共秩序带来挑战；各国关于人工智能的技术标准和监管政策不一致，易形成对人工智能产品和服务的贸易

壁垒，阻碍各国数字经济发展合作。

人工智能的研发和使用具有国际性，关乎全人类的未来。各国应当坚持“以人为本”与“科技向善”的理念，推动建立普遍参与的国际机制，形成具有广泛共识的治理框架和标准规范，确保人工智能安全、可靠、可控、公平，更好赋能全球可持续发展，增进全人类共同福祉。各国应在尊重国家主权的基础之上加强信息交流和科技合作，促进人工智能的和平利用，共同应对人工智能带来的风险挑战，共同反对利用人工智能从事危害他国主权和安全的行为。

（二）关于数据治理

数据治理事关国家安全、经济安全、社会稳定和个人权益保护。个别国家基于技术优势通过数据手段实施危害他国网络安全和国家安全的行为，加剧网络空间的对抗。个别国家滥施数据治理“长臂管辖”和跨国数据监控，严重侵害他国网络主权。滥用技术垄断和单边强制措施损害全球数字发展的公平性、有效性和普惠性，限制发展中国家的数字发展权，削弱其行使和维护网络主权的能力。

面对这些挑战，各国应尊重网络主权，尊重各国司法管辖权和行政管理权，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。尊重各国根据自身国情自主选择数据治理路径的权利，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。各国应以事实为依据全面公正客观看待数据安全问题，促进数据依法有序自由流动。各国应加强数据安全合作，推动数字技术转移和能力建设，弥合数字鸿沟，支持向发展中国家提供能力建设援助。国际社会应以联合国为主导，探讨制定各方普遍接受的全球可互操作的共同规则，防止全球数据治理规则分裂和碎片化。

（三）关于卫星互联网

卫星互联网将人类活动的两大前沿领域——外层空间和网络空间紧密联系在一起，给网络主权带来新挑战：如何公平合理地分配无线电频率和卫星轨道资源；卫星互联网可能绕开地面国家监管，对他国网络主权的行使构成挑战；非法入侵网络系统可能导致卫星被操纵、功能丧失或被毁损，影响外空安全；卫星受到破坏，可能导致基于卫星构建的网络系统受到破坏，影响网络空间安全。

各国应坚持和平利用外层空间的原则，坚持《国际电信联盟组织法》所确立的合理、有效、经济和公平使用无线电频率和卫星轨道资源的原则，在尊重各国国家主权、平等参与、充分协商的基础之上，就卫星互联网的建设、运营和监管问题形成国际共识性规范。各国应加强国际合作，提高外层空间危机管控和综合治理效能，保障外层空间的长期可持续发展，维护国家网络主权和网络空间安全。

（四）关于“长臂管辖”

近年来，“长臂管辖”已经延伸至网络空间，构成对网络主权的重大挑战。一国对外行使“长臂管辖”往往会与他国的属地管辖或属人管辖发生冲突。在网络空间，个别国家对“长臂管辖”的频繁使用已构成一种网络霸权行为，极易威胁其他国家网络主权。滥用“长臂管辖”违反国际法上的主权平等原则，威胁安全稳定的网络空间秩序，破坏正常的国际商业贸易秩序和数字经济合作。

各国应秉承《联合国宪章》宗旨与原则，尤其是主权平等原则，抵制滥用“长臂管辖”的国家行为。各国应秉承网络空间命运共同体理念，加强网络空间管辖权的国际协调。个别国家应摒弃“长臂管辖”，切实履行不侵犯他国主权，不干涉他国内政的国际责任。

（五）关于“脱钩断链”

个别国家在经贸与科技领域不断推动“脱钩断链”，通过各种手段拉拢甚至强迫相关国家“选边站队”，干扰破坏市场规则和国际经贸秩序，对全球产业链供应链稳定以及世界经济发展带来消极影响。这种行为侵犯他国在产业发展与科技合作等领域的自主决定权，破坏《联合国宪章》规定的主权平等原则，加剧网络空间对抗，给网络空间的和平发展与合作带来严重威胁。

各国应当坚持合作共赢、开放包容的理念，旗帜鲜明反对各种“脱钩断链”行径。各国要充分讨论，不断凝聚“脱

钩断链”有害全球公共利益的共识，倡导有利于产业和市场发展的政策环境，重视发挥产业界力量，积极推动构建符合产业发展实际的供应链。各国应鼓励产、学、研多方合作，多渠道化解或对冲“脱钩断链”的负面影响。

六、基于网络主权建立更具包容性的国际协作框架

尊重网络主权，是在网络空间尊重《联合国宪章》所确立宗旨与原则的表现，是维护网络空间和平安全的基础与前提，也是维护网络空间战略稳定的必要路径。倡导和实践网络主权，并不意味着各国在网络空间各行其是、以邻为壑。基于网络主权建立更具包容性的国际协作框架，旨在尊重各国主权的基础上，平衡各国主权权利与义务之间的关系，有利于各方享受数字时代的发展红利，进而维护网络空间的和平、安全与发展。

（一）以理念认同为基础，推动和巩固网络主权国际共识的形成。各国行使网络主权的实践将长期存在多样性，但国家主权原则适用于网络空间，已在许多重要的国际文件中得到确认。各国应摒弃成见，正视网络空间休戚与共的事实，维护以联合国为核心的国际体系和以国际法为基础的国际秩序，承认网络主权是客观存在的，求同存异，相互尊重，相互谅解，积极互动，避免相互掣肘，鼓励开展全球、区域、多边、双边与多方等各层级的合作与对话，共同促成网络主权的国际共识，增进国家间在网络空间的互信，共同推进实

现和平、发展、公平、正义、民主、自由的全人类共同价值。

（二）以制度构建为保障，在网络主权的基础上，积极构建有助于包容性国际协作的网络空间国际规则和制度。各国除应增加内部制度构建外，还应完善国际制度协作，积极参与网络空间的国际机制构建。各国应以联合国为主渠道，支持联合国在网络空间全球治理中发挥核心作用，以《联合国宪章》宗旨和原则为基础，积极推动构建网络空间基础设施和行为主体合理权利的安全保障机制、数字技术和数据信息等交流共享与合作机制、网络空间恶意活动的风险防范机制、网络犯罪的打击惩治机制、解决网络空间争端的磋商与调停机制等制度规范。各国应秉承坦诚和善意，尽可能促成网络空间国际制度和国际准则的订立，并采取一切必要措施保证相关准则或制度的严格执行，以实现国际规则的长效约束力，从而推动网络主权权利的平等实现，推动国际社会对网络主权义务的共同遵守，为人类共同利益推进网络空间合作，避免霸权主义、零和思维、冷战思维等对网络空间和平发展带来不利影响，促进网络主权的相互协作和良性发展。

（三）以合作行动为途径，在行动实践中积极推进各国网络主权的协调发展与合作。网络主权存在于网络空间命运共同体中，网络主权的有效保障有赖于国际社会在网络主权基础上的合作与努力，即发展共同推进，采取更加积极、

包容、协调、普惠的政策，加快全球信息基础设施建设，推动数字经济创新发展，提升公共服务水平；安全共同维护，倡导开放合作的网络安全理念，坚持安全与发展并重，积极参与联合国网络安全进程，共同维护网络空间和平与安全；治理共同参与，坚持多边参与、多方参与，加强对话协商，推动构建更加公正合理的全球互联网治理体系；成果共同分享，坚持以人为本、科技向善，缩小数字鸿沟，实现共同繁荣。通过共同合作和行动实践，共同推动网络主权的“善意合作”，从而实现网络空间的共享、共治和共赢。

七、尊重网络主权，携手构建网络空间命运共同体

网络主权原则是习近平主席关于推进全球互联网治理体系变革的“四项原则”和构建网络空间命运共同体的“五点主张”中的首要原则。倡导与实践网络主权，绝不意味着封闭或割裂网络空间，而是要在国家主权基础上构建公正合理的网络空间国际秩序，共同构建网络空间命运共同体。构建网络空间命运共同体是维护网络主权的内在动力和远景目标，将网络空间建设成造福全人类的发展共同体、安全共同体、责任共同体和利益共同体，必须在尊重各国主权的基础上实现。

（一）构建网络空间命运共同体必须坚持网络主权的原则。构建网络空间命运共同体需要各国共同努力来应对风险和挑战。只有首先明确和界定国家在网络空间的主权，

在尊重各国网络主权的基础上，才能携手构建网络空间命运共同体。只有确保各国拥有自主选择网络发展道路、治理模式和公共政策的独立权，参与网络空间国际治理和规则制定的平等权，通过立法、行政和司法手段对其网络进行管理的管辖权，抵御网络空间外来风险和应对外部侵犯的防卫权，才有可能通过平等协商和合作，在国家之间建立有效的对话与协商机制，携手构建网络空间命运共同体。

（二）网络主权需要通过构建网络空间命运共同体来加以更好的维护和保障。互联网的飞速发展为人类文明进步创造了前所未有的机遇，但发展不平衡、规则不健全、秩序不合理等问题也更加突出；霸权主义和强权政治以及保护主义和单边主义在网络空间持续存在。侵犯隐私、侵犯知识产权、散播虚假信息、网络诈骗、网络恐怖主义等违法犯罪活动已成为全球公害。在网络空间，各国命运相连，休戚与共，有效应对网络空间安全与发展的威胁有赖于各国共同参与、协同合作，唯有通过构建网络空间命运共同体，才能有效维护网络主权。

然而，各国国家利益存在差异，有时甚至相互冲突，在维护本国利益与提供国际公共产品之间始终保持平衡并不容易。面对跨境数据流动、虚假信息、供应链安全等新问题，日益加剧的地缘政治紧张局势使得相关国际规则和规范的谈判进程步履维艰。只有遵循尊重网络主权、维护和平安全、

促进开放合作、构建良好秩序的基本原则，才能找到各国国家利益的最大公约数。

人类社会再次站在历史的十字路口，各国在网络空间的主权、安全和发展利益正面临着前所未有的挑战，网络主权的实践没有止境，理论创新也没有止境，凸显了携手构建网络空间命运共同体的长期性和艰巨性。我们呼吁各国共同致力于维护全球互联网互联互通，在网络空间国际合作与交流中共同坚持和共同发展网络主权原则，推进数字经济高质量发展，构筑高水平网络安全，推动数字领域高水平开放，打造包容共生的数字文明。我们呼吁国际社会在联合国框架下共同努力，秉持平等协商、求同存异、互利共赢的原则，加强沟通、协调立场，在尊重和维护国家网络主权的基础上，制定普遍接受的网络空间国际规则，凝聚广泛共识，贡献智慧力量，共同构建和平、安全、开放、合作、有序的网络空间。

附件

部分国家关于网络主权的主要实践

近年来，越来越多的国家，特别是发展中国家认同并积极践行网络主权原则，维护国家利益，保障国家安全，增进国民福祉，促进国际合作，携手构建网络空间命运共同体，充分体现了网络主权原则的理论价值和实践意义。

（一）中国

近年来，中国政府相继出台多项政策法规，坚定维护本国的网络主权，进一步完善以《网络安全法》《数据安全法》《个人信息保护法》为核心的法规体系。陆续发布或修订《出口管制法》（2020）、《关键信息基础设施安全保护条例》（2021）、《网络安全审查办法》（2022）、《数据出境安全评估办法》（2022）、《个人信息出境标准合同办法》（2023）等法律法规规章，分别从网络技术出口管制、关键信息基础设施保护、网络安全维护以及数据和个人信息安全出境等层面维护国家网络主权。

在网络主权理念践行方面，一是持续在国际社会倡导网络主权理念。2021 年，中国向联合国信息安全开放式工作组提交关于网络空间国际规则的立场文件以及关于网络主权的立场文件，均确认“国家主权原则应适用于网络空间”，并从权利和义务两个维度阐述网络主权的涵义。二是积极在网络空间国际合作中践行网络主权理念。先后发布《全球数

据安全倡议》（2020）、《中国-东盟关于建立数字经济合作伙伴关系的倡议》（2020）和《中非携手构建网络空间命运共同体倡议》（2021）等倡议，并于 2022 年发布《携手构建网络空间命运共同体》白皮书，承诺在相互尊重网络主权的基础上，共同维护网络安全，推进网络发展；在《中俄关于深化新时代全面战略协作伙伴关系的联合声明》(2023）中提出，在确保各国互联网治理主权和安全的前提下打造多边公平透明的全球互联网治理体系。三是中国在连续多年举办世界互联网大会基础上，于 2022 年成立世界互联网大会国际组织，更好地助力各国平等参与网络空间国际治理，维护自身网络主权与发展利益，共建网络空间命运共同体。

（二）俄罗斯

俄罗斯提出“信息主权”、“数字主权”、“信息通信技术主权”等术语，意在强调国家不仅应确保对技术性基础设施的控制，而且还应控制信息的跨境流动。在国家层面，俄罗斯已发布两份与确保信息安全直接相关的战略文件，分别为 2016 年修订发布的《俄罗斯联邦信息安全学说》和 2021 年发布的《俄罗斯联邦国际信息安全领域国家政策框架》，使用了“信息主权/信息空间的主权”和“信息与通信技术主权”等类似术语。

2019 年 11 月，俄罗斯施行《稳定俄罗斯网络法案》，即 2019 年 5 月第 90-FZ 号的《<俄罗斯联邦通信法>及<俄

罗斯联邦关于信息、信息技术和信息保护法>修正案》，授权国家权力机关对国境内互联网实施集中管理,包括允许强制安装应对威胁的技术设备;在出现威胁时对电信网络进行集中管理，并对跨越俄罗斯边境的通讯线路建立控制机制;实施俄罗斯国家域名系统等。

2022 年，俄罗斯开始更新其在维护信息主权方面的政策，例如，一些西方信息技术平台在俄罗斯的活动被封禁，是俄罗斯加强其信息主权的新动作。

（三）印度

在新冠疫情大流行期间，印度的教育、医疗、农业、研究等各领域的数字化程度均有普遍提高,国家对网络空间的主权意识不断增强。莫迪总理提出打造“智慧城市”和“数字印度”的战略政策，可以被视作运用网络主权保障本国国民权益的例证。

印度在 2000 年颁布了保护网络空间的第一部全面性立法——《信息技术法》，并在 2008 年对其进行大幅修订。该法为印度网络空间的商业利用营造了有利的法律环境。为解决数据安全问题，印度在 2019 年的《个人数据保护法（草案）》中，试图规定并推动数据本地化要求，同时也尝试规定私营网络公司有配合调查机构共享数据的义务。印度还在 2000 年的《信息技术法》授权印度可在领土范围外行使管辖权,但由于与外国执法机构的合作存在严重困难以及相关

法律框架的不兼容，印度很少将域外管辖权付诸实践。

目前，印度国内仍在就网络主权进行持续辩论，预计将在《2023 网络安全战略》进一步澄清印度在网络空间主权原则方面所持有的立场、政策、法律和实践。

（四）墨西哥

墨西哥的国家网络安全政策由一系列指南和战略组成，旨在确保并保护国家关键基础设施、信息和系统的安全。2017 年，墨西哥推出第一个网络安全框架《国家网络安全战略》，由联邦政府和国家安全局共同制定。该战略由八大举措构成，目的在于加强社会、经济、政治等各领域的网络安全水平。维护“国家安全”是战略所列五大目标的重中之重，要求“提升网络能力，以防止网络空间出现可能侵犯国家主权、领土完整、政治独立或损及国家发展与利益的风险与威胁”。

墨西哥尚未出台网络主权专门性法律，但在一些法律或规则中对在线安全和隐私作出了规定。例如，《保护私人持有的个人数据联邦法》规定了个人数据持有者和个人数据处理者的权利和义务，包括如何在线收集和处理数据；《联邦电信和广播法》确立了有关互联网接入、网络中立性和保护在线用户权利等方面的基础性规则；《联邦刑法》规定了对非法进入计算机系统和网络、干扰计算机系统以及传播计算机病毒等网络犯罪的刑事处罚。

（五）土库曼斯坦

土库曼斯坦坚持独立选择自身网络发展道路、网络治理模式和有关互联网政策，并努力确保此种权利不受任何外部干预。2018 年 11 月，土库曼斯坦发布《2019-2025 数字经济发展构想》，旨在推进国家治理能力现代化，提升政府行政效能，同时使土库曼斯坦的经济发展引擎多元化。2019 年 9 月成立国家网络安全局（SCS）。2021 年 2 月通过《2021-2025 土库曼斯坦国家数字经济发展规划纲要》。土库曼斯坦还通过了《2022-2025 国家网络安全计划》。

土库曼斯坦主张每一个国家都拥有独立选择自身网络发展道路的权利，强调本国的网络治理模式和互联网政策不应受任何外部干涉；主张尊重各国网络主权，提倡各国应在国际舞台上以平等为基础参与网络空间全球治理；欢迎各国在监测和应对国际信息安全领域新出现的威胁上进行合作。

（六）坦桑尼亚

网络主权和安全是坦桑尼亚网络空间治理的重要领域。坦桑尼亚将信息通信技术视为经济发展的重要推动力，力图通过推进关键基础设施建设以维护网络安全。2022 年，坦桑尼亚决定开展“数字坦桑尼亚项目”，计划投入 1.5 亿美元，通过完善法律体系、培养数字经济专家、建设国家数据中心等加快推动数字经济建设。

以立法强化网络管理是坦桑尼亚维护网络主权的重要

方式。坦桑尼亚先后出台《国家安全机构法》、《个人数据保护法》、《网络犯罪和计算机犯罪法》等法律。2015 年通过《电子签名法》，详细规定电子签名的认证程序和使用方法，为网络交易提供法律认定和保护。2017 年实施《数据安全和防范网络犯罪方案》，对各行业数据保护提出标准和要求。同年，还成立电子政府安全运营中心，对网络安全进行国家级别的监管。2020 年通过《电子和邮件通信（在线内容管理）规定》，进一步加强社交网络监管力度。2021 年，推出《网络反恐治理计划》，在加强数据安全治理及打击网络犯罪和网络恐怖主义上发挥重要作用。坦桑尼亚坚持团结互助的外交理念，积极同其他国家和国际组织合作，共同维护网络安全，进一步彰显其自身的网络主权。

（七）尼日利亚

尼日利亚于 2020 年将电信设备指定为国家关键基础设施，并在《2021-2025 年国家发展计划：第一卷》中对数字经济发展做出详尽规划，计划到 2025 年将 400 亿美元的私人资本投资引入数字基础设施建设。尼日利亚《国家数字经济政策和战略（2020-2030）》提出数字扫盲与技能培训、本土内容开发和利用等多条支柱举措，积极维护网络空间安全。尼日利亚还颁布一系列法律法规，包括：2015 年《尼日利亚网络犯罪(禁止和预防)法》，建立起了一个禁止、预防、侦查、起诉和惩罚网络犯罪的全面法律框架。2019 年

颁布《尼日利亚云计算政策》、《尼日利亚数据保护条例》等政策法规，赋予尼日利亚以更广泛地控制其数据的收集、共享和使用的权利。2023 年通过的《数据保护法案》则是一项最新的立法努力。

2019 年，尼日利亚宣布加强对社交媒体的监管，以打击假新闻和虚假信息。2021 年 6 月，推特删除时任总统布哈里关于国内东南部动乱的推文，并冻结其账户 12 小时。尼日利亚政府则宣布暂停推特在本国的运营，至 2022 年初方解除有关禁令并要求国家广播委员会立即开始对尼日利亚所有从事社交媒体业务的应用程序进行审核并发放执照。2022 年，尼日利亚采取成立数据保护局和国家共享服务中心等多项措施，保护数据和网络空间的安全。

Sovereignty in Cyberspace: Theory and Practice (Version 4.0)

Jointly Launched by

Wuhan University

China Institute of Contemporary International Relations

Shanghai Academy of Social Sciences

Fudan University

Beihang University

National Institute for Global Strategy, Chinese Academy of Social Sciences

Tsinghua University

University of International Business and Economics

Southwest University of Political Science & Law

Beijing Institute of Technology

China Center for Information Industry Development

Throughout the history of world civilization, the meaning of national sovereignty has changed and been enriched over time. Humanity has successively undergone agricultural, industrial, and information revolutions, which have had enormous and profound impacts on the connotation and denotation of national sovereignty. In the agricultural age, human activity was mainly confined to land, so the focus of national sovereignty was on protecting territorial integrity. In the industrial age, human activity extended from land to the sea and sky. The scope of national sovereignty expanded accordingly. Highly integrated with the physical space of human activity in the information age, cyberspace has become a new frontier for modern states and a new domain of global governance. It is from this that sovereignty in cyberspace has emerged.

Sovereign states are key actors in carrying out activities and maintaining order in cyberspace. The principle of sovereign equality enshrined in the Charter of the United Nations is a basic norm governing contemporary international relations. Covering all aspects of state-to-state relations, its principle and spirit also apply to cyberspace. In practice, all countries have extended national sovereignty to cyberspace, but different understandings exist around the ideas and practices for exercising it. To facilitate more just and equitable global Internet governance and build a community with a shared future in cyberspace, the international community should, with the common well-being of humanity in mind, follow and practice the notion of sovereignty in cyberspace in line with the principles of equal consultation and seeking common ground while setting aside differences.

The Sovereignty in Cyberspace: Theory and Practice paper series have been dedicated to building consensus and promoting practice. Compared to the previous three versions, Version 4.0

takes further steps in the theoretical exploration and practical development on the basis of the existing logical framework, and reflects new changes and new demands. It aims to promptly present the latest global developments in cyberspace, and respond to new challenges at the practical level. "Prominent challenges and solutions for sovereignty in cyberspace in the new circumstances" are newly added into the paper. Experts from multiple countries were invited to contribute under "Main practices of some countries regarding sovereignty in cyberspace". Explorations are made in the continuous expansion of the connotation and denotation of sovereignty in cyberspace amid the global transformations unseen in a century, especially the new round of technological revolution and geopolitical changes. We would like to express our thanks to Professor Nicholas Tsagourias from the University of Sheffield in the UK, Professor Yana Leksyutina from St. Petersburg State University in Russia, Professor Swaran Singh from the Law School of Jawaharlal Nehru University in India, Professor Ricardo Israel Robles Pelayo from Universidad Anáhuac México, Mr. Leonid Demidov, Chief Marketing Officer of Ak Ussa Consulting in Turkmenistan, Professor James Jesse from the Law School of the University of Dar es Salaam in Tanzania, Associate Professor Ehizuelen Michael Mitchell Omoruyi from the University of Ibadan in Nigeria, and others for their contributions to the writing of the report.

Sovereignty in cyberspace is a theoretical issue, and, more importantly, a practical one, which requires continuous study. In the principle of embracing harmony without uniformity and seeking common ground while reserving differences, we will work for peace, openness, and development of cyberspace with an open mind and a pragmatic approach.

Contents

The Concept of Sovereignty in Cyberspace 1

Fundamental Principles of Sovereignty in Cyberspace 5

Key Manifestations of Sovereignty in Cyberspace 7

Sovereignty in Cyberspace in Practice 9

Prominent Challenges and Solutions for Sovereignty in Cyberspace in the New Circumstances 16

Building a More Inclusive International Cooperation Framework Based on Sovereignty in Cyberspace 21

Respecting Sovereignty in Cyberspace and Jointly Building a Community with a Shared Future in Cyberspace 24

Annex: Main Practices of Some Countries Regarding Sovereignty in Cyberspace 28

The Concept of Sovereignty in Cyberspace

I. Rights

Sovereignty in cyberspace is the extension of national sovereignty to cyberspace. It is the internal supremacy and external independence that a state enjoys, on the basis of its national sovereignty, over cyber infrastructure, entities, behavior as well as relevant data and information in its territory. Specifically speaking, it primarily includes the following rights.

● Independence. A sovereign state has the right to independently choose its own path of cyber development, model of cyber governance, and Internet public policies, free from any external interference.

● Equality. In line with the principle of sovereign equality enshrined in the UN Charter, a sovereign state has the right to participate in global governance in cyberspace on an equal footing and jointly formulate international rules.

● Jurisdiction

• Legislative Jurisdiction. A sovereign state has the right to enact legislation to regulate cyber infrastructure, entities, behavior as well as relevant data and information in its territory, in order to protect its national security, public interests, and the legal rights and interests of its citizens, legal persons, and other organizations.

• Administrative Jurisdiction. A sovereign state has the right to administer cyber infrastructure, entities, behavior as well as relevant data and information in its territory according to law, so as to maintain good order in cyberspace.

• Judicial Jurisdiction. A sovereign state has the right to exercise judicial jurisdiction over cyber infrastructure, entities, behavior as well as relevant data and information in its territory

according to law.

A sovereign state has the right to exercise, in accordance with the universally recognized principles and rules of international law, necessary and reasonable personal, protective and universal jurisdiction over specific cyber activities outside its territory that have genuine and substantial connection to the State as well as over relevant cyber facilities, entities, data and information. In order to exercise its jurisdiction, a State may seek assistance from other countries and regions in the spirit of self-restraint, comity and reciprocity.

• Cyber-defense. A sovereign state has the right to conduct capacity building on cyber security and adopt lawful and reasonable measures under the framework of the UN Charter to protect its legitimate rights and interests in cyberspace from external infringement.

II. Obligations

Whether in the physical world or cyberspace, sovereignty incorporates both rights and obligations. The connectivity and interdependence among countries in cyberspace all the more requires countries to respect the basic norms and general principles of international law and earnestly fulfill their due obligations specified in international law while enjoying the rights derived from sovereignty in cyberspace.

● Non-infringement of the sovereignty of other countries. No country shall without permission access the cyber infrastructure of another country or infringe on cyber systems within the jurisdiction of another country. No country shall engage in acts of cyber surveillance, theft or sabotage.

● Non-interference in other countries' internal affairs. No country shall interfere in other countries' rights to survival, security

and development in cyberspace, or their rights to maintain cyberspace order, security and development. No country shall support or allow separatist forces to undermine other countries' territorial integrity, national security and social stability through cyberspace.

● Due diligence. No country shall knowingly allow its territory, or territory or Internet facilities, data and information under the control of its government, to be used for cyber activities undermining national security or interests of other countries.

● Protection. All countries have the obligation to protect lawful rights and interests of relevant cyberspace entities within their jurisdiction. They also have the obligation to promote openness and freedom of cyberspace while ensuring order, security and development.

III. The Legal Status of Sovereignty in Cyberspace

As the extension of state sovereignty in cyberspace, sovereignty in cyberspace is also a legally binding principle and rule. States may define their sovereignty differently and may have different perceptions of the threshold for violating sovereignty in cyberspace, but these differences do not affect the legal status of sovereignty in cyberspace under international law.

If a country infringes on the internal supremacy and external independence that another country enjoys on the basis of its national sovereignty over cyber infrastructure, entities, behavior as well as relevant data and information in its territory, this will be a violation of the principle of sovereignty and will constitute a wrongful act under international law. The acts may include, among others, unauthorized penetration into the network systems in the territory or within the jurisdiction of another country, causing disruption or damage of relevant infrastructure or undermining a

country’s exclusive sovereign rights both internally and externally in cyberspace. A cyber operation may simultaneously violate the principles of sovereignty, non-interference in internal affairs and the prohibition of the use of force. The application of this principle to a specific set of circumstances may require certain contextualization.

IV. Some Concepts Related to Sovereignty in Cyberspace

In view of the diverse application scenarios and domains of the principle of sovereignty in cyberspace, the concepts of "information sovereignty", "technological sovereignty", "data sovereignty" and "digital sovereignty" have been put forward by various parties in the international community in recent years.

● **"Information sovereignty" that focuses on content management.** Information can be divided into broad and narrow senses. The former covers technology and content, as is meant by "information security" proposed by Russia. However, "information sovereignty" is more narrowly defined among the academic community. It mainly refers to the information content produced and disseminated by using information and communication technologies and network. The main goal of upholding "information sovereignty" is to ensure effective governance and regulation of information content.

● **"Technological sovereignty" that focuses on capabilities in developing home-grown technologies in key areas.** In February 2020, the European Commission released three important strategic documents: *Shaping Europe's Digital Future*, the *White Paper on Artificial Intelligence* and the *European Data Strategy*. According to Ms. Ursula von der Leyen, President of European Commission, this was aimed at regaining "technological sovereignty" and strengthening EU's ownership in the development and standard setting of cutting-edge technologies and applications

such as artificial intelligence, big data and 5G.

● **"Data sovereignty" that places importance on the strategic value of data.** In the era of big data, the strategic value of data has drawn unprecedented attention. Relevant countries are working to improve data governance in an effort to balance security and development. For example, in 2020 the European Commission issued *A European Strategy for Data* and the *Data Governance Act*.

● **"Digital sovereignty" aimed at enhancing "strategic autonomy".** In the *Digital Sovereignty for Europe* released by the European Parliament in July 2020, "digital sovereignty" was defined as "Europe's ability to act independently in the digital world and should be understood in terms of both protective mechanisms and offensive tools to foster digital innovation (including in cooperation with non-EU companies)". The notion was put forward by the EU to maintain its independence, competitiveness and leadership in the face of competition in the digital world, emphasizing the ability of states to lead their own digital development.

The above concepts may differ in their goals or emphasis, but they are interrelated in nature. Relevant practices and explorations have substantiated the connotation and extension of sovereignty in cyberspace.

Fundamental Principles of Sovereignty in Cyberspace

I. Equality

Sovereign equality as set forth in the UN Charter is the primary principle that all states should follow in the exercise of their sovereignty in cyberspace. All sovereign states, regardless of size, wealth, or strength, are equal before the law and have the right

to participate on an equal footing in international cyberspace affairs. Each state should be treated equally, and each state is also obligated to treat others as equals.

II. Fairness

All states should uphold the principles of fairness and justice in cyberspace and facilitate a more just and equitable global Internet governance system that reflects the wishes and interests of the majority of countries, protects the legitimate rights and interests of developing countries, and ensures the people of countries around the world get to decide on the development of cyberspace. States should not abuse their superiority in Internet facility, technology, system and data to interfere in other countries' exercise of sovereignty in cyberspace or promote unjust acts such as cyber hegemony or isolation.

III. Cooperation

Cyberspace is global in nature. It is difficult for any state to achieve effective governance in cyberspace solely through its own efforts. In line with the principle of cooperation in good faith contained in the UN Charter, states should respect others as subjects of international law, follow the principle of extensive consultation, joint contribution and shared benefits, support multilateral and multi-party participation, and build a holistic governance system across multiple fields and levels to ensure the security and development of cyberspace.

IV. Peace

In an interconnected cyberspace, the interests of all countries are deeply intertwined. All countries should act in conformity with the purposes and principles enshrined in the UN Charter, use the Internet for peaceful purposes, and settle cyber disputes by peaceful means. They should take effective measures to guard against the

use of information and communications technology (ICT) to engage in activities that undermine peace, prevent an arms race in cyberspace, and prevent and fight cyberterrorism to maintain peace and security in cyberspace.

V. Rule of Law

All states should make steady progress in domestic legislation and advance the rule of law in global governance in cyberspace, uphold the authority of international law, and oppose double standards. In the exercise of sovereignty in cyberspace domestically, states should protect the legal rights of their citizens, legal persons, and other organizations in cyberspace, and internationally, states should respect the sovereignty of others in cyberspace, and observe international law. ; states shall not use the Internet to interfere in the internal affairs of other countries or engage in, encourage, or support cyber activities that endanger the national security of other countries.

Key Manifestations of Sovereignty in Cyberspace

Based on the architecture of cyberspace, sovereignty in cyberspace can be divided into four layers, namely physical infrastructure layer, logic layer, application layer and social layer. Each of these layers is a manifestation of national sovereignty.

I. Manifestation of Sovereign in the Physical Infrastructure Layer

A sovereign state has jurisdiction over the physical infrastructure and basic telecommunications services within its territory. In some circumstances, a state may also be entitled to take necessary measures to maintain the security of the physical infrastructure according to national law and in conformity with

international law. A sovereign state participates in the management of and international cooperation on the global cyber infrastructure.

II. Manifestation of Sovereignty in the Logical Layer

A sovereign state can independently enact or adopt the relevant technical regulations or standards on the premise of not violating their obligations under international law, while maintaining the compatibility of the Internet.

III. Manifestation of Sovereignty in the Application Layer

A sovereign state may exercise its jurisdiction over the development and operation of software, protects lawful data and information, especially those related to national security, from theft or destruction in accordance with national and international law. The state can regulate the dissemination of online content stored in its territory, and restricts the dissemination of information that infringes upon public interests. A sovereign state prohibits overseas organizations from fabricating and distorting facts and disseminating online information content in its territory that seriously damages its national security and public interests. A sovereign state participates in international coordination and cooperation on cross-border data flow and information governance.

IV. Manifestation of Sovereignty in the Social Layer

A sovereign state can exercise jurisdiction over its Internet users and platforms, provide proper guidance to cyber entities and foster a social environment suitable for the development of cyberspace.; upholds its independent Internet governance system and participates in international cooperation on improving the Internet governance model on an equal footing. A state has the right to take an equal part in the development of the global digital economy.

The above reflects the systemic nature and integrity of sovereign activities in cyberspace. Respect for sovereignty in cyberspace promotes orderly cooperation, harmony and stability in cyberspace and its sustainable development. At the same time, when exercising sovereignty in cyberspace, a country should adhere to universally recognized principles and rules of international law, respect the interconnected and interactive nature of cyberspace, and avoid fragmentation of the Internet. A state should not politicize cyber security issues in the name of exercising sovereignty in cyberspace, violate international economic and trade rules or market rules, interfere with normal cooperation in cyber infrastructure and service projects, and impose isolation or repression on other states in cyberspace. A state should not use its technological, economic and political power to unfairly allocate or block important network resources or endanger the security of the global supply chain.

Sovereignty in Cyberspace in Practice

I. A number of important international documents affirmed the application of the principle of state sovereignty to cyberspace.

The *Declaration of Principles* adopted at the World Summit on the Information Society in 2003 stated that "policy authority for Internet-related public policy issues is the sovereign right of States". The *Tunis Agenda for the Information Society* adopted at the 2005 WSIS highlighted the key roles and responsibilities of national governments in the summit process.

In 2011 and 2015, the *International Code of Conduct for Information Security* put forward by China, Russia and other

countries reaffirmed that “policy authority for Internet-related public policy issues is the sovereign right of States”.

The reports of the UN Group of Governmental Experts (UN GGE) in 2013, 2015 and 2021 stressed that “state sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities”, emphasized “the principle of sovereignty as the basis for increased security in the use of ICTs by States” and the centrality of “international cooperation, dialogue, and due regard for the sovereignty of all States".

The Leaders Communiqué of G20 Antalya Summit in 2015 affirmed that “international law, and in particular the UN Charter, is applicable to state conduct in the use of ICTs and commit ourselves to the view that all states should abide by norms of responsible state behavior in the use of ICTs”.

The *Goa Declaration* at 2016 BRICS Summit reiterated that “the use and development of ICTs through international and regional cooperation and on the basis of universally accepted norms and principles of international law, including the Charter of the UN in particular political independence, territorial integrity and sovereign equality of States, the settlement of disputes by peaceful means, non-interference in internal affairs of other States as well as respect for human rights and fundamental freedoms, including the right to privacy; are of paramount importance in order to ensure a peaceful, secure and open and cooperative use of ICTs”.

In 2019, the World Internet Conference released the concept document entitled *Jointly Build a Community with a Shared Future in Cyberspace*, stressing that "Sovereignty in cyberspace is a natural extension of the national sovereignty in cyberspace. We should respect the right of each country to independently choose its

own development path and governance model, and to participate in global governance in cyberspace on an equal footing."

The *China-ASEAN Initiative on Establishing a Digital Economy Partnership* issued in 2020 emphasized "respect for sovereignty in cyberspace on the basis of respecting laws and Internet policies of individual countries," and"building a global community with a shared future in cyberspace in a multilateral, democratic and transparent way".

In 2020, the World Internet Conference released the *Initiative on Jointly Building a Community with a Shared Future in Cyberspace*, reaffirming the importance of respecting sovereignty in cyberspace.

The China-Africa Internet Development and Cooperation Forum in 2021 launched the *Initiative on China-Africa Jointly Building a Community with a Shared Future in Cyberspace,* which stated that "On the basis of respecting sovereignty in cyberspace and Internet policies of individual countries, we should explore acceptable means of expanding Internet access and connection, and deliver development opportunities brought by the Internet to more developing countries and peoples."

In the *Samarkand Declaration* and the *New Delhi Declaration* adopted by the Shanghai Cooperation Organization in 2022 and 2023 respectively, "Member States emphasize a key role of the UN in countering threats in the information space, creating a safe, fair and open information space built on the principles of respect for state sovereignty and non-interference in the internal affairs of other countries. They consider it important to ensure equal rights for all countries to regulate the Internet and sovereign right of states to manage it in their national segment".

II. Relevant states have affirmed the application of

the principle of state sovereignty to cyberspace in their position papers.

In recent years, some countries have issued position papers on the application of international law in cyberspace, stating their positions and propositions on the application of the principle of national sovereignty in cyberspace.

In confirming the applicability of state sovereignty to cyberspace, New Zealand released in 2020 *the Application of International Law to State Activity in Cyberspace* which said that it "considers that the standalone rule of territorial sovereignty also applies in the cyber context". In the same year, the *International Law and Cyberspace: Finland's National Positions* also stated that "Finland sees sovereignty as a primary rule of international law" and that "this rule is fully applicable in cyberspace". The *Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace* issued in 2020 maintains that "the territorial sovereignty and jurisdiction of the states are also extended to all elements of the cyberspace". *The Republic of Poland's Position on the Application of International Law in Cyberspace* issued in 2022 also advocates that "the principle of sovereignty applies to cyberspace."

In confirming sovereignty in cyberspace as a binding rule in international law, the document entitled *International Law in Cyberspace* issued by the Netherlands in 2019 said that sovereignty constitutes an independent and binding rule in international law and that "States have an obligation to respect the sovereignty of other states and to refrain from activities that constitute a violation of other countries' sovereignty." In its document *On the Application of International Law in Cyberspace* issued in 2021, Germany clearly

states that "Germany agrees with the view that cyber operations attributable to States which violate the sovereignty of another State are contrary to international law. In this regard, State sovereignty constitutes a legal norm in its own right." In the same year, Norway and Italy expressed in their position papers that sovereignty is not only a principle but also "a primary rule of international law that is applicable in cyberspace". In 2021, China advocated in its position paper submitted to the United Nations Open-ended Working Group on security of and in the use of information and communication technologies 2021-2025 that "State sovereignty in cyberspace is a legally binding principle under international law".

In determining what constitutes an infringement of a state's sovereignty in cyberspace, according to the French document entitled *International Law Applied to Operations in Cyberspace* released in 2019, “Any authorized penetration by a State of French systems or any production of effects on French territory via a digital vector may constitute, at the least, a breach of sovereignty." Iran stressed in its *Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace* issued in 2020 that "Any utilization of cyberspace if and when involves unlawful intrusion to the (public or private) cyber structures which is under the control of another state, maybe constituted as the violation of the sovereignty of the targeted state." In addition, the *National Security Strategy of the Russian Federation* adopted in 2021 states that "The use of information and communications technology is expanding. The use of communication technologies to interfere in the internal affairs of states, undermine their sovereignty, and violate their territorial integrity, is posing a threat to international peace and security." In the same year, Norway declared in its position paper: "Causing

physical damage by cyber means on another State's territory may easily qualify as a violation of territorial sovereignty...In addition to physical damage, causing cyber infrastructure to lose functionality may also be taken into consideration and may amount to a violation...Similarly, a cyber operation that interferes with or usurps the inherently governmental functions of another State may constitute a violation of sovereignty". Brazil stated in its position paper that "Interceptions of telecommunications, for instance, whether or not they are considered to have crossed the threshold of an intervention in the internal affairs of another State, would nevertheless be considered an internationally wrongful act because they violate state sovereignty. Similarly, cyber operations against information systems located in another State's territory or causing extraterritorial effects might also constitute a breach of sovereignty".

III. States affirm the exercise of their sovereignty in cyberspace through legislative, administrative and judicial means.

With regards to advocating and practicing principle of sovereignty in cyberspace, China stated at the 2nd World Internet Conference that respecting sovereignty in cyberspace is an important principle in the reform of the global Internet governance system. In the *Law on Cybersecurity* adopted in 2016, China embraces "safeguarding national sovereignty in cyberspace" as a fundamental purpose of cyberspace legislation. The *National Cyberspace Security Strategy* released in 2016 stresses that "national sovereignty extends to cyberspace" and upholds sovereignty in cyberspace as an important part of national sovereignty. The *Strategy on International Cooperation in Cyberspace* released in 2017 places the principle of national sovereignty on the list of the basic principles for

international cooperation in cyberspace and regards “safeguarding national sovereignty and security” as the primary strategic goal of engaging in such cooperation. The *Data Security Law* adopted in 2021 states that "safeguarding national sovereignty, security, and development interests" is one of the primary objectives of the legislation. China has also made it clear that national sovereignty applies to cyberspace in the UN Group of Government Experts and the Open-Ended Working Group (OEWG), the Asian-African Legal Consultative Organization and in other multilateral fora.

As far as exploring the Internet development path and cyber administration models is concerned, *The Law on Cybersecurity* of Vietnam in 2018 makes it clear that “mutual respect for independence, sovereignty and territorial integrity, mutual non-interference in internal affairs, equality and mutual benefit” form the basic principles of cybersecurity cooperation. It provides a detailed list of acts that are prohibited in cyberspace such as distorting historical facts, undermining ethnic unity, offending religious belief and other acts that violate national sovereignty, interests and security. The European Union put forward “technological sovereignty” in February 2020 in a bid to reinforce its control and dominance in technologies, rules and values in cyberspace.

As for protecting domestic network from threats, disruptions, attacks and sabotage, Russia adopted the *Stable Runet Act* in May 2019 to ensure independence and reliability of its own Internet resources so that it can still function properly when it is unable to connect to servers outside the country. In 2021, Pakistan introduced its inaugural *National Cybersecurity Policy* which confirms that a cyber-attack on its key information infrastructure will be “regarded as an act of aggression against national sovereignty and [Pakistan]

will defend itself with appropriate response measures".

In regard to protecting the rights and interests of citizens in cyberspace and the development of the digital economy, the EU adopted the *General Data Protection Regulation* in May 2018 to put cross-border flow of personal data under strict control, and expands the confines of sovereignty through extra-territorial jurisdiction over processing of personal data. In 2021, the EU issued the *2030 Digital Compass: The European Way for the Digital Decade*, with the aim of guiding the EU in building a sustainable digital society and enhancing the EU's digital sovereignty, ensuring that the EU becomes one of the most advanced regions in the digital economy worldwide. In 2021, France published its *National Cybersecurity Strategy*, outlining its goal to develop the technological capability, so as to protect sovereignty in cyberspace and foster the growth of the cybersecurity industry within the next five years.

Prominent Challenges and Solutions for Sovereignty in Cyberspace in the New Circumstances

The world today is experiencing historic changes in a way never seen before. The new round of technological revolution and industrial transformation, represented by big data and artificial intelligence, is reaching greater depths. The international balance of power is undergoing profound adjustments. A small number of countries are creating "exclusive circles" and engaging in "decoupling" in an attempt to sow division and confrontation in cyberspace. They are developing offensive cyber military capabilities, spreading offensive cyber technologies, and openly conducting offensive cyber operations against other countries. They

have even listed critical infrastructure as targets for wartime cyber attacks. The sovereignty, security, and development interests of countries in cyberspace are facing unprecedented challenges.

I. Artificial Intelligence

In recent years, significant breakthroughs have been made in artificial intelligence (AI) technology which has been widely applied in various fields such as industry, healthcare, transportation, and information content. It has brought tremendous opportunities for humanity but has also posed new challenges to sovereignty in cyberspace. Misuse and abuse of AI technology will lead to the widespread dissemination of misinformation, which constitutes an infringement upon the legal rights of citizens and challenges to countries in maintaining public order. Inconsistent technical standards and regulatory policies on AI among countries can create trade barriers for AI products and services, hindering cooperation in digital economic development among nations.

The development and use of AI have international implications and bear on the future of humanity. Countries should adhere to the principles of people-centeredness and "technology for social good" and promote the establishment of universally inclusive international mechanisms. This will help shape a governance framework and set standards and norms based on broad consensus to ensure the safety, reliability, controllability, and fairness of AI, so that it will empower global sustainable development and enhance the collective well-being of humankind. Countries should strengthen information exchange and technological cooperation based on respect for national sovereignty, promote the peaceful use of AI, jointly address the risks and challenges it poses, and collectively oppose any act of using AI to undermine the sovereignty and security of other countries.

II. Data Governance

Data governance bears on national security, economic security, social stability, and the protection of individual rights. A very few countries, leveraging their technological advantages, have committed acts that harm the cybersecurity and national security of other countries and exacerbate the confrontation in cyberspace through the means of data. A very few countries also use "long-arm jurisdiction" at their own will and engage in cross-border data surveillance, seriously infringing upon the sovereignty in cyberspace of other nations. The abuse of technological monopolies and unilateral coercive measures undermines the fairness, effectiveness, and inclusiveness of global digital development, restricts the digital development rights of developing countries, and weakens their ability to exercise and protect sovereignty in cyberspace.

In the face of these challenges, countries should respect sovereignty in cyberspace, respect the jurisdictional and administrative rights of other countries, and refrain from directly accessing data from businesses or individuals located in other countries without legal permission. Countries should respect the right of each country to choose its own path of data governance based on its national circumstances, and reject acts of using information technology to undermine the critical infrastructure or steal important data of other countries, as well as acts of using it to harm the national security and public interests of other countries. Countries should approach data security issues comprehensively, objectively, and impartially based on facts, and promote the lawful, orderly, and free flow of data. Countries should enhance cooperation on data security, promote the transfer of digital technology and capacity building, bridge the digital divide, and

support capacity-building assistance to developing countries. The international community should, under the leadership of the United Nations, develop common rules that are universally accepted and globally interoperable, and prevent division or fragmentation of global rules on data governance.

III. Satellite Internet

Satellite internet tightly connects the two frontiers of human activities - outer space and cyberspace, and poses new challenges to sovereignty in cyberspace. These include, among others, fair and reasonable allocation of radio frequencies and satellite orbital resources, the possibility of satellite internet bypassing ground-based national regulations and posing challenges to the exercise of sovereignty in cyberspace by other countries, illegal intrusions into network systems that may lead to the manipulation, loss of functionality, or destruction of satellites, which affect security in outer space, as well as damage to satellites which may disrupt satellite-based network systems and affect security in cyberspace.

Countries should adhere to the principle of peaceful use of outer space and the principles established in the International Telecommunication Union (ITU) Constitution for the rational, efficient, economical, and equitable use of radio frequencies and satellite orbital resources. Globally recognized norms should be formed on the construction, operation, and regulation of satellite internet based on respect for national sovereignty, equal participation, and full consultation. Countries should enhance international cooperation, improve crisis management and comprehensive governance in outer space, ensure the long-term sustainable development of outer space, and safeguard national sovereignty and security in cyberspace.

IV. "Long-arm Jurisdiction"

In recent years, "long-arm jurisdiction" has been extended to cyberspace, posing a significant challenge to sovereignty in cyberspace. The exercise of "long-arm jurisdiction" by one country often conflicts with the territorial or personal jurisdiction of other countries. In cyberspace, the frequent exercise of "long-arm jurisdiction" by a very few countries has constituted a form of cyber hegemony, which easily threatens the sovereignty in cyberspace of other countries. The abuse of "long-arm jurisdiction" violates the principle of sovereign equality under international law, threatens the security and stability of cyberspace, and disrupts the normal order of international trade and digital economic cooperation.

Countries should adhere to the purposes and principles of the United Nations Charter, especially the principle of sovereign equality, and resist the abusive behavior of "long-arm jurisdiction" by a very few countries. Countries should uphold the vision of a community with a shared future in cyberspace and strengthen international coordination on jurisdiction in cyberspace. A very few countries should abandon the practice of "long-arm jurisdiction" and fulfill their international responsibilities of non-infringement of other countries' sovereignty and non-interference in their internal affairs.

V. "Decoupling"

A very few countries are pushing for "decoupling" in the fields of economy, trade, and technology and using various means to coerce or even force relevant countries to take sides, which has disrupted market rules and the international economic and trade order, and had a negative impact on the stability of global industrial and supply chains as well as the development of the world economy. Such an act infringes upon the autonomy of other countries in areas

such as industrial development and technological cooperation, undermines the principle of sovereign equality stipulated in the United Nations Charter, intensifies conflicts in cyberspace, and poses a serious threat to peace, development and cooperation in cyberspace.

Countries should adhere to the philosophy of win-win cooperation, openness, and inclusiveness, and firmly oppose various acts of "decoupling". Countries should build consensus on the harms that "decoupling" does to global public interests through extensive discussions, advocate for policy environments conducive to industrial and market development, and give more play to the role of the industrial sector, so as to build supply chains that meet the practical needs of industrial development. Countries should encourage multi-party cooperation between businesses, universities, and research institutes, and explore multiple channels to mitigate or offset the negative impact of "decoupling".

Building a More Inclusive International Cooperation Framework Based on Sovereignty in Cyberspace

Respect for sovereignty in cyberspace means respect for the purposes and principles enshrined in the UN Charter in cyberspace. It is the basis and the prerequisite for upholding peace and security in cyberspace and a necessary means to ensure strategic stability in cyberspace. Advocating and practicing sovereignty in cyberspace does not mean that countries can do as they wish in cyberspace or pursue a beggar-thy-neighbor policy. The establishment of a more inclusive international cooperation framework based on sovereignty in cyberspace aims to balance the relationship between sovereign rights and obligations of all states on the basis of respecting their

sovereignty. It helps all parties enjoy the benefits of the digital era and promotes peace, security and development of cyberspace.

First, it is important to coordinate different perceptions of sovereignty in cyberspace, and on this basis promote and consolidate international consensus on sovereignty in cyberspace. The difference among states in exercising sovereignty in cyberspace will remain for a long time, but the application of the principle of state sovereignty in cyberspace has been confirmed by many important international documents. Countries should remove prejudice, recognize the fact that cyberspace is a world of shared interests, and uphold the international system with the UN at its core and the international order based on international law. Countries should recognize that sovereignty in cyberspace is an undeniable reality, seek common ground while shelving differences, respect and understand each other, actively interact, and avoid mutual constraints. Countries should encourage multilateral, bilateral and multi-party cooperation and dialogue at global and regional levels, jointly build international consensus on sovereignty in cyberspace, enhance mutual trust in cyberspace, and jointly promote the realization of the common values of peace, development, equity, justice, democracy, and freedom for humanity.

Second, based on the principle of sovereignty in cyberspace, international rules and systems conducive to inclusive cooperation should be established. Mechanisms within and among countries should be endorsed or established as an institutional guarantee for international cooperation. Countries should not only improve their domestic systems, but also enhance international coordination and actively participate in global institutional building on cyberspace. With the UN as the main channel and based on the purposes and principles of the UN Charter,

countries should support the UN in playing a core role in global cyberspace governance, and work together to build systems and norms such as a security mechanism to protect the cyber infrastructure and the legal rights of entities, a cooperative mechanism on exchange and sharing of data information and digital technology, a risk prevention mechanism against malicious activities in cyberspace, a mechanism to crack down on cybercrimes, and a consultation and mediation mechanism on settling disputes in cyberspace. All countries should, in the spirit of honesty and goodwill, do their best to establish effective international rules and systems to govern cyberspace. Countries should ensure the equal realization of sovereign rights in cyberspace and universal compliance with international law obligations in cyberspace. States should promote cooperation in cyberspace for the benefit of mankind. They should prevent hegemonism, zero-sum thinking, and Cold War mentality from adversely affecting peace and development in cyberspace.

Third, states should promote joint development and cooperation of countries on sovereignty in cyberspace with concrete actions. Sovereignty in cyberspace exists in the community with a shared future in cyberspace. To effectively protect sovereignty in cyberspace, the international community needs to:

Achieving shared development. Countries should adopt more proactive, inclusive and coordinated policies that benefit all, speed up global information infrastructure construction, promote innovative development of the digital economy and enhance public service capacity.

Jointly pushing for development. Countries should adopt more active, inclusive and coordinated policies that benefit all for

faster global information infrastructure construction, innovation in digital economy, and higher level of public services;

Jointly safeguarding cybersecurity. Countries should advocate the notion of cybersecurity based on openness and cooperation, attach equal importance to security and development, take an active part in the UN cyberspace security process, and work together to uphold peace and security in cyberspace;

Jointly participating in cyberspace governance. Countries should uphold multilateral and multi-stakeholder governance, strengthen dialogue and consultation, and build a more just and equitable global Internet governance system;

Sharing the benefits. Countries should develop science and technology that are human-centered for the greater good, in order to narrow the digital divide and achieve common prosperity. Countries should jointly promote "goodwill cooperation" on sovereignty in cyberspace with joint efforts and concrete actions, so as to ensure joint governance, win-win development and shared benefits in cyberspace.

Respecting Sovereignty in Cyberspace and Jointly Building a Community with a Shared Future in Cyberspace

The principle of sovereignty in cyberspace comes first in President Xi Jinping's "Four Principles" for promoting the reform of the global internet governance system and his "Five Proposals" on building a community with a shared future in cyberspace. Advocating and practicing sovereignty in cyberspace does not mean sealing off the cyberspace or breaking it up. Instead, it means facilitating a just and equitable international cyberspace order that respects national sovereignty and building a community with a

shared future in cyberspace. The latter is the driving force and long-term goal for safeguarding sovereignty in cyberspace. Building cyberspace into a community of common development, security, responsibility and interests that benefit all humanity must be achieved on the basis of respecting the sovereignty of all countries.

In building a community with a shared future in cyberspace, countries must adhere to the principle of sovereignty in cyberspace. Building a community with a shared future in cyberspace requires the concerted efforts of all countries to address risks and challenges. Clearly defined national sovereignty in cyberspace and respect for it is essential for jointly building a community of shared future in cyberspace. Only when countries are assured that they have independent rights in choosing their own cyberspace development paths, governance models, and public policies, have equal rights in participating in the rule setting for international cyberspace governance, have jurisdiction over their own cyberspace through legislative, administrative, and legal means, and enjoy right of defense against external risks and infringements in cyberspace, can there be an effective dialogue and consultation mechanism among countries through exchange and cooperation on an equal footing, which serves a community with a shared future in cyberspace.

Sovereignty in cyberspace needs to be better secured and protected through building a community of shared future in cyberspace. The rapid development of the Internet has created unprecedented opportunities for the progress of human civilization, yet problems such as unbalanced development and flaws in rules and order have become more prominent. Hegemonism, power politics, protectionism, and unilateralism persist in cyberspace.

Infringement on privacy and intellectual property rights, dissemination of false information, online fraud, cyber terrorism, and other illegal and criminal activities have become a global scourge. In cyberspace, countries have enormous shared interests. Effective responses to threats to security and development in this domain count on the cooperation and coordination of all countries. Building a community with a shared future in cyberspace can effectively safeguard the sovereignty of all countries in cyberspace.

However, as national interests are not the same and are sometimes even conflicting with one another, it is not always easy to strike a balance between safeguarding national interests and providing international public goods. Rising geopolitical tensions in the context of emerging issues concerning cross-border data flow, disinformation and supply chain security, etc. have made it difficult to push for progress in negotiations on international rules and norms. To identify the converging interests among all countries, it is imperative to follow the principles of respecting sovereignty in cyberspace, maintaining peace and security, promoting openness and cooperation, and building a sound order.

Human society once again stands at a historic crossroads, where countries are facing unprecedented challenges to their sovereignty, security, and development interests in cyberspace. The practice of sovereignty in cyberspace knows no bounds, and so does theoretical innovation. This reveals the long-term and arduous nature of building a community with a shared future in cyberspace. We call on all countries to jointly commit to maintaining global internet interconnectivity, uphold and develop the principle of sovereignty in cyberspace through international cooperation and exchanges in cyberspace, promote high-quality development of the digital economy, realize high-level network security, advance

high-standard opening up in the digital domain, and foster an inclusive and symbiotic digital civilization. We call on the international community to work together under the UN framework and uphold the principles of engaging in discussions as equals, seeking common ground while shelving differences, and pursuing mutual benefits. We call on all countries to strengthen communication, coordinate positions, and on the basis of respecting and upholding sovereignty in cyberspace, formulate universally acceptable international rules and codes of conduct for cyberspace, broaden consensus, and contribute wisdom and strength for building a peaceful, secure, open, cooperative, and orderly cyberspace.

Annex:

Main Practices of Some Countries Regarding Sovereignty in Cyberspace

In recent years, an increasing number of countries, especially developing countries, have embraced and actively practiced the principle of sovereignty in cyberspace in their effort to safeguard national interests, ensure national security, enhance the well-being of their citizens, promote international cooperation, and jointly build a community with a shared future in cyberspace. These practices fully demonstrate the theoretical value and practical significance of the principle of sovereignty in cyberspace.

I. China

In recent years, the Chinese government has successively introduced a series of policies and regulations to firmly uphold its sovereignty in cyberspace, further improving the regulatory framework centered around laws such as the *Cybersecurity Law*, the *Data Security Law*, and the *Personal Information Protection Law*. China has also issued or revised laws, regulations, and rules, including the *Export Control Law* (2020), the *Regulations on the Security Protection of Critical Information Infrastructure* (2021), the *Measures for Cybersecurity Review* (2022), the *Measures for Data Security Assessment for Cross-Border Transfer* (2022), and the *Measures for Standard Contracts for the Cross-Border Transfer of Personal Information* (2023). These laws and regulations have helped safeguard national sovereignty in cyberspace from various aspects such as controlling the export of network technologies, protecting critical information infrastructure, maintaining cybersecurity, and ensuring the security of data and personal

information during cross-border transfers.

In practicing the concept of sovereignty in cyberspace, China has taken the following actions. First, it continues to advocate the concept of sovereignty in cyberspace in the international community. In 2021, China submitted the position paper on international rules for cyberspace and the position paper on sovereignty in cyberspace to the United Nations Open-ended Working Group on Information Security, affirming that "the principle of national sovereignty should be applicable to cyberspace" and elaborating on the meaning of sovereignty in cyberspace from the perspectives of both rights and obligations. Second, China actively practices the concept of sovereignty in cyberspace in international cooperation in cyberspace. It has issued initiatives such as the *Global Data Security Initiative* (2020), the *China-ASEAN Initiative on Building a Digital Economy Partnership* (2020), and the *China-Africa Initiative on Building a Community with a Shared Future in Cyberspace* (2021). In 2022, China published a white paper titled *Building a Community with a Shared Future in Cyberspace*, pledging to jointly safeguard cybersecurity and promote digital development on the basis of mutual respect for sovereignty in cyberspace. In the *Joint Statement on Deepening the Comprehensive Strategic Partnership of Coordination* between China and Russia (2023), both countries proposed the building of a multilateral, fair, and transparent global internet governance system under the premise of ensuring the national sovereignty on internet governance and security of all countries. Third, building upon the World Internet Conference held for consecutive years, China established the International Organization of the World Internet Conference in 2022 to better support equal participation of all countries in international

cyberspace governance, and further safeguard their own sovereignty in cyberspace and development interests, in an effort to jointly build a community with a shared future in cyberspace.

II. Russia

Russia proposes such terms as “information sovereignty”, “digital sovereignty”, and “technological sovereignty in the ICT” to accentuate the importance of ensuring control not only over technical infrastructure, but also over the cross-border flow of information. At the national level, Russia has issued two strategic planning documents that are directly related to ensuring information security: The *Doctrine of Information Security of the Russian Federation*, approved in 2016, and the *Basic Principles of State Policy on International Information Security*, issued in 2021. They use similar terms like "information sovereignty/information space sovereignty" and "information and communication technology sovereignty."

In November 2019, Russia enforced the *Stable Runet Law*, also known as the *Federal Law No. 90-FZ of May 1, 2019 on Amending the Federal Law on Communications and the Federal Law on Information, Information Technologies and Protection of Information*. It formed the legal basis for the centralized Internet management system within the state borders by the state authority. It authorized the compulsory installation of technical equipment for counteracting threats; centralized management of telecommunication networks in case of a threat and a control mechanism for connection lines crossing the border of Russia; and the implementation of a Russian national Domain Name System.

In 2022, Russia initiated the update of its policy in the field of information sovereignty. For example, the activities of a number of Western IT platforms were banned in Russia, which was a step

towards strengthening information sovereignty.

III. India

The pandemic years have seen increasing digitization of all Indian sectors — education, healthcare, agriculture, research, government, workplaces, and marketplaces. This has enhanced the national consciousness about sovereignty in cyberspace. Prime Minister Modi's missions of "smart cities" or "Digital India" can be seen as examples of protecting citizens through sovereignty in cyberspace.

In 2000, India first enacted a comprehensive *Information Technology Act* which was substantially amended in 2008. It creates an enabling environment for the commercial use of cyberspace. To address issues relating to data security, India's *Personal Data Protection Bill* of 2019, for instance, propagates data localization and private cyber firms' obligation to share data with investigating agencies. Moreover, although India's *Information Technology Act* of 2000 stipulates exercising jurisdiction beyond India's territorial borders, yet this has rarely been put into practice owing to serious difficulties in cooperation with foreign law enforcement agencies and incompatible legal regimes.

As debates on sovereignty in cyberspace remain yet work-in-progress, India's much anticipated *Cybersecurity Strategy 2023* — which is expected to be released this year — should bring further clarity on India's narratives, policy, legal frames, and practices of sovereignty in cyberspace.

IV. Mexico

The National Cybersecurity Policy in Mexico is a set of guidelines and strategies designed to ensure the security and protection of the country's critical infrastructure, information, and information systems. In 2017, Mexico launched its first

cybersecurity framework called the *National Cybersecurity Strategy* (NCS) which was developed by the federal government and the National Security Agency of Mexico (CISEN). The NCS has eight cross-cutting pillars to strengthen cybersecurity actions applicable in the social, economic, and political spheres. Moreover, the NCS lists five strategic objectives, among which "National Security" stands out, consisting of "Develop capacities to prevent risks and threats in cyberspace that may alter national sovereignty, integrity, independence, and impact development and national interests".

Mexico does not have a specific law that regulates the sovereignty in cyberspace. However, there are some provisions and laws in place that seek to regulate aspects related to online security and privacy. For example, the *Federal Law on Protection of Personal Data Held by Private Parties* establishes the obligations and rights of holders of personal data and those responsible for its treatment, including data that is collected and processed online. The Federal *Telecommunications and Broadcasting Law* establishes the basis for regulating access to the Internet, network neutrality, and the protection of user rights online, among other aspects. The *Federal Penal Code* establishes sanctions for crimes committed online such as illicit access to computer systems and networks, interference in computer systems, and the dissemination of computer viruses.

V. Turkmenistan

Turkmenistan upholds its rights to independently choose its own path of cyber development, model of cyber governance, and internet policies free from any external interference. In November 2018, Turkmenistan adopted the *Concept for the Development of the Digital Economy in 2019-2025*, and the main purpose of this

document is to modernize state governance, improve administrative functionality, and diversify the engines of economic development of Turkmenistan. In September 2019, Turkmenistan established the Cybersecurity Service (SCS). In February 2021, Turkmenistan adopted the *State Program on the Development of the Digital Economy of Turkmenistan for 2021–2025*. Turkmenistan has also approved the *State Cybersecurity Program for 2022-2025*.

Turkmenistan holds the view that every country preserves the right to choose its own path of cyber development independently, emphasizing that the model of its cyber governance and internet policies should be free from any external interference. It advocates respect for other countries' sovereignty and continues to practice global governance in cyberspace on an equal footing in an international arena. Turkmenistan welcomes cooperation in monitoring emerging threats in the field of international information security and responding to them.

VI. Tanzania

Sovereignty in cyberspace and security are important areas of cyberspace governance in Tanzania. Tanzania considers information and communication technology a crucial driver of economic development and seeks to safeguard cybersecurity through the advancement of critical infrastructure. In 2022, Tanzania decided to launch the Digital Tanzania Project with a planned investment of $150 million to accelerate the development of the digital economy through the improvement of legal frameworks, the training of digital economy experts, and the construction of a national data center.

Legislation plays an important role in strengthening internet management and protecting sovereignty in cyberspace in Tanzania. Various laws have been enacted, including the *Tanzania*

Intelligence and Security Service (Amendment) Act, the *Personal Data Protection Act*, and the *Cybercrime Act*. The *Electronic Transactions Act* adopted in 2015, provides detailed provisions on the authentication procedures and usage of electronic signatures, offering legal recognition and protection for online transactions. The Data Security and Cybercrime Prevention Program was implemented in 2017, setting standards and requirements for data protection in various industries. In the same year, the e-government security architecture was established for state-level regulation of cybersecurity. The *Electronic and Postal Communications (Online Content) Regulations* adopted in 2020 has further strengthened social media regulation. In 2021, the *Cyberterrorism Governance Plan* was introduced which played an important role in enhancing data security governance and combating cybercrime and cyberterrorism. Tanzania adheres to the diplomatic principle of unity and mutual assistance. It has actively cooperated with other countries and international organizations to jointly safeguard cybersecurity and further assert its own sovereignty in cyberspace.

VII. Nigeria

Nigeria designated telecommunications equipment as Critical National Infrastructure in 2020, and it lays out a plan in the *National Development Plan 2021-2025: Volume I* for the development of the digital economy and plans to channel $40 billion of private capital investment into digital infrastructure by 2025. In the *National Digital Economy Policy and Strategy (2020 - 2030) For A Digital Nigeria*, some pillars were proposed such as Digital Literacy and Skills, Indigenous Content Development, and Adoption, in an effort to positively maintain security in cyberspace. Nigeria has issued a series of laws and regulations, including the *Cybercrimes (Prohibition and Prevention) Act (2015)*, which

creates a comprehensive legal, regulatory, and institutional framework in Nigeria to prohibit, prevent, detect, prosecute, and punish cybercrime. Nigeria has issued the *Nigeria Cloud Computing Policy (2019)*, *Nigeria Data Protection Regulation (2019),* and other policies and regulations. The *Nigeria Data Protection Regulation (2019)* provides for Nigerians to have greater control over how their data is collected, shared, and used. Moreover, the *Data Protection Act 2023* which was signed into law in 2023 is Nigeria's latest effort in this regard.

In 2019, Nigeria announced that it would tighten regulation of social media to combat fake news and disinformation. In June 2021, after Twitter deleted a tweet from President Buhari warning of recent unrest in the southeast and freezing his account for 12 hours, the Nigerian government suspended the operation of Twitter until early 2022, and instructed the National Broadcasting Commission (NBC) to immediately begin reviewing and licensing all Over The Top (OTT) and social media apps in Nigeria. Nigeria has taken several measures to secure data and cyberspace in 2022, such as establishing the Data Protection Bureau (NDPB) and the National Shared Services Center.