

美国数据殖民主义的多重逻辑批判及应对*

刘 妍

【内容提要】 国际政治经济格局的演变、信息技术的革新，使殖民主义在大数据时代发展出新的形态，以美国为代表的数字霸权国家在虚拟空间开启了新一轮的殖民掠夺与剥削。在时空维度的演进中，殖民主义经历了显著嬗变，发生了空间扩散、对象变迁、暴力更新与权力重组。基于压迫、剥削、掠夺、垄断与依赖五大殖民要素，美国数据殖民主义呈现四重逻辑：占领数字领土，独享根域控制，以拓展本国“数字版图”；掠夺数据资源，攫取数字红利，来扩大全球“数据势差”；主导数字技术，控制技术传播，以加深全球“技术鸿沟”；垄断数字市场，构筑贸易壁垒，以加剧他国“数字依赖”。美国数据殖民主义具有新特征：数字技术成为新的殖民理性，规则成为殖民者的辅助工具，数据平台成为殖民化的共谋，甚至主权国家也沦为被殖民者。为打破美国数据殖民主义的桎梏，需建立完善有效的数据主权法律框架，塑造自主可控的数字技术创新能力，构建安全互信的区域数字经济业态，培育公平正义的全球数字人文生态。

【关键词】 数据殖民 数字帝国 数字资本 数据平台 数据霸权

作者简介：刘妍（1996-），湘潭大学习近平新时代中国特色社会主义思想研究中心研究员，湘潭大学法学学部知识产权学院讲师（湖南湘潭 411105）。

随着数字技术的迅猛发展，数据已从单纯的信息记录载体跃升为关键性生产要素与战略性资源，成为重塑世界格局的重要驱动力。在这一数字化转型的浪潮中，美国凭借其数字技术的先发优势与雄厚的资本实力，逐步构建起数字领域的霸权体系。这种由美国主导的数据控制与资源攫取模式，是“帝国的新衣”^①，实质上构成了一种新型的“数据殖民主义”形态。

国内外有关数据殖民主义的主流研究范式倾向于将数据殖民主义界定为数据平台对个体的殖民过程。代表性观点如科技巨头的榨取行为是殖民主义的延续、数据殖民主义是数据平台对数据和数据基础设施的控制等，具体又体现为通过剥夺个体数据并将其转化为可用于算法分析和市场交易的数字商品，将社会关系量化为数据关系，导致人的个性丧失和人文精神消弭，并带来算法歧视等一系列负面影响。殖民主义天然地与帝国主义相关联，是西方宗主国为维护中心与外缘地区之间的不平等关系而制定的方针、政策^②。因此，殖民主义是与国家行为相联系的。而所谓由数据平台主导的以商业利益为核心的数据殖民主义，实质上是“数据榨取主义”^③。事实上，自2019年尼克·库

* 本文系国家社科基金重大项目“总体国家安全观下产业知识产权风险治理现代化研究”（21&ZD204）的阶段性成果。

① 蔡翠红、于大皓：《“帝国的新衣”：世界数字体系下的美国数字霸权》，《当代世界与社会主义》2024年第3期。

② 参见高岱：《“殖民主义”与“新殖民主义”考释》，《历史研究》1998年第2期。

③ Juliane Jarke and Jo Bates (eds.), *Dialogues in Data Power: Shifting Response-abilities in a Datafied World*, Bristol: Bristol University Press, 2024, pp. 120-137.

德里等人^①第一次系统性论证数据殖民主义，并将焦点集中在数据平台对数据的垄断与对个人的剥削之后，国内外几乎所有研究都在关注数据平台之于数据殖民主义的作用与意义。这些将美国的谷歌、亚马逊、苹果、Meta等数据平台视作美国推进数据殖民主要路径的研究，其实忽略了数据殖民的本质——如果数据殖民的发展与扩散是基于哪个国家的数据平台更多更强，那中国无疑也要被纳入讨论之中；同时也看低了美国数据殖民对全球产生的危害——如果被殖民只是被数据平台剥削，那人们也无需对美帝国主义的数据殖民感到如此焦虑。我们当下要将目光从数据平台移开，或者说要透过数据平台，直接看向其背后的“驼背侏儒”^②，即美国政府。

当然，揭露美国政府在万物互联时代的殖民行径并非新鲜事。我国学者张纯厚早在2012年就通过科索沃战争、乌鲁木齐暴力事件等案例，揭示了美国通过国际互联网操纵他国政治、分裂他国政权的“网络殖民主义”行径^③；美国著名学者迈克尔·奎特也指出，“全球南方”正笼罩在美国数据殖民主义的阴影之中^④；西班牙一些公司同样对过度依赖美国的数据巨头企业表示高度担忧，认为美国的数据霸权地位已构成一种“新殖民主义”^⑤。当下，我们需要在TikTok事件与美国系列“数据脱钩”政策的警醒下，系统回顾大数据时代以来殖民主义的嬗变形态，在与历史上的殖民主义进行对比分析的基础上，把握美国数据殖民主义的核心逻辑与崭新特征，进而为我国乃至世界各国有效反抗美国的数据殖民主义提供有效指引。

一、殖民主义在大数据时代的嬗变

理解数据殖民主义，首先要回到殖民主义的传统语境。殖民主义是一种群体统治形式，即一个群体对另一个文化异质群体的控制，其本质是强国凭借暴力占领弱国的生存空间，并对其进行资源掠夺、政治控制与文化渗透，既打断了这些国家和地区的社会发展进程，又在客观上对这些国家和地区进行了社会改造，为西方社会发展奠定物质基础。大数据时代，殖民主义发生了深刻且复杂的嬗变，其演变轨迹跨越多个关键维度，历经殖民空间的扩散、对象的变迁、暴力的更新以及权力的重组（详见表1）。

1. 空间扩散：从局部地理域到全球数字域

后殖民主义研究的创始人之一爱德华·萨义德指出，地理是帝国主义的核心与灵魂，领土控制是殖民主义的基础，任何对数据殖民主义的探究都应从在数字世界中建立地理思维开始^⑥。毋庸置疑，数据殖民主义超越了历史殖民主义时期的地理空间概念，通过数字技术和网络连接实现了对数据的全面攫取与控制。一方面，历史上的殖民主义主要发生在特定的地理区域，尤其是第三世界，数据殖民主义的影响范围则依托互联网的全球化连接和数字基础设施的广泛铺设，突破了传统地理疆域的束缚。在数字空间，“第一、第二和第三世界的空间划分已被打乱……我们正面对一个由新

① Nick Couldry and Ulises A. Mejias, “Data Colonialism: Rethinking Big Data’s Relation to the Contemporary Subject”, *Television & New Media*, Vol. 20, No. 4, 2019.

② 《本雅明文选》，陈永国、马海良编，北京：中国社会科学出版社，1999年，第403页。

③ 参见张纯厚：《全球化和互联网时代的国家主权、民族国家与网络殖民主义》，《马克思主义与现实》2012年第4期。

④ 参见〔美〕迈克尔·奎特：《数字殖民主义：美帝国与全球南方的新帝国主义》，顾海燕译，《国外理论动态》2022年第3期。

⑤ Carla Hobbs (ed.), “Europe’s Digital Sovereignty: From Rulemaker to Superpower in the Age of US-China Rivalry”, https://ecfr.eu/wp-content/uploads/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry.pdf.

⑥ Petar Jandrić and Ana Kuzmanić, “Digital Postcolonialism”, *IADIS International Journal on WWW/Internet*, Vol. 13, No. 2, 2015.

的复杂分化和同质化、去领土化和再领土化机制所定义的世界”^①，任何接入互联网的国家都有被殖民的风险。另一方面，数据殖民的范围不仅仅是不发达地区或发展中国家，而且波及全球各个国家和地区。在传统地缘政治格局中，美国通过军事同盟、经济援助等手段构建起以自身为核心的盟友体系，欧盟、澳大利亚、新西兰、日本等国家和地区在政治、经济和军事上与美国保持着紧密联系。然而，在数据殖民背景下，大多数基于域名生成的虚拟土地已经被殖民化，其他国家与美国的盟友关系并不能让其逃脱受美国掠夺的命运。

表 1 殖民主义在大数据时代的嬗变

殖民主义类型 嬗变内容	历史上的殖民主义	数据殖民主义
殖民空间	局部地理域 (殖民范围主要是第三世界、全球南方)	全球数字域 (任何接入互联网的国家、地区)
殖民对象	物质资源 (如土地、矿产)	数字资源 (如数据、数据基础设施)
殖民暴力	物理暴力 (如实体军队、钢枪、大炮)	数字暴力 (如网络部队、算法、病毒)
殖民权力	分散、有限 (权力受制于地理、多利益攸关者等因素)	集中、无限 (权力在数据、算法的协助下愈发集中、无限制)

2. 对象变迁：从物质资源到数字资源

大规模的资源掠夺、对殖民对象的高度控制，是历史上的殖民主义的两个根本性特征^②。空间的拓展、技术的赋能，使殖民者实现了对殖民对象在资源掠夺上的演变，殖民者不再直接侵占物质性生产资料，数字资源成为更重要的资本积累对象。其一，历史上的殖民主义主要关注土地、矿产等物质资源的占有和掠夺，而数据殖民主义则将重点转向了数据与数据基础设施等数字资源的垄断与控制。通过垄断数据、硬件、软件、技术等数字资源，以及控制电缆、稀土及其他建造和维护数据基础设施所需的物质材料，将供应链中最具创新性和复杂性的部分内迁，殖民者进行着多样化的资本积累。当数据基础设施、数字技术等关键数字资源无法独立生产或创新时，一种不对等的依赖关系就会被殖民者培养出来，将被殖民者推向遭受技术经济奴役的境地^③。其二，历史上的殖民主义控制殖民对象的方式一般是直接的政治统治与军事镇压，而数据殖民主义控制殖民对象的方式高度依赖数据规则和数据关系。例如，发达国家以数据标准为中介，将国内规则国际化，造成他国对本国规则的接受与追随^④。美国通过《跨大西洋数据隐私框架》等多边条约实现数据领域的长臂管辖就是典型例子。其三，历史上的殖民主义控制下的人口一般会沦为廉价劳动力，数据殖民主义控

① Michael Hardt and Antonio Negri, *Empire*, Cambridge: Harvard University Press, 2000, p. xiii.

② 参见刘皓琰：《新帝国主义的数字殖民——从网络族群与注意力时间谈起》，《国外理论动态》2020年第3期。

③ Hermann Hauser and Hazem Danny Nakib, “The Rise of Techno-Colonialism”, <https://www.stabroeknews.com/2024/08/09/features/project-syndicate/the-rise-of-techno-colonialism/>.

④ 参见徐秀军：《规则内化与规则外溢——中美参与全球治理的内在逻辑》，《世界经济与政治》2017年第9期。

制下的人口实现了数字化，人类的行为被转化为可收集的数据^①，为数据平台创造收入的内容创作者沦为没有工资的纯粹“产消者”^②。

3. 暴力更新：从物理暴力到数字暴力

暴力执行者、暴力组织和暴力工具是组成传统物理暴力的三要素^③，我们这个时代的暴力正在进行数字化转型，物理暴力正在更新为“数字暴力”。其一，国家行为体这一传统暴力执行者，正在更新为国家行为体与非国家行为体相结合的暴力执行者。在俄乌冲突中，首次出现了多家美国的综合性科技公司参与战争的现象。如 SpaceX 公司的星链卫星在保持乌克兰通讯方面发挥着至关重要的作用，Maxar 公司将俄罗斯车队、部队、机场活动的高清图像提供给乌克兰^④。其二，实体军队这一传统暴力组织，正在更新为实体军队与网络部队相结合的暴力组织。网络战已从以前的辅助战、补充战范式转变为影响力巨大的独立战范式，网络部队在攻击他国时与实体军队联合，补充了新兴领域的作战力量。其三，钢枪、大炮等传统暴力工具，正在更新为病毒、算法、人工智能等数字化暴力工具。当前，数字武器（Digital）与原子武器（Atomic）、生物武器（Biological）和化学武器（Chemical）并称为“ABCD”大规模杀伤性武器。技术的不断发展则使数字武器更为精确，可以增强战场上的态势感知和决策能力，加快情报收集过程并提高其质量，因而人工智能等数字技术被大量用于军事领域。算法则是一种隐蔽性更强的数字暴力，利用精准的内容推送机制实践着葛兰西的文化领导权理论，即资本主义社会已经开始从依赖武装暴力到开展文化宣传来控制社会，通过在道德和精神方面占据领导地位，让人们接受它们的世界观、价值观、人生观和一系列的法律制度来达到统治的目的。

4. 权力重组：从分散有限到集中无限

历史上的殖民主义，交通与通信技术的落后严重制约了殖民者对殖民地的管控效率，导致殖民权力呈现分散、有限的状态。比较而言，数据的无边界性与数字技术的增强，使得殖民权力得到了更为集中的重组。其一，从行使权力的主体来看，历史上的殖民主义权力主体较为多元、分散。以英属非洲殖民地为例，其权力运作既受到殖民政府的约束，又受到白人移民、商业公司、传教士等不同利益群体的制约^⑤；而数据殖民主义体系下的权力则主要集中在美国政府与其大型科技公司手中，后者又受到政府法律的约束。可以说，美国政府通过先进的技术与严密的法律在数字空间构建起了强大的、集中的殖民权力网络。其二，从权力实施的限度来看，受制于地理范围，历史上的殖民主义权力存在明显的限度，英国殖民统治在一些地方“只不过是两个人加上一条狗”^⑥，无法实现对内陆的深度管控，权力在地理上的延伸受到极大限制；而数据殖民主义的权力覆盖范围不受地理的限制，美国政府可以通过算法跨越物理界限，对全球实施无限监控，“斯诺登事件”就是最有力的证据。其三，从权力作用的劳动对象来看，历史上的殖民主义将工人局限在固定的物理空间进行

① Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York: PublicAffairs, 2019, p. 233.

② “产消者”也称“生产型消费者”，是美国著名未来学家阿尔文·托夫勒在其专著《第三次浪潮》中提出的概念，意即可以自行生产所需商品和劳务的消费者，结合了专业生产者和消费者的角色。参见〔美〕阿尔文·托夫勒：《第三次浪潮》，黄明坚译，北京：中信出版社，2018年，第338页。

③ 参见黄其松：《数字时代的国家理论》，《中国社会科学》2022年第10期。

④ Marko Höyhtyä and Sari Uusipaavalniemi, “The Space Domain and the Russo-Ukrainian War: Actors, Tools, and Impact”, <https://www.hybridcoe.fi/wp-content/uploads/2023/01/20230109-Hybrid-CoE-Working-Paper-21-Space-and-the-Ukraine-war-WEB.pdf>.

⑤ 参见李鹏涛：《20世纪80年代以来英美学界的殖民时期非洲史研究述评》，《世界历史》2015年第5期。

⑥ 李鹏涛：《殖民主义与非洲社会变迁——以英属非洲殖民地为中心（1890-1960年）》，北京：社会科学文献出版社，2019年，第11-27页。

监督控制，并通过建立跨国公司将世界范围内的更多劳动者裹挟到资本控制中以服务于剩余价值生产；数据殖民主义则凭借算法实现超空间集中控制和监视，数字劳动者在数字技术的全天候、全景式监控下进行劳动。

二、美国数据殖民主义的四重逻辑

为了“占领”更辽阔的数字版图、掠夺更丰富的数据资源、加速对数字暴力的垄断、扩大数据殖民的范围，从而在第四次工业革命中迅速完成资本积累，获取更加坚固的结构性殖民权力，美国以殖民主义的压迫、剥削、掠夺、垄断、依赖五大要素为基准，对其他国家进行数据殖民（详见表2）。这些殖民行为暗含在美国占领数字领土、掠夺数据资源、主导数字技术与垄断数据市场的四重逻辑之中，随之给世界带来了系列严重后果，侵犯着他国数据主权，扩大了全球“数据势差”，加深了全球“技术鸿沟”，加剧了他国“数字依赖”。

表2 历史上的殖民主义与数据殖民主义的关键措施比较

殖民主义类型 殖民逻辑	历史上的殖民主义	数据殖民主义
领土占领	控制港口、海峡、重要贸易城市等关键地理节点	控制 DNS，尤其是根区 DNS
资源掠夺	掠夺土地与自然资源	掠夺数据资源
技术主导	延长落后国家工业化进程，限制和阻碍落后国家的技术发展	通过限制技术许可、限制企业合作控制数字技术传播速度
市场垄断	通过法律和贸易公司控制殖民地的贸易	依托数据企业和贸易规则构建全球市场依赖关系

1. 占领数字领土：独享根域控制拓展本国“数字版图”

历史上的殖民主义，控制港口、海峡、重要贸易城市等关键地理节点是维持宗主国经济优势的战略举措，如英国对直布罗陀海峡的控制使其扼住了海上贸易的咽喉。在数字空间，这些关键地理节点就是互联网的“中枢神经网络”——域名系统（以下简称 DNS）。互联网诞生以来，支撑全球 DNS 的共有 13 台根服务器，其中 1 台主根服务器位于美国本土，其余 12 台根域名解析服务器有 9 台位于美国，3 台位于美国盟友（英国、瑞典、日本）境内，且均由美国一家名为互联网名称与数字地址分配机构（ICANN）的企业控制。从本质上看，美国政府控制全球互联网、占领数字领土、拓展本国“数字版图”的方式就是通过监管 ICANN 及其控制的根域实现的。质言之，美国通过独享互联网根域控制，掌控数字领土的“封疆权”。

即便在国际社会的质疑和批评下，美国商务部已在 2014 年将数字地址和域名管理权移交给全球互联网社群，但美国政府仍保有对 ICANN 的监督权，仍可实质性地对其进行政治控制进而实现美国国家利益^①。全球互联网的“根”也仍在美国，世界各国人民的信息交流绝大多数要经过一次“美

^① 参见〔美〕弥尔顿·L. 穆勒：《网络与国家：互联网治理的全球政治学》，周程等译，上海：上海交通大学出版社，2015 年，第 72-25 页。

国游”才能到达目的地^①。各国都意识到了这一风险，如巴西时任总统迪尔玛·罗塞夫在联合国大会上呼吁其他国家切断与美国互联网的联系，发展自己的技术和治理结构^②。2020年欧盟委员会同样强调了由各国自己独立监督DNS服务能力的必要性：“欧洲的个人和组织越来越多地依赖非欧盟实体运行的一些公共DNS解析器……这使得解析过程本身在发生影响主要提供者的重大事件时变得脆弱，并使欧盟当局更难处理可能的恶意网络攻击以及重大地缘政治和技术事件。”^③由此可见，美国对根域名的独家主管，使得各国在数字空间的主权得不到自主控制。

从结构上看，域名解析呈“自顶向下”的结构，整个解析过程的“要塞”在于根域名解析服务器，位于美国的主根域名解析服务器则具有使一个国家互联网瘫痪的能力。这不仅剥夺了其他国家互不干涉他国网络空间管理事务的主权独立，对于非美国之外的国家而言还存在着“消失性风险”“致盲性风险”和“孤立性风险”^④，即一国网络空间或网络资源受到封锁、屏蔽或隔离。美国也确实付诸了行动，如在伊拉克战争、利比亚事件以及俄乌冲突期间，通过停止或干扰域名解析对他国进行网络攻击，拓展自身在数字空间的殖民霸权，将全球数字空间变成其可以肆意操控的“数字版图”。

2. 掠夺数据资源：攫取数字红利扩大全球“数据势差”

历史上的殖民主义，土地与自然资源被殖民者从当地人手中夺走，为殖民者的经济建设提供空间和原材料。数据不仅仅是数据殖民主义的原材料，还能够转化为资本、劳动力，成为美国剥削、垄断的关键对象。当前，美国政府主要通过两种方式垄断数据，巩固其殖民权力。第一，借助其本国企业垄断数据，并限制他国获取或使用这些数据。美国的数据企业在全世界数字市场中占据着最大份额^⑤，美国政府与其本国数据巨头签订“零成本合同”采购最先进的数字服务，同时限制这些数据巨头与他国政府的合作，“控制通往数字空间的通道”^⑥，制约他国数字创新发展空间。此类行为是数据殖民主义控制资源流通的典型方式，其本质在于通过控制数据传输渠道，确保美国在数据资源的获取与分配中占据主导地位，从而构筑起一种结构性的数据优势。其他国家因此难以打破这种不平等的数据流通格局，进而陷入数据资源获取与利用的劣势之中。第二，通过强制收购他国数据企业，获取他国企业宝贵的数据资源。以美国政府对TikTok采取的系列措施为例，2020年7月至8月，特朗普政府接连两次签署行政令，禁止美国机构与TikTok交易；2024年3月，美国国会众议院以TikTok收集了过量数据、TikTok可能被中国政府利用来监视用户等借口通过《保护美国人免受外国对手控制的应用程序法案》（即“剥离法案”），要求字节跳动公司在6个月内剥离TikTok，否则将禁用TikTok。TikTok事件凸显出美国无视TikTok在数据安全上的努力和成果，通过政治手段强行打破正常的市场竞争规则，以莫须有的“国家安全威胁”为由进行粗暴干涉，试图将他国企业积累的数据资源据为己有，是典型的殖民主义做派。

以上两种美国垄断数据的方式共同折射了数据殖民主义所带来的深层危害，即数字革命不仅没有形成相互受益的权力格局，反而使现实不平衡的权力结构得到巩固，加剧了数字空间的两极分化，形成了严峻的“数据势差”。处于“高位势”的“数据强国”利用其数据平台、科技企业攫取“低

① 参见陈春彦：《连线与断网：俄罗斯互联网国家治理研究》，北京：北京大学出版社，2022年，第37页。

② 参见[加拿大]泰勒·欧文：《技术与权力》，孟彦莉等译，北京：中信出版社，2023年，第195页。

③ “The EU’s Cybersecurity Strategy for the Digital Decade”，<https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0>。

④ 方滨兴主编：《论网络空间主权》，北京：科学出版社，2017年，第300-301页。

⑤ 参见刘妍、冉从敬：《中美欧“泛数据主权”竞争格局及中国应对——基于数字堆栈模型》，《中国科学院院刊》2024年第12期。

⑥ 胡莹：《数字帝国主义视阈下美国的数字霸权批判》，《马克思主义研究》2023年第11期。

位势”的“数据弱国”的数据资源与经济利益，利用其国内法的溢出效应遏制他国数字创新发展，致使以美国为核心的“数据强国”越来越富，以众多发展中国家为代表的“数据弱国”越来越贫。“数据势差”的形成与深化，将使得美国在数字空间的殖民统治秩序愈加坚固，全球绝大部分数字红利向美国集中积累，美国将牢牢掌握数据产业价值链的高端环节，把握数据的定价权与规则的制定权，而其他国家将被迫长期处于价值链的低端，从事数据采集、简单数据标注等低附加值工作，成为美国数字市场的附庸。

3. 主导数字技术：控制技术传播加深全球“技术鸿沟”

技术与殖民主义的辩证关系不仅在历史上有迹可循，在如今的数字时代依然存在。历史上的殖民主义，殖民者使用地图和人口普查等实用技术来监视和控制土著人民；数据殖民主义中，美国同样使用技术对他国开展情报、监视和侦察行动。如同马克思指出的，“指南针打开了世界市场并建立了殖民地”^①，数字技术现已成为美国资本主义建立数据殖民地的新杠杆和手段。

历史上的殖民主义国家通过最大限度地延长落后国家工业化的过程，限制和阻碍落后国家的技术发展，从而巩固其殖民统治；当今，美国则依托其数字技术优势，有意识地调控他国技术发展进程，不断加深全球“技术鸿沟”，进而确立其在数字领域的技术霸权地位。这种技术支配策略在通信领域表现得尤为显著：美国不仅严格控制关键数字技术的全球扩散速度，还通过构建排他性的法律制度和政策框架，为这种新型殖民主义提供制度性保障。其手段之一是通过限制技术许可，控制特定技术的传播和应用。例如，2024年5月7日，拜登政府撤销了高通4G SOC及英特尔、AMD的个人电脑及平板X86架构CPU对华为的供货许可，冲击了华为的个人电脑和平板业务。手段之二是通过限制企业合作，强化技术壁垒。美国对数据企业的歧视性监管不仅影响了企业自主经营权，更使其在国际合作中不得不屈从于美国的意志。2022年8月美国出台的《芯片与科学法案》明确规定，获得美国政府补贴和税收减免的厂商需承诺，十年内不得在中国开展任何使半导体生产能力发生实质性扩张的重大交易，否则需全额退还联邦补贴及减免的税收。此外，美国半导体鼓励政策明确将“中国大陆控制的企业”排除在受益范围之外。除通信领域外，在人工智能领域同样对中国不断“卡脖子”。当前全球AI算力芯片市场仍由英伟达垄断，其最强大CPU之一A100在美国法律限制下不能向中国出售。2025年1月，中国大模型初创公司智谱及其子公司首次被纳入美国实体清单。若美国这些技术限制措施进一步加深、扩大，许多国家都将在很长一段时间被笼罩在美国的“算力霸权”中，难以快速取得技术上的突破。

美国这些技术封锁措施是典型的殖民行径，即试图通过“技术隔离”来限制一国技术对另一国技术知识的外溢，在全球技术格局中形成“技术高地”与“技术洼地”的鲜明落差，加深全球“技术鸿沟”，以实现美国对全球数字技术发展节奏的把控，让其他国家在技术发展上长期依附美国。

4. 垄断数字市场：构筑贸易壁垒加剧他国“数字依赖”

市场垄断在殖民主义历史上具有极其重要的意义，它不仅是殖民主义实现经济剥削的重要手段，也为殖民主义的文化渗透创造了条件。历史上，欧洲列强通过建立东印度公司等贸易垄断公司对殖民地的市场进行严格控制。当今，美国数据殖民主义遵循了类似的市场垄断逻辑，通过加深他国对美国的“数字依赖”建构起一种不平等贸易关系，以维持自身霸权以及对他的控制。

第一，借助本国数据企业的资本扩张，加深他国对美国的数字市场依赖。马克思恩格斯在《共产党宣言》中写道：“不断扩大产品销路的需要，驱使资产阶级奔走于全球各地。它必须到处落户，到

^① 《马克思恩格斯文集》第8卷，北京：人民出版社，2009年，第338页。

处开发，到处建立联系。”^① 美国在数字空间奔走的过程中，造就了一大批全球垄断企业，如生产路由器和服务器的思科公司、生产计算机芯片的英特尔公司、生产软件的微软公司、生产个人电脑的戴尔公司、IBM公司和苹果公司。这些美国数据企业通过技术封锁、专利壁垒和品牌营销手段，不断在全球各地拓展业务，建立生产基地、研发中心和销售网络，将全球数字市场纳入掌控范围，进一步巩固了美国在全球数字市场的霸主地位，也使得其他国家陷入对美国所生产商品的深度依赖。

第二，设置不平等的数据贸易规则，维护美国在数字市场的垄断地位。从多边条约来看，美国推动制定了一系列数字贸易协定，如《美墨加协定》，这些协定中涉及数字经济的规则往往更有利于美国企业，比如关于知识产权保护和数字服务税等方面的规定。从单边法律来看，美国政府近两年对数据市场的治理采取了日益严格的方法，国际著名互联网治理学者弥尔顿·穆勒将这种现象称作“数字新重商主义”。通过统计2000—2021年中美在互联网和数据平台市场的贸易情况，弥尔顿·穆勒等人发现，自2009年起，美国开始限制中国企业在美国市场的经济行为，对华为、TikTok、WeChat的歧视性监管就是例证^②。

我们看到，冷战后的大国博弈已从地缘政治转向地缘经济，权力的来源越来越体现为对市场的控制，而不仅仅是对领土和军事力量的控制。以美国田纳西大学著名法学教授莫里斯·斯图克有关“大数据竞争”的论断来形容美国在数据市场的殖民霸权行径可谓恰如其分：在巨大的数据优势下，美国相比其他国家拥有一套独一无二的雷达系统，能够在竞争威胁起飞之时就对其飞行路线进行远距离追踪，并将之拦截或击落。

三、美国数据殖民主义的崭新特征

虽不似历史上的殖民主义那般血腥，但美国数据殖民主义仍表现出内在的不可抗拒性、强制性，且体现了殖民主义在大数据时代的崭新特征。

1. 数字技术成为新的殖民理性

美国数据殖民主义的实践逻辑揭示，其对数字技术的野心已经取代了历史上的殖民主义各国对领土展开的竞争，数字技术也因此成了数据殖民者新的殖民理性。一方面，数字技术的广泛传播应用产生了新的殖民意识形态。技术在人类事务中占据着越来越重要的地位，这与我们正在经历的人工智能革命交织在一起，形成了一种技术决定论。在数据殖民情境中，技术决定论本质上采取了与《圣经》服务历史上的殖民主义控制思想传播的相同路径——信息和通信技术是人类唯一的命运，只有温顺的使用者才能融入网络社会^③。美国则利用这一论调，通过“数字启蒙”的形式，将“文明”国家的技术优势转化为对“落后”国家的控制手段。例如，伴随着美国数据企业在全球的广泛普及，其背后所蕴含的个人主义、消费主义等价值观念，通过海量的信息传播、技术扩散潜移默化地影响着他国人民的思想与行为，并逐渐侵蚀他们本土文化与价值观的认同，进而在思想层面实现对他国的殖民控制。另一方面，数字技术也已经成为新的殖民力量。正如阿贝巴·柏哈尼所指出的：“传统殖民主义是由政治和政府力量驱动的，而人工智能时代的殖民主义则采取‘最先进的算

① 《马克思恩格斯文集》第2卷，北京：人民出版社，2009年，第35页。

② Milton L. Mueller and Karim Farhat, “Regulation of Platform Market Access by the United States and China: Neo-mercantilism in Digital Services”, *Policy & Internet*, Vol. 14, No. 2, 2022.

③ Petar Jandrić and Ana Kuzmanić, “Digital Postcolonialism”, *IADIS International Journal on WWW/Internet*, Vol. 13, No. 2, 2015.

法’和‘人工智能驱动的解决方案’来解决社会问题。”^①这种殖民主义的核心不在于掠夺手段的暴力性，而在于其世界观，即极少数拥有先进数字技术的人理所当然地拥有全球主导权。

2. 规则成为殖民者的辅助工具

历史上的殖民主义，规则往往建立在武力征服之后，殖民者通过在殖民地建立规范制度维护殖民统治秩序。而美国进行数据殖民的非常突出的一个特征在于，美国在法律制度、技术标准上的领先话语权便利了其殖民过程，规则成为“探索”数据殖民主义的隐蔽而又强大的辅助工具。一方面，美国凭借其强大的影响力，影响着国际数据立法，使许多国家在数据立法取向上服务于美国国家利益。例如，在国际数据跨境流动规则方面，美国一开始倡导“数据自由”，呼吁“网络无边界”，在一些国际数据合作框架讨论中，主张降低数据跨境流动的限制条件，并在多份报告中引导国际社会谴责对数据跨境流动施加本地化条件的国家，意在使各国数据更大程度地汇聚到美国本土。而在部分国家的通信技术崛起时，美国又开始部分限制自由流动，针对“受关注国家”开启“数据脱钩”，带领盟国在数据流动互操作上孤立俄罗斯、中国、伊朗、朝鲜、委内瑞拉等国。这也正是美国“制度帝国主义”^②的体现，即在国际贸易中拥有强大经济和政治实力的一方，利用其优势将本国利益制度化并纳入国际贸易规则体系，从而彰显霸权。另一方面，美国通过长臂管辖跨境执法，令全球为其本国利益添砖加瓦。例如，《美国反海外腐败法》允许美国政府对其他国家的企业和相关机构进行调查、制裁，允许美国政府随意逮捕一个公司的任何一名员工，不论何时何地。2014年，美国利用这一法律强制法国能源巨头阿尔斯通将所有能源业务出售给作为其主要竞争对手的美国通用电气公司^③。2018年发生的“孟晚舟事件”实则是美国想要故技重施，只是我国在后续的司法与行政的应对中保持足够的警惕，其图谋才没有得逞。即便特朗普上台后，于2025年2月暂停实施《美国反海外腐败法》，但美国殖民霸权思维仍体现在诸多其他法律与实践之中。

3. 数据平台成为殖民化的共谋

无论是历史上的殖民主义还是数据殖民主义，国家与企业之间都存在着广泛合作。历史上进行殖民的君主制国家授权的公司（如英国南非公司）是为殖民开采而设立的特殊用途工具。如今，数据殖民主义是国家权力与商业更为复杂的混合，企业在与民族国家及其政府建立复杂联盟方面发挥了更为重要的作用^④。美国的数据平台与数字资本牵引着数字市场的发展，一旦数据开始流动，就会被资本化^⑤，成为美国数据殖民主义下资本积累与增殖的资源 and 工具。在美国政府与数据平台的深度合作下，一种由数据平台参与推动的新的殖民秩序正在逐步建立。正如贝茨学院保罗·奥比所形容的：“美国硅谷的数据平台既传播资本主义，又挖掘殖民主义，同时在同一过程中建立起经济二元对立和不平等。”^⑥鉴于数据平台在数据、技术与算法方面的强大优势，这一新的殖民秩序不仅将延续历史上的殖民主义的剥削与压迫，还将通过与国家权力的结合、对用户数据的深度挖掘利用以及多边市场的构建，进一步加剧全球数据资源分配的不平等，将数据殖民主义推向新的高度。

① Abeba Birhane, “Algorithmic Colonization of Africa”, *SCRIPTed*, Vol. 17, Issue. 2, 2020.

② Zerui Zhao, “The Dilemma of Cross-Border Data Flow and the Construction of Mutual Trust Platform in Asia”, *Asian Journal of Law and Society*, Vol. 11, No. 1, 2024.

③ 参见〔法〕弗雷德里克·皮耶鲁齐、马修·阿伦：《美国陷阱》，法意译，北京：中信出版社，2019年，第177页。

④ Ulises A. Mejias and Nick Couldry, *Data Grab: The New Colonialism of Big Tech and How to Fight Back*, Chicago: The University of Chicago Press, 2024, p. 18.

⑤ 参见蓝江：《如何思考全球数字资本主义？》，上海：上海人民出版社，2024年，第206页。

⑥ Paul A. Obi, “Labouring and Smiling: Re-Imagining Digital Colonialism in Africa, Silicon Valley Big Techs, and the Politics of Prosumer Capitalism in Nigeria”, *tripleC: Communication, Capitalism & Critique*, Vol. 22, No. 1, 2024.

4. 主权国家同样沦为被殖民者

历史上，被殖民国家不能够独立自主地处理国内国际事务，即缺乏完整的主权。当下情况发生了显著变化，即便拥有完整主权的国家也可能遭遇显性的或隐性的殖民统治。如果说历史上的殖民主义是一种凭借强权剥夺他国政治独立进而开展直接统治的方式，那么数据殖民主义就是一种不强求政治控制但一定获取经济控制或剥削的间接统治方式。帝国主义“在承认殖民地政治独立的同时，采取代理人制度、经济援助、军事援助、不平等贸易、文化侵略、科技垄断、跨国公司等手段，在经济上继续殖民落后国家，使其充当商品市场、原料产地和投资场所，最大限度地榨取财富”^①。现在许多主权国家虽然在政治上不受美国直接的控制，但在技术、市场上深度依赖美国，无法获得真正的独立和发展。而且，美国对主权国家的数据殖民范围是相当广泛的，有学者绘制了美国基于“依附性差序圈层”的数据劫掠体系，以美国为中心区，五眼联盟、欧盟及北约国家、日本与印度等亚太国家、中国与俄罗斯等南方国家都在美国的数据掠夺圈层内^②。可见，美国的数据殖民主义不以直接的政治失序为代价，而以一种新颖的方式构建了空间尺度和社会群体之间的不平等，并通过分类、等级化和排斥三种机制巩固了这种不平等^③，任何主权国家都受到了程度不一的剥削。

四、防范数据殖民主义的可行方案

面对世界百年未有之大变局加速演进，在实现中华民族伟大复兴的宏伟目标之际，我国应当警惕美国的数据殖民主义，采取必要措施应对数字空间的霸权行为及殖民行径，保障国家富强、民族振兴与人民幸福的全面愿景得以实现；应当承担起网络空间负责任大国责任，构建起反美国数据殖民的主权安全防线和民族尊严防线，提供反数据殖民的中国样本，维护国际数字社会的和平与稳定。

1. 建立完善有效的数据主权法律框架

主权的确立向来被视作去殖民化的标志，如冷战期间的去殖民化意味着争取第三世界的解放，成功后则形成宣称拥有主权的民族国家^④。虽然数据殖民不以直接侵蚀民族国家的主权统治为目的，但数据主权仍然是国家在数字空间生存的生命线，正如欧盟与非盟强调的，数据主权是国家在数字世界独立行使的能力^⑤，能够使本国成为全球经济中的生产者，而不只是消费者^⑥。数据主权也是对抗数据殖民主义的一种有效制度^⑦，以至于印度等发展中国家将对公民数据和数据基础设施的主权主张，视为对抗西方数据殖民主义掠夺印度数据资源的唯一解药^⑧。因此，捍卫国家在数字空间的主权，建立完善的数据主权法律框架并保证数据主权规则得以落地实施，是防范数据殖民主义的根本要求。

我国虽尚未对数据主权相关问题作出统一制度安排，但维护国家数据主权及其安全的思想已散见于一些重要战略性文件中。譬如，《国家网络空间安全战略》与《网络空间国际合作战略》两份

① 李梅敬：《资本逻辑下的“数据殖民”风险及数字中国建设》，《理论月刊》2021年第10期。

② 参见何渊、王源主编：《欧盟人工智能法合规手册》，北京：北京大学出版社，2024年，第7页。

③ Surinder S. Jodhka and Boike Rehbein (eds.), *Global Handbook of Inequality*, Cham: Springer, 2024, pp. 794-797.

④ Walter D. Mignolo and Catherine E. Walsh, *On Decoloniality: Concepts, Analytics, Praxis*, Durham: Duke University Press, 2018, p. 5.

⑤ European Parliament, “Digital Sovereignty for Europe”, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI\(2020\)651992_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf).

⑥ African Union, “The Digital Transformation Strategy for Africa (2020-2030)”, <https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030>.

⑦ Renata Ávila Pinto, “Digital Sovereignty or Digital Colonialism? New Tensions of Privacy, Security and National Policies”, *International Journal of Human Rights*, Vol. 15, No. 27, 2018.

⑧ Steven Feldstein (ed.), *New Digital Dilemmas: Resisting Autocrats, Navigating Geopolitics, Confronting Platforms*, Washington: Carnegie Endowment for International Peace, 2023, p. 21.

文件均强调维护国家在网络空间的主权。《中国关于全球数字治理有关问题的立场》指出国家主权原则应适用于网络和数字空间，则是对数据主权的直接承认。我国应当在此基础上继承发展，建立完善的数据主权法律框架，为保障数字空间国家主权与安全、防范数据殖民主义的规则入侵提供坚实的制度支撑。

首先，应当提高数据主权的立法位阶，出台一部具有更高效力的行政法规，统领数据主权实践的关键场景，完成对本国数据资源的有效管辖。可以将成熟的政策尽快上升为法律制度，把看得准的方向及时确定为法律原则^①，对数据出境、数据入境、数据本地化、数据跨境执法、国内数据法的域外适用、数据安全审查与风险评估、数据分类分级、国际数据合作等重点内容作全局性规定，统筹国内法治与涉外法治，实现数据流动和安全保障的统一。其次，应当配套实施细则，强化主权制度的可操作性。例如，可以明确数据分级标准并匹配不同的跨境数据监管方式，参考《金融数据安全 数据安全分级指南》将数据安全级别从高到低划分为1至5级的分级思路，综合考量安全级别、影响对象和程度等因素，提供一套区分不同安全等级的数据跨境监管方式，为分类分级制度提供可落地的操作指南，加强数据跨境监管规则的落地性。最后，完善反制措施回应他国歧视性贸易规则，对抗美国长臂管辖。可以适当扩大《阻断外国法律与措施不当域外适用办法》和《中华人民共和国反外国制裁法》的适用范围与对象。我国目前的规定适用于“不当禁止或限制中国与第三国（地区）进行正常经贸活动”的情形，应当将我国企业和个人也纳入保护范围。除经贸活动外，还应将更多类型的歧视性贸易制裁如经济制裁、金融制裁、科技封锁等纳入阻断法体系。

2. 塑造自主可控的数字技术创新能力

技术的强大从来都是颠覆国际格局的关键力量，技术的自主则一直是改变国际权力平衡的最主要方式。虽然在发达资本主义国家数字技术现已被资本裹挟并与之形成“同盟”，服务于资本的逐利逻辑，强化着数字资本主义的剥削体系，但正如马克思所言：“机器本身对于工人从生活资料中‘游离’出来是没有责任的……矛盾和对抗不是从机器本身产生的，而是从机器的资本主义应用产生的！”^②因而，数字技术本非数字资本主义剥削市场、影响国家公权力的原罪，其背后的资本家、殖民者才是激发矛盾的元凶。抵制数据殖民最关键的仍然在于技术革新，塑造自主可控的数字技术以减轻对美国的依赖，将是去数据殖民化最有力的途径。

近些年，俄罗斯将其在数字技术方面的自主创新追求称为“去美国化”，即去除美国等发达国家的绝对控制地位。然而，“去美国化”与“网络中立”同样属于听起来很美妙但真正实施起来困难重重的设想^③。因此，在数字技术的创新探索中，不必将地缘政治过度带入，而应当重点关注技术本身的进步，以促进本国数字技术高度自主为目的，突破他国技术封锁重围实现基本自主。

首先，我国应当关注技术制造全流程，实现供应链自主。这既要通过收购与合作等纵向整合的方式，构建自主完整的产业链，涵盖从原材料到终端产品的各个环节，降低对国外供应链的依赖；又要通过横向合作、培育本土供应商、加强与国际供应商的合作与竞争等方式构建多元化的供应链网络，在重要领域和关键环节建立自主可控的供应链体系。其次，应当改变美国通过控制根区DNS以控制全球数字版图的现状，打造安全独立的主权域名系统，将数字疆域的安全牢牢掌握在自己手中。鉴于互联网正由IPv4向IPv6演进升级，我国应当加强IPv6关键技术的研发和相关技术标准的研制，提前布局新型网络体系结构与IPv6安全可信技术，推动建立以联合国为主导的IPv6地址分

① 参见李爱君、于施洋：《论数据治理》，北京：法律出版社，2024年，第20页。

② 《马克思恩格斯文集》第5卷，北京：人民出版社，2009年，第508页。

③ 参见陈春彦：《连线与断网：俄罗斯互联网国家治理研究》，北京：北京大学出版社，2022年，第406页。

配、互联网域名管理机制，促进下一代互联网国际治理秩序由当前西方主导、美国实控的、影响其他国家主权独立性的模式，向由联合国主导的、保证各国主权独立平等的模式转变，在世界范围内实现各国域名系统的安全。

3. 构建安全互信的区域数字经济业态

不同国家数字经济的协同发展是抵御外部数据霸权、实现内部数据资源优化配置的重要途径。在美国数据平台一家独大并导致其他国家对其产生深深的依附性时，构建安全互信的国际数字经济业态、增强国家之间的数据合作，可以在一定程度上突破美国的限制，在提升整体数字竞争力的同时防范数据殖民主义的渗透。当然，在全球数据治理阵营相对未统一的背景下，期待一种各国均参与其中的、全球法样态的规范性合作协议仍将任重道远，因而，我国可在区域合作中发力，探索有效的双边、多边合作模式。

当前最为可行的方式包括，第一，巩固现有“朋友圈”，在“一带一路”共建国家落实数字经济领域的安全互信合作。数字合作在近十年来是“一带一路”共建国家关注的重点，未来的工作应进一步加强务实合作，强化独立、平等、互相尊重的数据主权主张，借鉴《中阿数据安全合作倡议》《“中国+中亚五国”数据安全合作倡议》等成熟经验，推动数字经济合作的深入开展。以非洲国家为例，在技术合作上，要充分发挥中国科技公司的作用，鼓励中企扩大和优化对非投资，在“非洲创新创业之都”阿尔及利亚广泛开展业务合作，支持中非企业深度联合攻克数字基础技术。在市场合作上，则可借鉴 Kilimall、Kikuu、Amanbo 和 Tospino 等中方跨境电商的成功经验，培育更多面向非洲的“数据企业名片”，供需对接提高非洲数字化技术能力、培育非洲数字创新生态系统。同时，依托“塞内加尔国家数据中心”等中非合作建设的数据平台共同在国际社会发声，维护共同利益、共谋发展合作。第二，拓展新的合作关系，与德法等欧盟国家就网络安全、数据跨境等议题达成更深层次的合作。基于2019年中欧领导人会晤时发表的联合声明，持续巩固双方在网络空间合作上达成的共识，利用“亚欧会议”“欧亚经济论坛”等多边机制，深化中欧在网络规则方面的对话，强化网络安全、数据保护以及人工智能等领域的合作。同时，以2024年6月签订的《关于中德数据跨境流动合作的谅解备忘录》为推进点，促进中德网络交流合作取得更多成果。加速构建“中德数据政策法规交流”对话机制，加强在数据跨境流动议题上的交流，以德国和法国为突破口，制定中德、中欧的双边数据跨境流动协议，实现相关组织之间的数据自由流动，使中德合作效应蔓延至其他欧盟国家，达成中欧数据跨境自由流动的长期伙伴关系。

4. 培育公平正义的全球数字人文生态

在建立制度、创新技术、发展市场等基础上，我们仍需要明白，获取技术、投资或融入全球市场并不会改变世界贸易中的结构性权力失衡状况，贫穷国家之所以贫穷，是殖民和压迫等历史因素造成的结果^①。各国要想彻底摆脱贫穷，在社会文化上应当有所升华。应抛弃一切形式的殖民主义，废除精神与物质的剥削，将数字空间的国家行动修订为以公平正义为主导的，而不是以掠夺剥削为主导的行为模式。这种诉求呼唤向上向善的数字空间生态建设，呼唤公平正义的、独立平等的、包容可持续的数字伦理与数字人文。

首先，需要推动全球数据治理的民主化，重申“以国际法为基础的国际秩序”，支持联合国在全球数据治理和数据安全保障中发挥更大作用，以联合国《全球数字契约》为指引，坚持“为所有

^① Azadeh Akbari and Silvia Masiero (eds.), *Critical ICT4D (Information and Communication Technologies for Development)*, Oxford: Taylor & Francis, 2025, p. 16.

人创造一个包容、开放、可持续、公平、安全和可靠的数字未来”^①。在关键技术标准的设立、关键通信技术的管理方面，应当由联合国主导开展，使世界各国均有参与数字空间重大决策的机会。例如，对于全球 DNS 由美国独家管理的问题，可以建议由联合国主导建设一个 DNS 管理联盟，将 ICANN 的职权全部转移到国际电信联盟或联合国信息安全政府专家组、开放式工作组等联合国平台统一管理与分配。其次，应着力推动数字技术的全球普惠性传播，取消先进技术使用与获取的藩篱。如前所述，美国通过出口管制和技术传播速度的刻意调控，严重制约了发展中国家的数字技术发展进程。我国应倡导建立公平、开放的技术合作机制，搭建更多全球性的数字技术合作平台，可将我国在数字技术基础设施建设领域积累的成熟标准和规范与国际社会共享，汇聚全球智慧与资源，共同设计并实施基于数字公共产品和数字基础设施的可持续发展解决方案。最后，需要引导数据平台等组织、人工智能等技术的向善发展。虽然美国通过数据平台加速了资本积累，但平台不应被妖魔化为殖民主义的生产者，在合理的使用与引导下，平台可能构成应对殖民主义的手段^②。为了确保这些新兴技术的“善意”使用，国际社会需要共同制定和推广符合全人类共同价值的数字伦理，加强对人工智能系统透明度和可解释性的监管，确保人工智能决策不被滥用，不受单一利益集团的操控。

结 语

以资源掠夺、市场垄断和财富霸占为核心特征的殖民主义从未结束，而是随着时代的变迁、人类生产工具的革新而嬗变。在大数据时代，美国数据殖民主义以其复杂而隐蔽的多重逻辑，深刻影响着全球数字生态、经济格局与主权安全。需要以史为鉴，直面任何形式的殖民主义可能对我国乃至全球安全与发展产生的威胁。国际社会的数字化转型之路已历经不少春秋，数字空间的未来发展充满着难以预见的机遇与挑战。唯一可以肯定的是，我们不能让数字空间成为新的殖民战场，而应使之成为促进各国社会、文化和经济共同繁荣的广阔舞台。我国应继续发挥大国担当，在国际数字舞台上积极发声，贡献更多中国智慧与中国方案，引领全球数字空间朝着更加公平、安全、繁荣的方向发展，打破美国数据殖民主义的桎梏，为推动构建人类命运共同体的数字篇章添砖加瓦，迈向更加美好的数字社会。

参考文献：

- [1] 冉从敬：《数据主权论纲：权利体系与规制进路》，北京：科学出版社，2023年。
- [2] 夏少光：《毛泽东反对新殖民主义的探索与启示》，《马克思主义与现实》2025年第1期。
- [3] 胡莹：《数字帝国主义视阈下美国的数字霸权批判》，《马克思主义研究》2023年第11期。
- [4] 黄其松：《数字时代的国家理论》，《中国社会科学》2022年第10期。
- [5] 刘贵祥：《历史唯物主义视阈中数字资本的异化及其扬弃》，《马克思主义研究》2022年第6期。
- [6] 常江、田浩：《尼克·库尔德利：数据殖民主义是殖民主义的最新阶段——马克思主义与数字文化批判》，《新闻界》2020年第2期。

(编辑：张 剑)

① 联合国：《全球数字契约》，<https://www.un.org/zh/documents/treaty/A-RES-79-1-Annex-I>。

② Dimitra Petrakaki, Petros Chamakiotis and Daniel Curto-Millet, “From ‘Making Up’ Professionals to Epistemic Colonialism: Digital Health Platforms in the Global South”, *Social Science & Medicine*, Vol. 321, 2023.