“主权人工智能”在“全球南方”的兴起及中国的合作应对*

张书言　陈志敏

【内容提要】“主权人工智能”是国家主导的人工智能治理实践：对内依托主权的“最高性”实现产业发展和安全风险的平衡；对外凭借主权的“独立性”追求战略自主和国际影响力。这一概念的理论内涵与人工智能技术特性密切相关：快速迭代性和不可控性要求国家需在技术安全问题上确立主体性地位；技术的通用性特点意味着国家权力需对人工智能多安全领域加以统筹；技术要素的跨国流动性使“主权人工智能”追求开放性战略自主。为避免技术标准和治理规则被垄断，“主权人工智能”需争取国际话语权以实现国际秩序的多样性价值。当前，不少全球南方国家正在通过这一战略回应人工智能发展中“技术要素不健全”“安全风险敏感”“结构性不平等”和“治理话语权失衡”等风险制约。巴西和印度尼西亚的案例表明，“主权人工智能”对全球南方国家实现技术自主、保障国家安全以及提升话语权具有积极作用。作为“全球南方”的天然成员，中国秉持平等共赢的合作理念，推动“开源战略和本地化部署结合”的能力建设模式，团结全球南方国家不断提升治理参与度和话语权。

【关键词】主权；人工智能；国家安全；全球南方；技术治理

【作者简介】张书言，复旦大学国际关系与公共事务学院博士研究生、全球人工智能创新治理中心研究助理；陈志敏，复旦大学国际关系与公共事务学院教授、全球人工智能创新治理中心执行主任（上海 邮编：200433）。

【DOI】10.14093/j.cnki.cn10-1132/d.2026.03.005

【中图分类号】D815；TP18　【文献标识码】A　【文章编号】2095-574X（2026）03-0104-29

* 作者感谢《国际安全研究》编辑部与匿名审稿专家的意见和建议，感谢姚旭副研究员、杨昭博士的支持与帮助，文责自负。

2024 年 2 月，在迪拜举行的世界政府峰会上，英伟达首席执行官黄仁勋（Jensen Huang）系统阐释了“主权人工智能”（sovereign AI）概念，提倡各国发展“利用本国基础设施、数据、劳动力和商业网络生产人工智能的能力”，从而拥有自主人工智能产品，将本国的语言和文化编入到大语言模型的开发中。① 事实上，自 2022 年生成式人工智能技术爆发以来，这一理念就已经受到不少国家的关注。法国将人工智能技术与国家的工业及数字主权挂钩，设立“生成式人工智能委员会”；印度电子和信息技术国务部长拉吉夫·钱德拉塞卡尔（Rajeev Chandrasekhar）曾公开表示，政府已经采取行动“打造属于自己的‘主权人工智能’”；② 巴西政府颁布了《人工智能计划 2024—2028》（*PBIA 2024—2028*），将算法、数据、计算能力、教育、电力和网络安全确立为其“主权人工智能”的六大关键要素。③ 此外，肯尼亚、泰国、印度尼西亚等国也在竞相研发基于本国语言的生成式人工智能产品。④

英伟达力推的“主权人工智能”概念，与各国提出的“主权人工智能”计划之间存在一定差异。英伟达的倡议偏重于人工智能的发展方向，即由跨国公司向主权国家提供 A100、H200、B200 等先进算力芯片，助力主权国家提升人工智能的技术能力。这本质上是服务于科技公司进一步拓宽国际市场、打开芯片和显卡销路的商业目的。就各国政府而言，“主权人工智能”计划既要解决技术能力层面的“发展问题”，也需要应对人工智能在政治、社会、经济、文化各领域带来的“安全问题”，这是主权国家统筹数据、算力、资金、人才等一系列要素，平衡“创新—监管”光

① Brian Caulfield, “NVIDIA CEO: Every Country Needs Sovereign AI,” NVIDA, February 12, 2024, https://blogs.nvidia.com/blog/world-governments-summit/; Angie Lee, “What Is Sovereign AI?” NVIDA, February 28, 2024, https://blogs.nvidia.com/blog/what-is-sovereign-ai/.

② Soumyarendra Barik, “India Is Building Its Own ‘sovereign AI’. What Does It Mean?” *Indian Express*, December 1, 2023, https://indianexpress.com/article/explained/explained-sci-tech/india-sovereign-ai-meaning-9048436/.

③ Luca Belli, “To Get Its AI Foothold, Brazil Needs to Apply the Key AI Sovereignty Enablers (KASE),” in Steven Feldstein, ed., *New Digital Dilemmas: Resisting Autocrats, Navigating Geopolitics, Confronting Platforms,* Washington, D.C.: Carnegie Endowment for International Peace, 2023; Germano Johansson Neto, Viviane Farias da Costa and Walter Britto Gaspar, “Brazil’s Artificial Intelligence Plan (PBIA) of 2024: Enabler of AI Sovereignty?” *The African Journal of Information and Communication (AJIC)*, Vol. 34, 2024.

④《多国看重“主权人工智能”竞相研发本地语言产品》，新华网，2024 年 2 月 5 日，https://www.news.cn/tech/20240205/093f34b6352d4a24ad4f14f5a33eb5e1/c.html; Fredrick Ogenga and Aaron Stanley, “Regulating Artificial Intelligence in Africa: Strategies and Insights from Kenya, Ghana, and the African Union,” Wilson Center, September 18, 2024, https://www.wilsoncenter.org/blog-post/regulating-artificial-intelligence-africa-strategies-and-insights-kenya-ghana-and-african。

谱的战略实践。首先，本文从主权国家的立场出发，梳理“主权人工智能”的学理内涵。其次，分析全球南方国家构建“主权人工智能”的实践特色。最后，讨论中国面向“全球南方”“主权人工智能”的国际合作路径。

一 “主权人工智能”的学理逻辑

当前，国内外学界已有不少关于人工智能治理“主权”问题的研究。有学者提出“人工智能主权”（AI sovereignty），强调政府对人工智能技术的开发、部署与治理享有至高无上的权力。[①] 然而，“主权人工智能”和“人工智能主权”在理论定位上仍存在不小的差异。

“人工智能主权”是一个规范性法理概念，其核心在于探讨国家对其领土范围内人工智能系统及其相关数据流享有最高权威。这一概念延续了传统主权理论关于“最高权威”和“领土管辖”等核心要素的观点，强调国家在人工智能技术领域中应然的“权利主张”。所以，“人工智能主权”是“技术主权”的子类，与“网络主权”“数据主权”“数字主权”有着相同的法理学基础。[②]“主权人工智能”则是一个具有实践属性的政策概念，核心在于描述国家为实现人工智能领域的自主可控所采取的一系列技术、产业和制度安排，是国家在实然层面的具体实践。这一概念主要突出“能力建设”和“实践自主”，关注国家“能够做什么”以实现技术上的战略自主，而不仅仅是国家“是否有权”规制人工智能活动。可以认为，“人工智能主权”描述了国家的战略目标，而建设“主权人工智能”则是国家实现“人工智能主权”的具体策略。[③]

本文选择以“主权人工智能”作为核心分析概念，主要基于以下三点考量：第一，更具实践性。“主权人工智能”概念直接回应了国家“如何建设”人工智能的现实问题，而非停留在国家“是否有权治理人工智能”的法理讨论，便于构建明确的分析框架并为具体的政策措施进行操作化。第二，在理论上更能反映人工智能技

① Daniel Mügge, “EU AI Sovereignty: For Whom, to What End, and to Whose Benefit?” *Journal of European Public Policy*, Vol. 31, No. 8, 2024; Chen Yu, “AI Sovereignty: Navigating the Future of International AI Governance,” PhilPapers, https://philpapers.org/archive/CHEASN-2.pdf.

② Huw Roberts, “Digital Sovereignty and Artificial Intelligence: A Normative Approach,” *Ethics and Information Technology*, Vol. 26, No. 70, 2024.

③ 相似的观点参见王天禅：《中等国家的“主权 AI”策略——基于荷兰、新加坡和韩国的比较分析》，《国际展望》2026 年第 1 期。

术与国家安全之间相互塑造的过程。目前学界已有大量分析“人工智能对国家安全带来哪些影响”的研究，[①] 但对于“国家如何回应人工智能的安全挑战”尚缺乏系统性的理论论述。本文从国家安全视角出发，探究“主权人工智能”对安全风险的回应，试图弥补已有研究的不足。第三，相较于“人工智能主权”，“主权人工智能”提供了一个更系统的分析范式。其在应然层面指向国家对内的权力，但在实然层面，国家可以通过对外的国际合作和全球治理实践来实现战略目标。因此，“主权人工智能”概念有助于揭示国家在对内和对外两个面向上的行为模式，更具统筹性。

（一）人工智能安全治理中的“国家回归”

“主权人工智能”重申了现代主权理论所强调的核心观点，即国家作为“最高权力”在处理安全问题时具有的主导性地位。对于国家作为“最高权力”的讨论可追溯至 16 世纪思想家让·博丹（Jean Bodin）所著的《主权论》。他将国家主权定义为“政治共同体拥有的绝对且永久的权力”。[②] 作为法律渊源，主权者制定法律时虽不受法律的约束，但其对神法和自然法的服从构成自身正当性的来源。[③] 主权具有“最高性”和“绝对性”，主要体现为主权拥有时间维度上的永久性和形式上的不可分割性。[④] 如果说博丹对主权的阐释是基于超越性的道德秩序，那么卡尔·施米特（Carl Schmitt）则是从关乎共同体存亡的功能性政治现实角度定义主权的“最高性”和“绝对性”。其将主权概念发展为“决断例外状态”的权力：当政体遭遇危机（社会规范失效的例外状态）时，国家拥有恢复社会秩序的决断权。[⑤] 与施米特同时期的政治哲学家沃尔特·本杰明（Walter Benjamin）以及后来的吉奥乔·阿

① 相关研究参见傅莹：《人工智能对国际关系的影响初析》，《国际政治科学》2019 年第 1 期；阙天舒、张纪腾：《人工智能时代背景下的国家安全治理：应用范式、风险识别与路径选择》，《国际安全研究》2020 年第 1 期；封帅：《国家安全学视域下的人工智能安全研究：议题网络建构的初步尝试》，《国际安全研究》2023 年第 1 期。

② 让·博丹：《主权论》，李卫海、钱俊文译，北京大学出版社 2008 年版，第 25 页；Marc Lombardo, *Critique of Sovereignty, Book 1: Contemporary Theories of Sovereignty*, Punctum Books, 2015, http://www.jstor.org/stable/jj.2354043。

③ Chris Brown, Terry Nardin and Nicholas Rengger, eds., *International Relations in Political Thought: Texts from the Ancient Greeks to the First World War*, Cambridge: Cambridge University Press, 2002; 郭逸豪：《博丹主权概念的公法属性及其中世纪基础——再论“君主不受法律约束”》，《清华法学》2024 年第 4 期。

④ 让·博丹：《主权论》，李卫海、钱俊文译，北京大学出版社 2008 年版。

⑤ 卡尔·施米特：《政治的神学》，刘小枫编，刘宗坤、吴增定等译，上海人民出版社 2015 版；武宇航、林进平：《例外状态的正当性探析——在施密特与阿甘本之间》，《国外理论动态》2023 年第 3 期。

甘本（Giorgio Agamben）也都将“例外状态”作为理论起点，分析国家作为“最高权力”的正当性。[①]

这些洞见对于理解数字时代的国家权力尤为关键：当技术变革引发的不确定性导致常规法律框架濒临失效时，国家必须借助例外状态的决断权来应对新型安全威胁。当前，人工智能技术的快速迭代性和模型自主性正在放大这种“例外状态”的风险，同时对国家作为最高权力的决断能力构成了严峻挑战。首先，人工智能技术的快速迭代性造成了显著的“治理滞后”问题。与传统技术不同，人工智能的发展呈指数级增长态势，其更新周期以月甚至以周为单位计算，而立法和监管框架的制定往往需要数年之久，这使得监管机构难以及时跟上技术发展的步伐。[②] 当新型安全威胁出现时，国家往往缺乏现成的法律工具和监管机制来有效应对，进而陷入一种事实上的“规范真空”状态，而这正是施米特所描述的“例外状态”的典型特征。其次，人工智能模型的自主能力所导致的不可控性特征，进一步削弱了国家在例外状态下的决断能力。深度学习模型的“黑箱”特性，使得即便是其设计者也难以对模型的行为进行完全预测和解释，造成了技术层面的不可解释性、组织层面的保密性以及法律层面的问责困难等三个层面的监管挑战。[③] 当系统产生有害输出时，国家不仅很难及时确定责任主体，更难以迅速采取有效决断遏制风险扩散。这种“不可控性”直接冲击了国家作为“最终决断者”的角色定位。最后，以大型科技公司为代表的非国家行为体掌握了大量数据要素与算力资源，拥有影响社会信息传播和国际规则制定的结构性权力，在一定程度上对主权国家维护经济安全、社会安全和政治安全的权威性构成了挑战。[④]

面对人工智能时代日益加剧的“例外状态”风险，以及由此导致的国家决断能力

① 瓦尔特·本雅明：《暴力批判》，王广州译，载陈永国、马海良主编：《本雅明文选》，中国社会科学出版社 1999 年版；Jan-Werner Müller, “Myth, Law and Order: Schmitt and Benjamin Read Reflections on Violence,” *History of European Ideas*, Vol. 29, No. 4, 2003；吉奥乔·阿甘本：《神圣人：至高权力与赤裸生命》，吴冠军译，中央编译出版社 2016 年版；吉奥乔·阿甘本：《例外状态》，薛熙平译，西北大学出版社 2015 年版；Francisco Naishtat, “Governance, Sovereignty and Profane Hope in a Globalised Catastrophe-World,” *Diogenes*, Vol. 57, No. 4, 2010。

② Keith M. Driver, “Predictable Progress: Constructive Autonomy and the Design of Dual-Loop Governance for AI Systems,” SSRN, 2025, http://dx.doi.org/10.2139/ssrn.5618452.

③ Simon Chesterman, “Through a Glass, Darkly: Artificial Intelligence and the Problem of Opacity,” *The American Journal of Comparative Law*, Vol. 69, No. 2, 2021.

④ 孙志伟、殷浩铖：《人工智能时代数字巨头的技术权力及其对“全球南方”的挑战》，《国际安全研究》2025 年第 2 期。

弱化，国家正重新确立其在技术治理中的主体地位，人工智能治理领域出现了明显的“国家回归”态势。已有不少研究指出，人工智能技术极易与黑客攻击、数据窃取、恐怖主义活动、生物安全、核武器等传统和非传统安全议题结合，人工智能治理进程呈现明显的安全议程前置特征。[①] 国家应具备对人工智能技术创新应用和风险管理的自主权，通过公共权力对私营部门实施监管，确保公民权益不受人工智能技术侵犯。[②] 而对于掌握人工智能系统与数据的科技公司和数字平台而言，其内部决策过程难以保证民主和透明，且商业利益可能侵犯公共利益，因而缺乏充分的合法性基础。由此，在人工智能领域，商业公司只能被视为“准主权行为体”。[③]

需要指出的是，“主权人工智能”的基本理念与“网络主权”“数字主权”等概念之间具有深刻的内在延续性。“网络主权”强调国家在网络监管中的作用。2017 年的“永恒之蓝”勒索软件攻击、俄罗斯黑客“干预”美国大选等“例外状态”的发生，令各国政府愈发重视信息技术对社会秩序和政体稳定的潜在威胁，并对网络空间治理中国家的主体地位逐渐形成共识。[④] 美国于 2001 年提出的《爱国者法案》（USA PATRIOT Act）、“棱镜门”等一系列事件，进一步推动了“数字主权”概念的发展。[⑤] 这一概念强调国家自主监管其数字基础设施、数据和技术路线的重要性。[⑥] 可以说，当前各国所追求的“人工智能主权”以及“主权人工智能”相关实践，是这些概念在人工智能时代的自然延伸。

---

① 李艳：《人工智能国际治理：“安全偏好”及其现实影响》，《国家安全研究》2025 年第 1 期。

② Gleb Papyshev and Masaru Yarime, “The State’s Role in Governing Artificial Intelligence: Development, Control, and Promotion through National Strategies,” *Policy Design and Practice*, Vol. 6, No. 1, 2023; Daniel Mügge, “EU AI Sovereignty: For Whom, to What End, and to Whose Benefit?” *Journal of European Public Policy*, Vol. 31, No. 8, 2024; Riccardo Nanni, Pietro G. Bizzaro and Maurizio Napolitano, “The False Promise of Individual Digital Sovereignty in Europe: Comparing Artificial Intelligence and Data Regulations in China and the European Union,” *Policy & Internet*, Vol. 16, No. 4, 2024.

③ Huw Roberts, “Digital Sovereignty and Artificial Intelligence: A Normative Approach,” *Ethics and Information Technology*, Vol. 26, No. 70, 2024.

④ 沈逸：《全球网络空间治理原则之争与中国的战略选择》，《外交评论》2015 年第 2 期；沈逸：《后斯诺登时代的全球网络空间治理》，《世界经济与政治》2014 年第 5 期；郎平：《数智化背景下全球网络空间治理的演变与特点》，《人民论坛·学术前沿》2025 年第 13 期；郎平：《数字革命视域下网络空间治理路径探究》，《人民论坛》2022 年第 4 期。

⑤ 关于“数字主权”研究的兴起，参见 Malte Hellmeier and Franziska von Scherenberg, “A Delimitation of Data Sovereignty from Digital and Technological Sovereignty,” ECIS 2023 Research Papers, 2023, https://aisel.aisnet.org/ecis2023_rp/306。

⑥ Sanjay Misra, Kousik Barik and Petter Kvalvik, “Digital Sovereignty in the Era of Industry 5.0: Challenges and Opportunities,” *Procedia Computer Science*, Vol. 254, 2025.

（二）“主权人工智能”在安全领域具有统筹性

人工智能技术的国家安全属性与其作为“通用目的技术”（General Purpose Technology，GPT）的本质密切相关，技术的通用性特征重构了国家安全的议题维度。“通用目的技术”是指能够在广泛领域产生深远影响、引发经济和社会结构发生根本性变革的技术。[①] 这意味着人工智能可应用于几乎所有经济和社会领域，借助技术进步催生大量互补性创新，从而形成技术创新的规模效应。[②] 同时，安全是一个动态演化的概念：随着时代变迁，新的安全议题不断涌现，安全的内涵与外延持续拓展，后冷战时代的国家安全超越军事范畴，已扩展到政治、经济、社会等多个领域。[③] 当人工智能技术的通用性与安全议题领域的扩展相结合，主权国家的安全形势便发生了结构性变化。[④]

在军事安全领域，具有双重属性的人工智能已成为国家技术权力的构成要素：致命性自主武器系统（Lethal Autonomous Weapons Systems，LAWS）的部署降低了武力的使用门槛，存在着系统失控导致战争升级的风险；[⑤] 人工智能系统的情报与信息识别能力则有助于提高军事行动决策效率，实现战略优势。[⑥] 因此，技术创新和高效部署是国家“主权人工智能”实践的首要目标。在经济安全领域，人工智能

① Elhanan Helpman, ed., *General Purpose Technologies and Economic Growth*, Cambridge: MIT Press, 1998.

② Timothy F. Bresnahan and Manuel Trajtenberg, “General Purpose Technologies ‘Engines of Growth’?” *Journal of Econometrics*, Vol. 65, No. 1, 1995; Richard G. Lipsey, Kenneth I. Carlaw and Clifford T. Bekar, *Economic Transformations: General Purpose Technologies and Long-term Economic Growth*, Oxford: Oxford University Press, 2005.

③ 巴瑞·布赞、奥利·维夫、迪·怀尔德：《新安全论》，朱宁译，浙江人民出版社 2003 年版。

④ 封帅：《国家安全学视域下的人工智能安全研究：议题网络建构的初步尝试》，《国际安全研究》2023 年第 1 期；阙天舒、张纪腾：《人工智能时代背景下的国家安全治理：应用范式、风险识别与路径选择》，《国际安全研究》2020 年第 1 期；封帅、周亦奇：《人工智能时代国家战略行为的模式变迁——走向数据与算法的竞争》，《国际展望》2018 年第 4 期。

⑤ James Johnson, “Artificial Intelligence: A Threat to Strategic Stability,” *Strategic Studies Quarterly*, Vol. 14, No. 1, 2020; Kelley M. Sayler, “Artificial Intelligence and National Security,” CRS Report, November 21, 2019, https://www.everycrsreport.com/files/20191121_R45178_ddbcce24a6fbf02ad9e81387b5623295ac60f017.pdf.

⑥ “Responsible Artificial Intelligence Strategy and Implementation Pathway,” U.S. Department of Defense, June 2022, https://media.defense.gov/2024/Oct/26/2003571790/-1/-1/0/2024-06-RAI-STRATEGY-IMPLEMENTATION-PATHWAY.PDF; Darrell M. West and John R. Allen, “How Artificial Intelligence is Transforming the World,” Brookings, April 24, 2018, https://www.brookings.edu/articles/how-artificial-intelligence-is-transforming-the-world.

的通用性将改变现代经济体系中的“资本—技术—劳动力”关系。[①] 人工智能驱动的“新工业化”将吸引制造业向发达经济体“回流”，冲击发展中国家在人力资源等方面的比较优势，进而通过重构价值链制造新的不平等问题。[②] 国家建设“主权人工智能”需要实现对技术要素和技术路线的自主掌控。在社会与政治安全领域，人工智能借助社交媒体的中介作用，对社会治理和政体稳定造成冲击：生成式大语言模型大幅降低了虚假信息的制作成本，对社会信任体系构成了严重挑战；在人工智能系统的加持下，网络攻击的效率大幅提升，更易与恐怖主义结合，进一步放大社会安全风险。相应地，“主权人工智能”需要通过国家权力对本国境内的人工智能技术应用进行立法监管。在文化安全领域，大模型的社会应用还伴随着“算法偏见”和“数据投毒”的风险，模型的输出内容可能会违背社会基本伦理和价值观，[③] 解构主权国家的自我叙事和身份认同，进而危及“本体安全”。[④] 因此，保证大模型的输出内容符合本土文化和价值观也是“主权人工智能”的重要任务之一。综上，国家的“主权人工智能”实践具有面向各个安全领域的统筹性。

（三）“主权人工智能”追求开放性战略自主

人工智能不仅是一项信息技术，更是一个复杂的产业生态系统。发展人工智能既需要硬件、软件、数据等要素，还要有技术路线、人才战略、能源结构、资金投入等全方位的支撑。[⑤] 因此，国家构建“主权人工智能”的过程，本质是将国家权力的边界向数字、网络和技术生态等非领土空间延伸。在此过程中，技术要素的流动是不可避免的。首先，大模型的训练高度依赖海量数据。当前，全球算力资源集中于少数国家，这意味着企业需要将数据传输至境外，并租用他国领土范围内的基

① 封帅：《从民族国家到全球秩序：人工智能时代的世界政治图景》，《外交评论》2020 年第 6 期。

② 傅莹：《人工智能对国际关系的影响初析》，《国际政治科学》2019 年第 1 期；蔡翠红、戴丽婷：《人工智能影响复合战略稳定的作用路径：基于模型的考察》，《国际安全研究》2022 第 3 期。

③ Abeba Birhane, “Algorithmic Colonization of Africa,” *SCRIPTed*, Vol. 17, No. 2, 2020.

④ Jennifer Mitzen, “Ontological Security in World Politics: State Identity and the Security Dilemma,” *European Journal of International Relations*, Vol. 12, No. 3, 2006; Brent J. Steele, *Ontological Security in International Relations: Self-Identity and the IR State*, London: Routledge, 2008.

⑤ Ludovic Dibiaggio, Lionel Nesta and Simone Vannuccini, “European Sovereignty in Artificial Intelligence: A Competence-Based Perspective,” 2024, https://hal.science/hal-04841182/document；谢新水：《智能跃迁、开源创新与主权 AI：DeepSeek 现象推动人工智能开源创新生态体系建设》，《电子政务》2025 年第 3 期。

础设施发展自身算法。[①] 其次，数据分布并不均衡。非英语国家若要训练本土大语言模型，需引进境外数据以满足语料库需求。再次，模型的境外部署是人工智能技术跨国流动的核心维度。越来越多的大模型采用云端部署模式，用户需通过互联网访问其他国家的服务器来获取模型服务。[②] 最后，人工智能产业发展所需的资金和人才本身就具有跨国流动性。技术要素的跨境流动已经成为人工智能技术发展的基本特征，国家要发展人工智能自主技术能力，必须面向全球价值链和国际市场开展开放合作，“主权人工智能”需要在追求技术自主与开放国际合作之间取得平衡。

由此，“主权人工智能”呈现对传统“技术主权”概念的超越性理解。“技术主权”理论认为，新技术革命和技术竞争加速，引发国家的战略焦虑，由国家主权和实力构成的各类屏障开始发生变化，国家不得不强化自身的技术实力并试图建立牢固的技术壁垒，以此作为巩固自身地位、避免外部力量形成竞争优势的重要手段。[③] 面对人工智能技术要素的跨国流动性，各国对“技术主权”的理解，从实现完全的“自给自足”转向在开放合作中强化“能力建设”。[④] 国家不再追求对人工智能所需要的数据、算法、算力等要素进行绝对性的占有，[⑤] 而是着力培养在自身管辖范围内，利用基础设施、劳动力、商业网络生产及应用人工智能系统的能力。[⑥] 人工智能时代的“技术主权”，是国家在复合相互依赖的全球技术生态中掌握“控制权”而非“所有权”。因此，“主权人工智能”追求的目标是一种开放性的战略自主。

（四）“主权人工智能”要求国际话语权

“主权人工智能”是指国家在人工智能时代巩固主权的具体实践，这一概念既涵盖国家对内的能力建设和监管举措，也包含国家开展国际合作、参与全球治理的具体行动。国家需积极参与技术安全的国际对话，将自身发展诉求和治理偏好

① Susan Ariel Aaronson, “Data Is Different, and That’s Why the World Needs a New Approach to Governing Cross-Border Data Flows,” *Digital Policy, Regulation and Governance*, Vol. 21, No. 5, 2019.

② Ruiqi Sun and Daniel Trefler, “The Impact of AI and Cross-Border Data Regulation on International Trade in Digital Services: A Large Language Model,” NBER Working Paper, No. 31925, 2023, https://www.nber.org/system/files/working_papers/w31925/w31925.pdf.

③ Walter B. Wriston, “Technology and Sovereignty,” *Foreign Affairs*, Vol. 67, No. 2, 1988.

④ Christoph March and Ina Schieferdecker, “Technological Sovereignty as Ability, Not Autarky,” *International Studies Review*, Vol. 25, No. 2, 2023.

⑤ Ludovic Dibiaggio, Lionel Nesta and Simone Vannuccini, “European Sovereignty in Artificial Intelligence: A Competence-Based Perspective,” 2024, https://hal.science/hal-04841182/document.

⑥ Trisha Ray, “The Future of AI Is Sovereign: How It Evolves Is Up to Us,” Observer Research Foundation, April 16, 2025, https://www.orfonline.org/expert-speak/the-future-of-ai-is-sovereign-how-it-evolves-is-up-to-us.

融入国际规则制定进程，为“主权人工智能”的发展创造良好外部环境。

随着技术复杂性的增加，技术系统对社会的塑造作用也在加强，不同国家因生产力基础和社会结构的不同，会产生不同的“技术—社会”互动模式。[①] 国家制度环境决定了其协调多元主体、减少信息不对称及增强系统韧性的具体路径，尊重制度差异是实现全球人工智能治理包容性的前提。[②] 全球人工智能治理的多样性共存格局既是各国根据自身条件和利益进行理性选择的结果，也体现了人工智能技术本身的复杂性和多维性，即不存在一种适用于所有情境的最优治理模式。[③]

人工智能技术的研发与应用具有资本密集型和知识密集型特征，技术能力高度集中于少数国家和企业。技术领先者凭借其市场地位强化垄断力量，构建额外的准入壁垒。[④] 以美国半导体联盟为例，其核心成员通过联合制定芯片设计标准与制造工艺规范，主导行业技术发展方向，致力于将这些技术标准转化为具有广泛约束力的产业规范。国际标准化组织的标准制定过程虽在形式上保持开放透明，但实质决策权集中于少数技术垄断企业。在人工智能管理系统标准（ISO/IEC 42001）的制定中，来自谷歌、微软、国际商业机器公司（IBM）等企业的代表占据了工作组超 60% 的关键职位，直接影响到人工智能治理和风险管理等核心章节的起草工作。[⑤]

在建设“主权人工智能”的过程中，国家不得不面对全球安全治理的多样化需求与人工智能技术标准垄断之间的张力。将本国的发展诉求和治理实践经验提炼转化为国际规范，是建设“主权人工智能”的重要任务之一。一国在建设“主权人工智能”的同时，也必须尊重其他国家的“主权人工智能”实践，进而在人工智能时代构建起平等包容的多样性国际秩序。[⑥]

---

① 余南平：《通用人工智能时代的国际权力重塑》，《中国社会科学》2025 年第 4 期。

② 蔡翠红、张璐瑶：《全球人工智能治理探究——基于委托—代理理论视角》，《国际政治研究》2025 年第 2 期。

③ 蔡翠红、张璐瑶：《人工智能区域合作的比较研究——以东盟、欧盟、海合会为例》，《同济大学学报（社会科学版）》2025 年第 4 期。

④ Jai Vipra and Anton Korinek, “Market Concentration Implications of Foundation Models,” Brookings, September 2023, https://www.brookings.edu/articles/market-concentration-implications-of-foundation-models-the-invisible-hand-of-chatgpt/.

⑤ 孙志伟：《从技术竞逐到“智能公域”：人工智能全球治理的范式转向》，《国际展望》2026 年第 1 期。

⑥ 国际学界在描述全球人工智能治理结构时常用“多元性”（Pluralism）概念，强调国家行为体与国际组织、跨国企业等非国家行为体的互动关系。本文采用“多样性”（Diversity）概念，意在突出主权国家之间的制度与发展模式差异。关于这两个概念的使用，参见俞沂暄：《多样性全球秩序研究导论》，上海人民出版社 2025 年版；姚旭、朱政宇：《全球人工智能治理：多元主体结构与互动机制》，《信息安全与通信保密》2025 年第 11 期。

综上，“主权人工智能”的理论内涵展现出对现代主权以及“网络主权”“数字主权”“技术主权”理念的延续与超越：在应对人工智能的快速迭代性和不可解释性时，国家需重新找回“例外状态”的决断权；人工智能技术的通用性赋予了“主权人工智能”统筹不同安全领域具体任务的能力；数据、模型、人才等技术要素的跨国流动，决定了“主权人工智能”的目标是追求开放性战略自主；针对人工智能的技术标准垄断，“主权人工智能”还体现出国家对治理话语权的诉求，反映了构建多样性国际秩序的安全治理理念（参见表 1）。

表 1 “主权人工智能”的理论内涵

人工智能技术特性	“主权人工智能”理论内涵
高速迭代、模型不可控	国家主体性
通用性	安全领域统筹性
技术要素流动性	开放性战略自主
技术标准与治理规则垄断	国际话语权诉求

资料来源：笔者自制。

二 “全球南方”的“主权人工智能”构建

当前，美欧开展了具有“主权人工智能”特色的战略实践，着力补齐各自在技术创新和供应链上的短板，试图减少外部依赖。特朗普第二任期以来，美国大幅降低法律监管对人工智能创新应用的阻碍，通过“星际之门”“创世纪”等国家计划，由政府引导私营部门进行产业布局和投资。[①] 欧盟将人工智能视为“数字主权”的构成要素，[②] 发布了《人工智能大陆行动计划》（*AI Continent Action Plan*）等一系列战略规划，并在法律执行层面适当放宽了《人工智能法案》（*Artificial Intelligence*

① “Fact Sheet: President Donald J. Trump Unveils the Genesis Mission to Accelerate AI for Scientific Discovery,” The White House, November 24, 2025, https://www.whitehouse.gov/fact-sheets/2025/11/fact-sheet-president-donald-j-trump-unveils-the-genesis-missionto-accelerate-ai-for-scientific-discovery/; “President Donald J. Trump Takes Action to Enhance America’s AI Leadership,” The White House, January 23, 2025, https://www.whitehouse.gov/fact-sheets/2025/01/fact-sheet-president-donald-j-trump-takes-action-to-enhance-americas-ai-leadership/.

② 宫云牧：《数字时代主权概念的回归与欧盟数字治理》，《欧洲研究》2022 年第 3 期；宫云牧：《欧盟的数字主权建构：内涵、动因与前景》，《国际研究参考》2021 年第 10 期；忻华：《“欧洲经济主权与技术主权”的战略内涵分析》，《欧洲研究》2020 年第 4 期；蔡翠红、张若扬：《“技术主权”和“数字主权”话语下的欧盟数字化转型战略》，《国际政治研究》2022 年第 1 期。

Act）的监管门槛，以鼓励欧洲本土的自主技术创新。[①] 相较于发达国家及相关行为体，全球南方国家在建设“主权人工智能”的过程中，面临着一系列特殊的安全风险与制约，其具体建设路径也存在差异。

（一）“全球南方”发展人工智能技术的风险与制约

第一，“全球南方”所拥有的技术要素和资源禀赋尚不充分。首先，数据是大语言模型预训练和部署的“血液”，唯有依托海量、高质量的数据，才能训练出先进的算法。“全球南方”的数据资源普遍存在匮乏且多样性不足的问题。以非洲为例，尽管当地拥有超过 2 000 种语言，但相关的高质量数字化语料库却较少，非洲语言内容在全球互联网内容中的占比仅为 0.02%。[②] 其次，算法的优化与迭代是人工智能模型发展的核心。以拉美地区为例，该地区在全球人工智能论文中的占比仅为 3%，在全球人工智能专利中的占比更是低至 0.06%；[③] 同时，其研发投入占国内生产总值（GDP）的比例仅为 0.7%，远低于发达国家和地区的平均水平。[④] 再次，算力是模型训练的基础，先进显卡芯片和超级数据中心构成了国家人工智能发展的基本能力。当前，中低收入国家仅拥有全球不到 6%的算力中心。[⑤] 中国生产的人工智能芯片在性能指标和量产能力方面正快速追赶技术发达国家，但用于模型预训练的高端算力芯片距离实现全面的国产替代还有一段距离。[⑥] 最后，新型算力基础设施建设需要大规模的资金投入。据预测，到 2030 年，非洲对数据中心容量的需求预计将增长至 1.5—2.2 吉瓦，为此需要 100 亿—200 亿美元的新增投资。[⑦]

---

① 杨昭：《“规制国家”的政策调适：欧盟人工智能治理逻辑》，《欧洲研究》2025 年第 5 期。

② Syed Khasru and Rubayat Anik, “AI and Africa: The Unexplored Frontier of Innovation and Inclusivity,” T20 South Africa, July 21, 2025, https://t20southafrica.org/commentaries/ai-and-africa-the-unexplored-frontier-of-innovation-and-inclusivity/.

③ “The 2025 AI Index Report,” Human-Centered Artificial Intelligence, 2025, https://hai.stanford.edu/assets/files/hai_ai_index_report_2025.pdf.

④ Julio Vasconcellos et al., “Latin America Digital Report 2025,” Atlantico, 2025, https:// docsend.com/view/it3dc7aexy3w9ggf.

⑤ “Strengthening AI Foundations: Emerging Opportunities for Developing Countries,” World Bank Group, November 21, 2025, https://www.worldbank.org/en/news/factsheet/2025/11/21/strengthening-ai-foundations-emerging-opportunities-for-developing-countries.

⑥《算力经济发展研究报告（2025 年）》，中国信息通信研究院云计算与大数据研究所，2025 年 9 月，https://www.caict.ac.cn/kxyj/qwfb/ztbg/202509/P020250910593366724819.pdf。

⑦ Kartik Jayaram et al., “Building Data Centers for Africa’s Unique Market Dynamics,” McKinsey & Company, November 24, 2025, https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/building-data-centers-for-africas-unique-market-dynamics.

在东南亚地区，尽管 2025 年获得了近 600 亿美元的基础设施投资，但这些资金主要来自英伟达、微软等外国企业，本土贡献占比极小。[①] 在拉美地区，2023 年电信基础设施公共投资占 GDP 的比例仅为 0.25%，难以应对日益增长的算力需求。[②]

第二，“全球南方”的人工智能抗风险能力有待提升。在技术的内生性安全层面，“全球南方”的模型稳健性显著弱于“全球北方”。由于“全球南方”缺乏本土化的高质量数据集，需要大量调用第三方数据库进行本土模型训练，所以更容易受到数据投毒及由此引发的机器“幻觉”影响。[③] 在技术的应用安全领域，“全球南方”正面临严峻的网络犯罪和网络攻击态势。据统计，非洲相关组织平均每周遭受 3 153 次攻击，而尼日利亚每周被攻击次数更是高达 4 200 次。[④] 2025 年，亚太地区的深度伪造欺诈案件激增 2100%，报案数量接近欧洲的两倍。[⑤] 中国面临的应用安全风险更为严重：2024 年，基于人工智能的深度伪造欺诈增长 3000%，生成式钓鱼邮件增长 1000%。[⑥] 在人工智能技术与其他前沿技术交叉的安全领域，全球南方国家普遍存在监管力度不足的问题。以生物安全为例，全球只有 27%的全球南方国家制定了人工智能国家战略，没有一个涉及人工智能生化武器与合成脱氧核糖核酸（DNA）筛查机制。[⑦] 此外，人工智能的技术安全风险还会引发社会、政治领域的衍生性风险。跨国数字平台拥有控制信息传播、塑造社会认知甚至干预选举的能力，进一步加剧了技术欠发达国家的安全风险。[⑧] 人工智能技术的滥用还可能侵蚀

① “Frontier AI Rising: Southeast Asia’s The Path to Economic Transformation,” SCB10X, July 8, 2025, https://www.scb10x.com/en/blog/frontier-ai-rising.

② “Latin American Economic Outlook 2023,” OECD, December 15, 2023, https://www.oecd.org/en/publications/latin-american-economic-outlook-2023_8c93ff6e-en.html.

③ Samuel Segun et al., “Towards an African Agenda for AI Safety,” Global Center on AI Governance, September 2, 2025, https://www.ai4d.ai/research/towards-an-african-agenda-for-ai-safety.

④ “Check Point 2025 Report: AI-Powered Cyber-Attacks Surge across Africa,” IT Edge News, November 19, 2025, https://www.itedgenews.africa/check-point-2025-report-ai-powered-cyber-attacks-surge-across-africa/.

⑤ “APAC Deepfake Fraud Climbs up to 2,100% as Attacks Become More Industrialised,” Fintech News Singapore, November 25, 2025, https://fintechnews.sg/122644/security/apac-deepfake-fraud-2025/.

⑥《2024 人工智能安全报告》，奇安信，2024 年 2 月 29 日，https://www.qianxin.com/threat/reportdetail?report_id=311。

⑦ Tina Wünn, “Exploring AI-Biosecurity Governance in the Global South,” The Nuclear Threat Initiative, December 5, 2024, https://www.nti.org/risky-business/exploring-ai-biosecurity-governance-in-the-global-south/?utm_campaign=buffer.

⑧ Maryanne Kelton et al., “Virtual Sovereignty? Private Internet Capital, Digital Platforms and Infrastructural Power in the United States,” *International Affairs*, Vol. 98, No. 6, 2022.

公民信任、破坏问责机制，对发展中国家的主权合法性构成危机。[①] 面对人工智能技术的内生、应用和衍生风险，“全球南方”抗风险能力有待提升。

第三，发达国家的技术垄断加剧全球南方国家面临的结构性不平等。广大全球南方国家与发达国家间的能力差距极易形成依附性发展结构，导致其陷入“发展陷阱”。[②] 在世界领先的大语言模型中，2/3 来自美国科技公司。[③] 在用于模型训练的高端芯片市场，仅英伟达一家企业就占据了约 95%的市场份额。[④] 而在非洲和东南亚的云计算市场，美国科技巨头亚马逊网络服务、微软 Azure 和谷歌云有着绝对的主导地位。[⑤] 特别是尼日利亚，尽管本地云服务商正逐渐兴起，却仍有超过 70%的政府部门及机构将数据托管于亚马逊和微软 Azure 平台之上。[⑥] 在基础设施方面，截至 2025 年 6 月，全球仅有 32 个国家拥有专门的人工智能数据中心，且大多集中于“全球北方”。整个非洲大陆的数据中心容量仅占全球总量的不到 1%，这迫使本地企业——尤其是初创公司和中小企业——不得不寻求外部解决方案，以满足自身计算和存储需求。[⑦] 在这种不平等结构中，“全球南方”可能因西方国家将供应链武器化而面临更深层次的发展制约，导致关键技术面临“卡脖子”风险。[⑧] 自

① Paul Timmers, “AI Challenging Sovereignty and Democracy,” *Turkish Policy Quarterly*, Vol. 20, No. 4, 2022；封帅：《从民族国家到全球秩序：人工智能时代的世界政治图景》，《外交评论》2020 年第 6 期。

② 全球人工智能创新治理中心：《全球人工智能治理新趋势：以“上海宣言”为起点的观察》，《复旦智库报告》2025 年第 8 期。

③ “Artificial Intelligence Index Report 2025,” Human-Centered Artificial Intelligence, 2025, https://hai.stanford. edu/assets/files/hai_ai_index_report_2025.pdf.

④ Kif Leswing, “Nvidia Dominates the AI Chip Market, But There’s More Competition than Ever,” CNBC, June 2, 2024, https://www.cnbc.com/2024/06/02/nvidia-dominates-the-ai-chip-market-but-theres-rising-competition-.html?msockid=32c08c419b5d63301ab898089ab76203.

⑤ “Cloud Computing in Africa: Why Local Startups Are Saving 40% on IT Costs,” Impronics Technologies, July 3, 2025, https://www.linkedin.com/pulse/cloud-computing-africa-why-local-startups-saving-cijke/.

⑥ Damilare Dosunmu, “Nigerians are Building Affordable Alternatives to AWS and Google Cloud,” Rest of World, February 25, 2025, https://restofworld.org/2025/aws-google-cloud-nigeria-alternatives/.

⑦ Zoe Jay Hawkins, Vili Lehdonvirta and Boxi Wu, “AI Compute Sovereignty: Infrastructure Control Across Territories, Cloud Providers, and Accelerators,” SSRN, 2025, http://dx.doi.org/10.2139/ssrn.5312977.

⑧《算力经济发展研究报告（2025 年）》，中国信息通信研究院云计算与大数据研究所，2025 年 9 月，https://www.caict.ac.cn/kxyj/qwfb/ztbg/202509/P020250910593366724819.pdf。

特朗普第一任期以来，美国频繁以国家安全为由实施技术出口管制，[①] 其中以中国为代表的全球南方国家遭受的技术管制最为严重。[②]

第四，全球南方国家参与国际规则制定受限，治理话语权和代表性不足。[③]“全球南方”因缺乏技术能力、数据基础设施或政策制定经验，难以在区域或全球人工智能治理中有效发声，这可能使全球治理框架被“技术精英主导”，无法反映多元利益诉求。[④] 全球南方国家的话语权失衡具体表现在三个方面：其一，治理代表性严重不足。至 2025 年，全球范围内有 118 个国家几乎完全被排除在人工智能治理讨论之外，其中大多数来自全球南方国家。[⑤] 例如，“全球人工智能伙伴关系”（GPAI）的 22 个创始成员中，全球南方国家仅占 2 席。其二，规则内容过度聚焦和反映北方利益。现有治理框架大多围绕发达国家的技术优势与市场需求进行构建，对“全球南方”关心的数字鸿沟、普惠性技术转移、数据本地化与主权保护等议题回应乏力。[⑥] 在全球已有的人工智能治理框架中，由“全球南方”提出的方案甚至不足 1/5。[⑦] 其三，在治理规则执行中缺乏主导权。全球南方国家常常被迫接受由发达国家主导制定的国际标准，这些标准往往与贸易优惠或援助资金挂钩，导致全球南方国家在规则适应性调整中陷入被动。[⑧]

---

① 刘国柱、尹楠楠：《美国国家安全认知的新视阈：人工智能与国家安全》，《国际安全研究》2020 年第 2 期。

② “PART 744-Control Policy: End-User and End-Use Based, ” Bureau of Industry and Security, https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-744#ap15.2.744_122.4; “Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence,” The White House, October 30, 2023, https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence; “Additional Information on Final Regulations Implementing Outbound Investment Executive Order (E.O.14105),” U.S. Department of the Treasury, October 28, 2024, https://home.treasurygov/news/press-releases/jy2690.

③ Giandomenico Majone, “From the Positive to the Regulatory State: Causes and Consequences of Changes in the Mode of Governance,” *Journal of Public Policy*, Vol. 17, No. 2, 1997.

④《人工智能或将加剧国家间发展差距，引发新一轮大分化》，联合国开发计划署，2025 年 12 月 2 日，https://www.undp.org/zh/china/press-releases/lianheguokaifajihuashubaogaorengongzhinenghuojiangjiajuguojiajianfazhanchajuyinfaxinyilundafenhua。

⑤ “2025 Technology and Innovation Report: Inclusive Artificial Intelligence for Development,” UNCTAD, July 2025, https://unctad.org/system/files/official-document/tir2025_en.pdf.

⑥《金砖国家领导人关于人工智能全球治理的声明》，中国外交部网站，2025 年 7 月 9 日，https://www. fmprc.gov.cn/web/zyxw/202507/t20250709_11668022.shtml。

⑦《为人类治理人工智能》，联合国，2024 年 9 月 19 日，https://www.un-ilibrary.org/content/books/9789211068863。

⑧ 于晓莉：《推动形成多元共治的全球人工智能治理格局》，《学习时报》，2025 年 8 月 2 日。

（二）“全球南方”构建“主权人工智能”的具体路径

基于对“主权人工智能”学理逻辑的梳理以及全球南方国家发展人工智能技术所面临的安全风险与挑战，本文尝试从主权的对内“最高性”和对外“独立性”双重维度，分析“全球南方”构建“主权人工智能”的具体路径（参见图 1）。“主权人工智能”的对内“最高性”表现为国家在国内人工智能产业发展中发挥的引领作用：一是制定纲领性战略文本，统筹国内人工智能产业发展；二是推进立法程序，引导人工智能监管。这两项任务分别回应了“全球南方”所面临的人工智能要素缺乏问题与技术安全风险。“主权人工智能”对外“独立性”则表现为追求技术自主和话语权：一方面，全球南方国家希望减少对他国技术和产品的依赖，保障本国的自主发展空间；另一方面，在贸易保护主义与国际秩序变革的背景下，“全球南方”只有团结合作、坚守多边主义原则，才能确保在人工智能发展浪潮中实现普惠受益。

第一，主导产业发展，实现技术进步。全球南方国家需根据自身实际，加快对数据要素、算力和基础设施的建设步伐，促进本土产业技术创新。这意味着国家需要充分调动技术生态体系中的各个环节，完善国家人工智能发展战略。“主权人工智能”不仅要求大力提升改进模型和算法，更重要的是要将模型部署和应用于整个国家的产业链中。而这种关乎整个创新生态系统的整合能力，也必须依靠国家的宏观政策规划才能实现。①

第二，通过立法增强风险防御能力。构建“主权人工智能”要求国家通过立法建立完备的人工智能监管体系，以应对内部与外部安全所面临的各项风险与挑战。世界各国的人工智能立法路径主要有两类，一是以欧盟为代表的“硬法”范式，二是以美国、日本为代表的“软法”范式。考虑到全球南方国家的多样性，各国在“创新—监管”光谱上的政策重点势必有所不同。但是，无论是哪一种技术监管范式，主权国家都应保留对于技术安全问题的最终“决断权”。

第三，通过国际合作寻求战略自主。面对全球地缘政治局势紧张和大国博弈加剧，国家间数字技术相互依赖的脆弱性和敏感性愈发凸显。全球南方国家只有建立本地基础设施，掌握技术研发的自主能力，才能减少对国外高端技术和先进数字产品的依赖，从而规避脱钩断链和“卡脖子”带来的结构性风险。而“主权人工智能”对技术自主性的追求并不意味着全球南方国家终将走向技术保护主义。相反，全球

① 余南平、栾心蔚：《构建链权：人工智能价值链与大国战略竞争》，《外交评论》2025 年第 5 期。

南方国家需开放市场，通过与发达国家的技术合作和南南合作消除技术依赖，推进全球南方国家自身能力建设。

第四，通过制度参与获取话语权。对于在全球治理体系中被边缘化的问题，“全球南方”要提升战略自主性、实现自身利益，就必须不断提升话语权。为实现这一目标，全球南方国家需协调一致、团结合作，在全球治理体系变革进程中携手发挥作用。以金砖国家为例，“大金砖合作”正积极推动各领域务实合作，通过成立中国—金砖国家人工智能发展与合作中心、中国—金砖国家新质生产力研究中心，以普惠共治为原则代表全球南方国家发声，在规则制定、议程设置和理念传播等方面持续推进全球治理体系改革。①

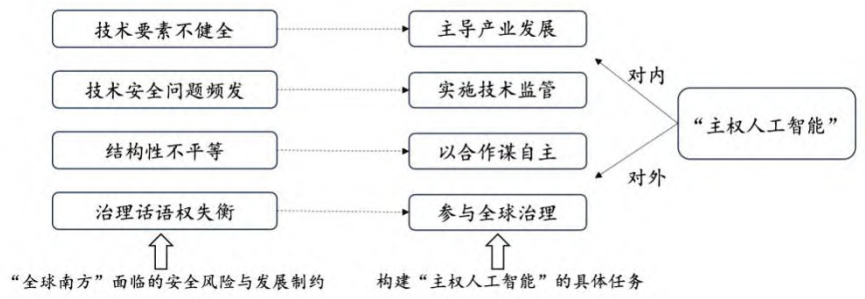

图 1 “全球南方”构建“主权人工智能”的风险挑战和具体路径

资料来源：笔者自制。

三 全球南方国家的“主权人工智能”实践

本文选取巴西和印度尼西亚作为案例，探究全球南方国家构建“主权人工智能”的具体实践路径。巴西与印尼都是重要的全球南方国家，其政策动向对理解全球南方国家的人工智能政策及人工智能南南合作具有重要的现实意义。同时，两国的人工智能技术水平均凭借体系化的制度设计与战略实践取得了一定进步，能够在一定程度上体现“全球南方”“主权人工智能”的共性特征。

（一）巴西的“主权人工智能”建设

近年来，巴西已成为拉丁美洲领先的人工智能创新中心之一。2022 年，巴西在

① 江天骄：《全球南方崛起背景下的“大金砖合作”与国际秩序转型》，《和平与发展》2025 年第 5 期。

全球人工智能研究领域位列第 15 位。[①] 巴西取得的进步与其“主权人工智能”建设密不可分。巴西已经在人工智能发展战略制定和立法监管方面采取行动，尝试在国际合作中寻求市场开放与技术自主的平衡。

第一，政府主导产业规划以提升人工智能竞争力。人才外流、数据要素匮乏和算力基础设施建设落后等问题，长期制约着巴西的人工智能技术发展。[②] 巴西政府从 2018 年起便开始对人工智能技术发展进行统筹规划，采取政府集中协调的方式，将财政预算和关键资源倾斜至人工智能相关产业。[③] 2021 年 4 月，巴西科技创新与通信部发布了《巴西人工智能战略》（EBIA），[④] 内容涵盖“教育”“劳动力与人才培养”“研发、创新与创业”“产业应用”“社会应用”“公共安全”等领域，[⑤] 并将其统称为实现“人工智能主权”的六大要素。[⑥] 然而，EBIA 曾因缺乏详细的预算分配和评估方法而一度受到批评。[⑦] 2024 年 7 月，巴西正式推出经多次修订的《巴西人工智能投资计划 2024—2028》（PBIA 2024—2028）。[⑧] 该计划提出，将 40 亿美元用于人工智能投资，主要覆盖公共卫生、农业、环境、商业和教育等方向：其中 24.94 亿美元用于商业创新项目，8.91 亿美元用于人工智能基础设施和开发，剩余资金则分配至培训计划、公共服务和人工智能监管等支持举措。[⑨] 通过政策规

① 谌园庭、李俊霖：《人工智能成为巴西发展新引擎》，《中国对外贸易》2025 年第 5 期。

② “ABC Lança Recomendações Sobre Inteligência Artificial no Brasil,” ATUAÇÃO DA ABC, November 9, 2023, https://www.abc.org.br/2023/11/09/abc-lanca-recomendacoes-sobre-inteligencia-artificial-no-brasil/.

③ “Brazilian Strategy for Digital Transformation,” OECD.AI, https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-24273.

④ “Estratégia Brasileira de Inteligência Artificial,” Ministério da Ciência, Tecnologia e Inovações, June 15, 2021, https://wp.oecd.ai/app/uploads/2022/01/Brazil_Brazilian_AI_Strategy_2021.pdf.

⑤ “Summary of the Brazilian Artificial Intelligence Strategy,” Ministry of Science, Technology and Innovations, Brazil, 2021, https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ebia-summary_brazilian_4-979_2021.pdf.

⑥ Luca Belli, “To Get Its AI Foothold, Brazil Needs to Apply the Key AI Sovereignty Enablers (KASE),” in Steven Feldstein, ed., *New Digital Dilemmas: Resisting Autocrats, Navigating Geopolitics, Confronting Platforms*, Washington, D.C.: Carnegie Endowment for International Peace, 2023.

⑦ “Regulating Artificial Intelligence in Brazil,” Center for Human Rights and Global Justice, May 25, 2023, https://chrgj.org/2023-09-28-regulating-artificial-intelligence-in-brazil/.

⑧ “Plano Brasileiro de Inteligência Artificial (PBIA) 2024-2028,” Ministério da Ciência, Tecnologia e Inovações, July 8, 2024, https://www.gov.br/lncc/pt-br/assuntos/noticias/ultimas-noticias-1/plano-brasileiro-de-inteligencia-artificial-pbia-2024-2028.

⑨ “Brazil Proposes $4 Billion AI Investment Plan,” Reuters, July 31, 2024, https://www.reuters.com/technology/artificial-intelligence/brazil-proposes-4-billion-ai-investment-plan-2024-07-30/.

划与机构设置，巴西形成了以政府为主、私营部门为辅的人工智能发展模式，即由政府对人工智能产业的发展重点和方向进行统一规划，统筹协调用于人工智能投资的财政预算，充分显示出其“主权人工智能”模式的国家主导性。

第二，推动人工智能立法进程，维护本国技术安全。随着巴西人工智能的广泛应用，针对模型训练数据的“投毒”行为及网络攻击风险也随之上升。2024—2025年，巴西62%的数据安全事件涉及个人敏感信息泄漏，44%的案件由源代码泄漏引发。对跨国数字平台监管的缺失，助长了人工智能相关的网络犯罪。例如，微软公司的OneDrive在2025年成为巴西境内传播恶意软件最多的平台。[①] 为应对数据安全问题，巴西政府推进数据保护立法：2020年9月通过并生效的《通用数据保护法》（LGPD），统一了40部规范个人数据处理的已有法律，对涉及位于巴西的个人、在巴西收集或处理数据，以及使用数据向巴西的个人提供商品或服务等方面进行规定。近年来，巴西的数据监管执法力度持续加强。2024年，巴西法院依据LGPD，对WhatsApp与Meta公司之间的不当数据共享处以约3亿美元罚款。[②] 巴西参众两院也在大力推动《人工智能法案》的完善与通过。2024年12月，巴西参议院通过了第2338号关于监管人工智能的法律监管框架的法案。该法案要求对巴西的人工智能行业进行持续监控和调整，并将人工智能系统划分为不同风险等级，根据其对人类生命和基本权利的影响，对不同系统进行不同等级的规定。[③]

第三，通过投资合作、开放市场、人才培养和国际交流等方式赋能本国的人工智能能力建设，提升技术自主性。在投资合作方面，2025年5月，巴西总统卢拉（Lula da Silva）访华，同中国签署包括人工智能合作在内的20项合作协议。[④] 人工智能相关合作协议主要聚焦风险解决、专业人员培训、大型语言模型及多模态系

① “Threat Labs Report: Brazil 2025,” Netskope, 2025, https://www.netskope.com/resources/threat-labs-reports/threat-labs-report-brazil-2025?trk=article-ssr-frontend-pulse_x-social-details_comments-action_comment-text#about-this-report.

② Tommaso Giardini et al., “DPA Digital Digest: Brazil,” Digital Policy Alert, December 18, 2024, https://digitalpolicyalert.org/digest/dpa-digital-digest-brazil; “General Personal Data Protection Act (LGPD),” Ecomply.io, https://lgpd-brazil.info/.

③ “Senado Aprova Regulamentação da Inteligência Artificial; Texto vai à Câmara,” Da Agência Senado, December 10, 2024, https://www12.senado.leg.br/noticias/materias/2024/12/10/senado-aprova-regulamentacao-da-inteligencia-artificial-texto-vai-a-camara.

④《国家发展改革委与巴西有关部门签署三份合作文件》，中国政府网，2025年5月14日，https://www.gov.cn/lianbo/bumen/202505/content_7023708.htm。

统训练合作，预计投资 230 亿巴西雷亚尔，有效期 3 年且可续签。[①] 在技术合作方面，深圳市江波龙电子股份有限公司于 2023 年收购巴西存储厂商 SMART Brazil 及其全资子公司 SMART Modular，投资 8.59 亿元人民币在圣保罗州扩建存储芯片封装测试生产线，以满足本土硬件需求。2024 年 11 月，巴西半导体行业协会与中国半导体行业协会签署合作谅解备忘录，计划联合开发存储芯片。[②] 在人才培养方面，2020 年，圣保罗大学与 IBM 深化合作，新建自然语言处理实验室，定向研究葡萄牙语大模型，培养本土语言领域的人工智能专家。[③] 2024 年 9 月，巴西政府参与微软“ConectAI”计划，联合巴西劳工部、SENAI 职业培训学院等 26 家机构，预计 3 年投资 147 亿雷亚尔，为 500 万人提供免费人工智能技能课程。[④] 此外，巴西与中国深化合作，借鉴中国 STEM 教育模式，推广“AI+远程教育”以解决偏远地区资源短缺问题。[⑤]

第四，巴西将“金砖国家”合作机制与二十国集团（G20）视为优先选择的国际合作平台，凸显全球南方国家的治理立场。[⑥] 巴西作为 2025 年金砖国家峰会的主席国，积极推动金砖扩员，吸纳印度尼西亚成为金砖正式成员，吸引古巴加入金

①《国家发展改革委与巴西有关部门签署三份合作文件》，中国政府网，2025 年 5 月 14 日，https://www.gov.cn/lianbo/bumen/202505/content_7023708.htm; Mauro Ramos, “China-Brazil AI Agreement Reinforces Joint Researches and Infrastructure Development,” Brasil de Fato, May 28, 2025, https://www.brasildefato.com.br/2025/05/28/china-brazil-ai-agreement-reinforces-joint-researches-and-infrastructure-development/。

②《IC China 2024：江波龙存储出海 打造中巴半导体产业合作新典范》，美通社，2024 年 11 月 21 日，https://www.prnasia.com/story/469875-1.shtml; “What’s Behind Zilia’s US$120mn Brazil Semiconductors Investment?” Bnamericas, July 12, 2024, https://bnamericas.com/en/features/whats-behind-zilias-us120mn-brazil-semiconductors-investment。

③《巴西加快发展人工智能 部分公司已着手为尚未具备资质的人员提供培训》，环球商业网，2020 年 11 月，http://m.chynews.cn/zhineng/2020/1104/16383.html。

④ “Microsoft Announces 14.7 Billion Reais Investment over Three Years in Cloud and AI Infrastructure and Provide AI Training at Scale to Upskill 5 Million People in Brazil,” Source LATAM Brasil, September 29, 2024, https://news.microsoft.com/pt-br/microsoft-announces-14-7-billion-reais-investment-over-three-years-in-cloud-and-ai-infrastructure-and-provide-ai-training-at-scale-to-upskill-5-million-people-in-brazil/.

⑤《巴西前部长：中巴 AI 合作前景广阔 中国经验值得借鉴》，中国日报网，2024 年 10 月 25 日， https://china.chinadaily.com.cn/a/202410/25/WS671b0e15a310b59111d9fd4e.html。

⑥ 姚旭、江天骄：《金砖国家推动人工智能治理的动因、实践和挑战》，《同济大学学报（社会科学版）》2025 年第 2 期。

砖伙伴国机制，通过推动扩员进程，提高“全球南方”的治理参与度。[①] 同时，巴西致力于推动金砖国家内部运作机制改革，在组织管理和运行效率方面提升金砖制度的治理能力。[②] 巴西积极推动倡导金砖国家“去美元化支付系统”，发展更高效的支付体系以促进金砖国家贸易与投资。[③] 这一倡议也将促进金砖国家围绕人工智能开展金融合作。此外，巴西还支持联合国和 G20 在全球人工智能治理中的作用，其核心主张是反对少数国家垄断多边机制，鼓励普惠包容的人工智能治理框架，加强“全球南方”的话语权。[④] 在 2024 年举行的 G20 峰会上，巴西积极对接经济合作与发展组织（OECD）的人工智能治理原则，推动将“人工智能向善、造福所有人”写入联合宣言，并设立 G20 人工智能任务组，强调以“负责任、包容和以人为本”原则解决技术鸿沟。同时，巴西还联合发展中国家共同呼吁合理使用人工智能，确保人类伦理规范和隐私权利受到保护。[⑤]

（二）印度尼西亚的“主权人工智能”建设

作为东南亚最大经济体和全球第四人口大国，印度尼西亚正加速拥抱人工智能技术革命。印尼生成式人工智能市场规模预计将从 2025 年的 3.56 亿美元增长至 2030 年的 22.02 亿美元，年复合增长率高达 44%，展现出巨大的市场潜力。[⑥] 由于庞大的人口基数及法律监管执行力度的不足，印尼正承受着深度伪造、网络攻击、数据泄露等安全风险的冲击。为此，印尼积极通过“主权人工智能”建设，寻求能力提升与国家安全之间的平衡，为全球南方国家提供了重要的参考样本。

第一，政府制定自主产业政策以提高技术实力。印尼国内数字鸿沟问题十分突

①《巴西宣布印尼成为金砖国家正式成员，印尼称将为金砖国家议程做出积极贡献》，环球网，2025 年 1 月 7 日，https://world.huanqiu.com/article/4KyTCt6CedB。

② “Brazil Officially Becomes BRICS Chair Country,” BRICS TV, January 1, 2025, https://tvbrics.com/en/news/brazil-officially-becomes-brics-chair-country/.

③ Carlos Albérico de Medeiros, “O Plano dos EUA Para Conter o BRICS e Salvar o Dólar,” Vermelho, June 12, 2025, https://vermelho.org.br/2025/12/06/o-plano-dos-eua-para-conter-o-brics-e-salvar-o-dolar/.

④ “Speech by Foreign Minister Mauro Vieira at the Opening of the BRICS Foreign Ministers’ Meeting,” BRICS TV, April 8, 2025, https://brics.br/en/news/brics-tv/speech-by-foreign-minister-mauro-vieira-at-the-opening-of-the-brics-foreign-ministers-meeting-rio-de-janeiro-april-28-2025.

⑤ “Global AI Ethics and Governance Observatory,” UNESCO, https://www.unesco.org/ethics-ai/en/brazil; Cristina Akemi Shimoda Uechi and Thiago Guimarães Moraes, “Brazil’s Path to Responsible AI,” OECD.AI Policy Observatory, July 27, 2023, https://oecd.ai/en/wonk/brazils-path-to-responsible-ai.

⑥ “GoGlobal Country Research, Indonesia AI Theme,” Equal Ocean, August 19, 2025, https://www.vzkoo.com/read/20250826e9353efd65c609059c526296.html.

出，全国约 5 700 万人无法获得稳定网络连接。此外，尽管印尼人口规模巨大，数字技术人才储备却严重不足，预计到 2030 年人才缺口将达到 900 万人。[①] 印尼技术评估与应用局发布的《国家人工智能战略（2020—2045）》（*Strategi Nasional Kecerdasan Artifisial Indonesia 2020-2045*），确定将医疗卫生、教育与研究、粮食安全、政府改革与智慧城市作为五大优先发展领域，计划每年培养 10 万名人工智能技术人才。该战略提出，由政府牵头设立多利益攸关方参与的政策协调框架，鼓励产业界、学术界、技术社群与政府一道设计技术路线、共享数据、调动投资，强化通信和信息部、国家发展规划署、卫生部、教育部、农业部、交通部以及地方政府之间的政策协调。[②] 2025 年 8 月，印尼通信与数字事务部起草了《国家人工智能白皮书与路线图》（*Buku Putih Peta Jalan Kecerdasan Artifisial Nasional*），以“包容、负责任、安全”为人工智能应用原则，规划了治理机制以及法律与体制改革的具体路线。[③] 为应对国内数字鸿沟和人才缺口，白皮书计划设立“主权人工智能基金”，对人工智能教育和连接性基础设施进行集中投资。[④] 上述两份国家级战略规划文件显示出印尼政府将人工智能纳入国家长期发展议程的政治意愿，为后续技术监管立法与国际合作实践奠定了政策框架基础。

第二，强化技术监管以应对安全风险。近年来，印尼对人工智能技术风险的敏感性凸显。2023—2024 年，印尼深度伪造欺诈案件数量激增 1550%。[⑤] 仅 2025 年

① “Komdigi Launches AI Policy Dialogue Country Report, Becomes the Basis For Making AI Policies,” VOI, July 29, 2025, https://voi.id/en/technology/499778.

② “Strategi Nasional Kecerdasan Artifisial Indonesia 2020-2045,” BPPT, August 10, 2025, https://oecd-ai.case-api.buddyweb.fr/storage//policy-initiatives/Jul2025/fu_4fi5jmh3ywepzcb.pdf.

③ “Buku Putih Peta Jalan Kecerdasan Artifisial Nasional,” Kementerian Komunikasi dan Digitall, Jakarta, August 2025, https://repository.radenintan.ac.id/39933/1/Buku%20Putih%20Peta%20Jalan%20KA%20Nasional.pdf.

④ Julian Isaac, “Indonesia Plans Sovereign AI Fund to Become Regional Technology Hub,” *Indonesia Business Post*, August 13, 2025, https://indonesiabusinesspost.com/4981/markets-and-finance/indonesia-plans-sovereign-ai-fund-to-become-regional-technology-hub#:~:text=The%20Ministry%20of%20Communication%20and%20Digital%20Application%20%28Komdigi%29,Indonesia%20as%20a%20regional%20hub%20for%20AI%20technology; “Indonesia Eyes ‘Sovereign AI Fund’ to Drive Development, Document Shows,” Reuters, August 11, 2025, https://www.reuters.com/world/asia-pacific/indonesia-eyes-sovereign-ai-fund-drive-development-document-shows-2025-08-11/.

⑤ “Deepfake Crimes in Indonesia: Legal Challenges and Criminal Liability in the AI Era,” SIP Law Firm, August 18, 2025, https://siplawfirm.id/deepfake-crimes-in-indonesia/.

上半年，印尼遭受的网络攻击数量达 36.4 亿次，为全球第十大网络攻击目标国。[①] 此外，印尼还是东南亚地区数据泄露账户记录数量最多的国家，达 1.44 亿条。[②] 为实现人工智能时代的国家安全，印尼政府持续推动数据本地化措施以维护数据主权，不断完善人工智能法律监管框架。2022 年，印尼通过《个人数据保护法》，为数据跨境传输构建了法律框架。该法规定，个人数据控制者虽可向境外传输数据，但离岸数据处理需监管部门批准，以确保监管监督和审计访问更为有效。[③] 2023 年，印尼通信与信息部发布了题为《人工智能伦理》的通函，提出了“公平性、人性化、安全性、透明度、问责制、隐私保护”等一系列伦理规范，对私营部门的人工智能研发起到指南和倡导作用。[④] 自 2024 年起，印尼启动了更具法律约束力的人工智能监管法案起草工作，拟对人工智能企业规定强制性的注册、评估和报告义务，并纳入风险分类管理制度。[⑤]

第三，通过国际技术合作推动本土能力建设。印尼对华技术合作持续扩大，展现出“主权人工智能”的务实合作特征。在国家级合作层面，印尼有关部门与中国国家互联网信息办公室续签《关于发展网络安全能力建设和技术合作的谅解备忘录》，形成了良好的互信基础。[⑥] 在企业合作层面，华为、阿里云和腾讯云等技术供应商已成为印尼人工智能能力建设的重要合作伙伴。2024 年，华为与印尼电信

① “Indonesia’s BSSN Records 3.64 Billion Cyberattacks in First Half of 2025,” Tempo, August 8, 2025, https://en.tempo.co/read/2037469/indonesias-bssn-records-3-64-billion-cyberattacks-in-first-half-of-2025.

② “Indonesia’s Cybersecurity Frontier: Embracing Data Sovereignty in the Digital Era,” Jagamaya, June 2, 2025, https://jagamaya.com/indonesias-cybersecurity-frontier-embracing-data-sovereignty-in-the-digital-era/.

③ “Undang-undang (UU) Nomor 27 Tahun 2022: Pelindungan Data Pribadi,” Indonesia Pemerintah Pusat, 2022, https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022%20.

④ “Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial,” Ministry of Communication and Informatics, December 19, 2023, https://jdih.komdigi.go.id/produk_hukum/view/id/883/t/surat%20edaran%20menteri%20komunikasi%20dan%20informatika%20nomor%209%20tahun%202023.

⑤ “AI Day Drives Indonesia’s AI Sovereignty, with Indonesia Leading Solutions and Connectivity,” Jakarta, November 18, 2024, https://www.thejakartapost.com/business/2024/11/18/ai-day-drives-indonesias-ai-sovereignty-with-indosat-leading-solutions-and-connectivity.html.

⑥《中国国家互联网信息办公室与印尼国家网络与密码局续签网络安全领域合作备忘录》，国家互联网信息办公室，2024 年 5 月，https://www.cac.gov.cn/2024-05/26/c_1718418714472207.htm。

公司 Indosat 合作，利用 5G 核心网络技术大幅提升 Indosat 用户网络流畅度。[①] 2025 年 6 月，印尼数字支付服务供应商 GoTo Financial 完成向阿里云雅加达数据中心的迁移，此次迁移旨在简化运营、降低成本和提高服务效率，并将所有数据保留在印尼境内以维护数据主权。[②] 在投融资方面，腾讯云承诺到 2030 年将在印尼基础设施和资源领域投资 5 亿美元建设其第三个互联网数据中心。[③] 印尼与中国企业的技术合作充分展现出其“主权人工智能”所具有的开放性战略自主特征：一方面，通过引入中国技术和资本加速数字基础设施建设；另一方面，通过本地化部署和数据主权要求，试图在技术依赖与自主可控之间寻求平衡。

第四，在全球治理中主张发展中国家权益和诉求。印尼通信和数字部已在多个区域和国际论坛上发起一系列人工智能政策对话，致力于构建以人为本、公平包容的人工智能治理体系，尤其关注发展中国家在人工智能治理中的特殊利益诉求。2025 年 2 月，在巴黎举行的全球人工智能伙伴关系（GPAI）部长级会议上，印尼通信与数字部长梅蒂亚·哈菲德（Meutya Hafid）指出：“必须确保人工智能政策反映发展中国家利益……印尼正制定合适的监管框架，并尝试将其与全球人工智能生态系统接轨。”[④] 东盟是印尼参与区域人工智能治理的重要平台，印尼积极参与东盟治理框架的构建，并发挥了积极作用。2024 年，东盟发布《东盟人工智能治理和伦理指南》，旨在促进区域内人工智能框架的“对齐”和互操作性建设。[⑤] 印尼分享了科技企业 Gojek 的分工治理架构，为区域性框架提供人工智能治理实践范例。[⑥] 此外，印尼在《伦理指南》制定过程中，积极主张保障成员国自主设立人工智能监管

① “Indosat and Huawei Boost Indonesia’s Connectivity with Network Consolidation,” Telecom Review, August 26, 2024, https://www.telecomreviewasia.com/news/network-news/4495-indosat-and-huawei-boost-indonesia-s-connectivity-with-network-consolidation/.

② “GoTo Group Migrates Digital Payments Unit to Alibaba Cloud,” Data Center Dynamics, 2025, https://www.datacenterdynamics.com/en/news/goto-group-migrates-digital-payments-unit-to-alibaba-cloud/.

③ “Tencent Cloud Commits US$500 Million Investment in Indonesia,” Yahoo Finance, 2024, https://finance.yahoo.com/news/tencent-cloud-commits-500-million-123237263.html.

④ Mochamad Azhar, “Indonesia Calls for Inclusive and Equitable AI Governance,” GovInsider, February 14, 2025, https://govinsider.asia/intl-en/article/indonesia-calls-for-inclusive-and-equitable-ai-governance.

⑤ Charles Labrecque, “ASEAN Issues Guidelines for Artificial Intelligence,” Asia-pacific Foundation of Canada, March 6, 2024, https://www.asiapacific.ca/publication/asean-issues-guidelines-artificial-intelligence.

⑥ Rifki Weno et al., “Artificial Intelligence (AI) and Digital Transformation in the ASEAN Region,” ASEAN Business Advisory Council, July 25, 2025, https://asean-bac.org/news-and-press-releases/artificial-intelligence-(ai)-and-digital-transformation-in-the-asean-region.

体系的权利，呼吁在东盟的区域性框架下维护各国的治理模式自主性。①

综上，巴西和印度尼西亚作为全球南方国家的典型代表，均基于自身的发展诉求和面临的安全风险，开展了体系化的制度设计，并积极建设和实践“主权人工智能”战略。两个案例共同表明，国家在人工智能产业规划中具有显著主导地位，推动人工智能监管立法也是两国的共同追求。巴西和印尼都倾向于开放国内市场，通过引入国外技术要素培育本土化产业，并在全球人工智能治理中主张发展中国家合理权益，体现了对自主话语权的追求。

四　中国面向“主权人工智能”的国际合作路径

“全球南方”的“主权人工智能”实践是一个多元包容的概念框架，全球南方国家的多样性决定了不同国家可能在“主权人工智能”实践中扮演差异化的国际角色。作为“全球南方”的重要一员，中国的人工智能政策实践就代表了“主权人工智能”一种相对特殊的情况。一方面，中国的人工智能发展与广大全球南方国家面临相似的风险挑战。在技术要素上，中国的先进芯片供应长期面临西方技术出口管制带来的“卡脖子”风险，亟须实现高端芯片的国产替代和供应链自主。② 在安全监管上，中国同广大全球南方国家一样，面对数据投毒、网络攻击、虚假信息等技术滥用风险时，具有敏感性和脆弱性，需通过扩展立法更好地实施技术监管。③ 另一方面，中国在人工智能技术水平和市场占有率方面均具备世界领先优势。根据斯坦福大学人工智能研究院统计，中国的人工智能专利申请数量和论文发表量稳居世界第一，顶级模型数量仅次于美国，排名世界第二。④ 此外，算力总规模和数据中心建设也处于世界第一梯队。⑤ 因此，中国并未像巴西和印度尼西亚那样，以追求技术追赶或规

① Karryl Kim Sagun Trajano, “Charting ASEAN’s Path to AI Governance,” The National Bureau of Asian Research, September 4, 2025, https://www.nbr.org/publication/charting-aseans-path-to-ai-governance-uneven-yet-gaining-ground/.

② 李巍、李玥译：《解析美国的半导体产业霸权：产业权力的政治经济学分析》，《外交评论》2022 年第 1 期。

③ Yoshua Bengio et al., “International AI Safety Report 2026,” February 2026, https://internationalaisafetyreport.org/sites/default/files/2026-02/summary-for-policymakers-2026-zh.pdf.

④ “The 2025 AI Index Report,” Human-Centered Artificial Intelligence, 2025, https://hai.stanford.edu/assets/files/hai_ai_index_report_2025.pdf.

⑤《先进计算暨算力发展指数蓝皮书（2025 年）》，中国信通院，2026 年 3 月，https://www.caict.ac.cn/kxyj/qwfb/bps/202603/P020260306392232241580.pdf。

避依附性发展为目标，而是在实现供应链自主和安全监管的同时，利用自身优势帮助其他全球南方国家进行能力建设，团结全球南方国家在人工智能治理领域争取话语权。中国是广大全球南方国家开展“主权人工智能”实践的重要合作伙伴。

（一）面向“全球南方”的合作共赢理念

中国的人工智能国际合作模式体现出两大核心特征：一是尊重各国自主的治理模式，二是秉持非零和博弈的安全观。

与欧盟凭借“布鲁塞尔效应”构建规范性权力，进而吸引其他国家将技术标准和监管路径向其靠拢的做法不同，中国尊重各国基于自身治理能力和治理范式建立技术监管体制，不强制要求其他国家加入或接受中国的治理方法和技术标准。2023 年 10 月，中国发布《全球人工智能治理倡议》（简称《倡议》），“欢迎各国政府、国际组织、企业、科研院校、民间机构和公民个人等各主体秉持共商共建共享的理念，协力共同促进人工智能治理”。[①] 《倡议》强调，“尊重各国主权、领土完整和发展利益”，“尊重各国自主选择的人工智能发展道路和治理模式”。[②] 这一表态明确传递出中国不将自身治理模式强加于人、尊重各国制度差异的基本立场。

中国不以牺牲其他国家的发展为代价来维持自己的技术领先地位，不借助技术垄断和技术遏制来制造技术依附，并尽可能避免人工智能加剧大国间军备竞赛、产生安全困境。相较而言，自特朗普第一任期以来，美国一直以国家安全为由开展对华技术竞争，频繁利用技术出口管制对非盟友国家开展技术封锁。中美两国的安全逻辑截然不同。正如习近平主席于 2022 年提出的全球安全倡议所言，应“坚持重视各国合理安全关切。人类是不可分割的安全共同体，一国安全不应以损害他国安全为代价”。[③] 这一主张充分体现了中国不以技术领先优势谋求霸权，而是致力于以发展谋安全、以合作促安全的取向。

（二）以能力建设赋能“主权人工智能”

2024 年 7 月，联合国大会通过了中国提出的加强人工智能能力建设国际合作

①《全球人工智能治理倡议》，中国外交部网站，2023 年 10 月，https://www.fmprc.gov.cn/web/ziliao_674904/1179_674909/202310/t20231020_11164831.shtml。

②《全球人工智能治理倡议》，中国外交部网站，2023 年 10 月，https://www.fmprc.gov.cn/web/ziliao_674904/1179_674909/202310/t20231020_11164831.shtml。

③《全球安全倡议》，中国外交部网站，2023 年 2 月 21 日，https://www.mfa.gov.cn/wjbxw_new/202302/t20230221_11028322.shtml。

决议。[①] 2024 年 9 月，中国发布《人工智能能力建设普惠计划》，系统地阐述了人工智能能力建设的目标和行动路径，包括促进人工智能和数字基础设施联通、推进“人工智能+”赋能千行百业、加强人工智能素养和人才培养、提升人工智能数据安全和多样性、确保人工智能安全可靠可控等。[②] 这两份文件标志着中国已形成面向“全球南方”围绕“主权人工智能”开展能力建设工作的系统性思考。中国的“能力建设者角色”主要体现在两个层次：

首先，中国积极推动开源，助力全球南方国家部署和采用中国的大模型。开源模型通过免费共享代码、参数与训练方法，显著降低了技术准入门槛，使“全球南方”开发者能以极低成本定制垂直模型。[③] 目前，DeepSeek 的 V3 模型、百度的文心大模型、阿里巴巴的通义千问系列模型、华为的盘古大模型都已经采用开源模式向全球南方国家开放。模型开源体现了中国对人工智能技术跨国流动性的尊重，让全球南方国家避免因技术价格高昂而被排除在发展浪潮之外；同时，代码的透明性使各国能够审查算法逻辑，确保模型输出符合本国价值观和监管要求。[④]

其次，中国主张因地制宜开展国际合作，结合“全球南方”的资源禀赋和发展诉求，提供定制化的本地技术部署方案。2025 年，“中国—东盟人工智能创新合作中心”系列项目在广西南宁投入（试）运营。[⑤] 广西提出“北上广研发+广西集成+东盟应用”路径，规划建设国际数据中心、算力中心集群、东盟国家语料库、中国—东盟人工智能算力调度平台等项目，鼓励中国企业直接将技术解决方案与东盟本土市场诉求对接。[⑥] 定制化的人工智能解决方案在尊重“全球南方”自身利益诉求的同时，为各国的战略自主保留了空间，使各国能够在国际合作中实现对产业和技术路线的控制权，体现了“主权人工智能”对开放性战略自主的追求。

① “Enhancing International Cooperation on Capacity-building of Artificial Intelligence,” United Nations General Assembly, July 1, 2024, https://digitallibrary.un.org/record/4054005?ln=en&v=pdf.

②《人工智能能力建设普惠计划》，中国外交部网站，2024 年 9 月 27 日，https://www.mfa.gov.cn/web/wjbz_673089/xghd_673097/202412/t20241218_11496414.shtml。

③ 魏钰明、贾开、曾润喜等：《DeepSeek 突破效应下的人工智能创新发展与治理变革》，《电子政务》2025 年第 3 期。

④ 席恒、王涵：《以开源通用模型奠定数字社会主义的技术基石》，《金融时报》2025 年 4 月 7 日。

⑤《中国—东盟人工智能创新合作中心系列项目投入（试）运营，新华网，2025 年 7 月 2 日，http://www.gx.xinhua.org/20250702/19869783b265419a8c1adfb2d8175779/c.html。

⑥《中国—东盟人工智能创新合作中心展示中心项目开建》，中国新闻网，2025 年 4 月 3 日，https://www.chinanews.com.cn/cj/2025/04-03/10394237.shtml；《“A 超”启航 智联东盟》，新华网，2025 年 12 月 5 日，https://www.xinhuanet.com/tech/20251205/9d5fccdfb23447f08a3b38c5ec4fe7fe/c.html。

（三）提升“全球南方”在人工智能治理中的参与度与话语权

作为全球南方国家建设“主权人工智能”的重要伙伴，中国积极参与和引领全球治理规则的制定，推动建立更加公平、包容、多元的人工智能治理体系。

“数字丝绸之路”作为中国“一带一路”倡议在数字经济领域的核心延伸，已超越传统基础设施互联互通的范畴，成为中国开展高水平人工智能国际合作的关键平台。[①] 2023 年 10 月，中国依托“数字丝绸之路”框架提出《全球人工智能治理倡议》，明确提出“增强发展中国家在人工智能全球治理中的代表性和发言权”，“确保各国人工智能发展与治理的权利平等、机会平等、规则平等”。[②] 这表明，“数字丝绸之路”有能力为沿线国家构建“主权人工智能”提供更具包容性的实践平台。

作为新兴市场和发展中国家的代表平台，“金砖国家”已成为推动全球人工智能治理改革的重要力量。中国积极参与“金砖国家”机制，旨在团结全球南方国家，在人工智能治理进程中发出共同声音。2025 年 7 月，金砖国家领导人第十七次会晤通过《金砖国家领导人关于人工智能全球治理的声明》，系统地阐述了金砖国家人工智能治理合作的共同立场：捍卫多边主义与数字主权，反对治理碎片化，弥合数字鸿沟，倡导协同治理与开放创新。[③] 这些主张充分反映了全球南方国家在人工智能治理中的共同诉求。

在联合国框架下，中国主张将联合国作为国际规则协商的核心平台，广泛吸纳全球南方国家参与治理进程。[④] 2024 年 7 月，第 78 届联合国大会经过协商，一致通过中国提出的加强人工智能能力建设国际合作决议，旨在帮助发展中国家从人工智能发展中平等受益，弥合数字鸿沟。该决议由超过 140 个成员国联署，其中绝大多数为全球南方国家。[⑤] 2024 年 12 月，傅聪大使在安理会“人工智能与维护国际和平与安全”公开会上发表演讲，呼吁遵循《联合国宪章》宗旨原则，反对以意识形态划界建立歧视性壁垒，损害各国特别是发展中国家平等利用新兴科技的权

---

①《世界互联网大会将积极推动“数字丝路”发展建设》，光明网，2025 年 7 月 3 日，https://politics.gmw.cn/2025-07/03/content_38132928.htm。

②《全球人工智能治理倡议》，中国外交部网站，2023 年 10 月，https://www.fmprc.gov.cn/web/ziliao_674904/1179_674909/202310/t20231020_11164831.shtml。

③《金砖国家领导人关于人工智能全球治理的声明》，中国外交部网站，2025 年 7 月 9 日，https:// www.fmprc.gov.cn/web/zyxw/202507/t20250709_11668022.shtml。

④ 阙天舒、郑兆辰：《“全球南方”参与人工智能国际治理的挑战及中国选择》，《当代中国与世界》2025 年第 3 期。

⑤《联大通过中国提出的加强人工智能能力建设国际合作决议》，中国政府网，2024 年 7 月 2 日，https://www.gov.cn/yaowen/liebiao/202407/content_6960524.htm。

利。[①] 这充分体现了中国对全球南方国家发展诉求的高度重视。

结　语

文章分析了“主权人工智能”的学理逻辑与实践内涵，并阐释了全球南方国家选择“主权人工智能”发展模式的外部约束和内生动力。在理论上，“主权人工智能”反映出人工智能治理中“国家角色回归”的普遍趋势。人工智能的通用性技术特征及技术要素的跨国流动性重构了国家安全议题的具体任务，扩展了国家安全的物理空间，使“主权人工智能”具有议题领域的统筹性和“开放—自主”的平衡性。国家建设“主权人工智能”的最终价值在于相互尊重利益诉求和发展模式差异，实现平等包容的多样性国际秩序。在实践层面，通过构建一个基于主权对内“最高性”与对外“独立性”的分析框架，研究揭示了“主权人工智能”是全球南方国家在国际权力结构不对称、技术鸿沟持续扩大的背景下，为维护国家自主性、构建更平等国际秩序所采取的战略回应。

巴西和印度尼西亚的案例研究展现了“主权人工智能”对全球南方国家技术水平的提升具有显著成效。在对内层面，巴西与印尼政府都通过战略规划、立法监管，协调人工智能发展中的“创新—监管”矛盾；在对外层面，两国借助国际合作策略，促进本土技术产业发展，并在全球人工智能治理进程和规则制定中主张凸显发展中国家的话语权。

中国始终秉持平等共赢的发展理念，尊重各国在技术治理中的制度差异与安全诉求：以能力建设为首要任务，推动开源战略与定制化技术援助相结合的国际合作模式；以联合国为核心，以“数字丝绸之路”和“金砖国家”为重要机制，推动人工智能治理体系改革，强化“全球南方”的话语权。中国的实践超越了传统地缘政治竞争的叙事，开创了人工智能国际合作新范式。

【来稿日期：2025-12-30】
【修回日期：2026-02-26】
【责任编辑：周子淙】

① 中国常驻联合国代表团：《傅聪大使在安理会“人工智能与维护国际和平与安全”公开会上的发言》，2024 年 12 月 19 日，https://un.china-mission.gov.cn/chn/hyyfy/202412/t20241220_11507076.htm。

[Abstract] In recent years, the bio-hegemon has increasingly weaponized biological capacities to monopolize high-end ecological niches amid the third biotechnology revolution. However, existing literature is largely confined to linear narratives of binary confrontations, lacking a systematic analysis of the interaction between competition and cooperation within biological power networks. This study integrates fundamental ecological principles to construct a theoretical framework that explains how the hegemonic power enhances its strength through "selective cooperation" and "panoramic containment." This study reveals that the bio-hegemon distorts the evolutionary logic of the international ecosystem by adopting structural configurations and exploiting the potential of niche differentiation. Specifically, on fentanyl-related issues, where niches are adjacent and domestic governance crises are intensifying, the hegemonic power transforms symbiotic cooperation into "parasitic cooperation," imposing governance risks on China through coercive functional collaboration. In the field of advanced biotechnology, overlapping niche positioning triggers potential displacement anxiety. The hegemonic power employs "blocking competition" to construct technical barriers, forcibly hindering China's niche advancement. In the bio-manufacturing sector with overlapping niches but lower target positional power, the hegemonic power promotes the restructuring of biological supply chains and industrial repatriation through expansionary competition strategies. These analyses unveil the internal logic behind the hegemonic power's niche maintenance strategy. Meanwhile, they provide a co-evolutionary paradigm of organizational ecology for avoiding the Thucydides Trap in bio-strategic competition. This study offers important theoretical insights for building a symbiotic and inclusive global biotechnology governance system.
[Keywords] bio-coopetition, biosecurity governance, niche maintenance, U.S. strategy towards China
[Author] PAN Ziyang, Joint Ph.D. Candidate, School of International Studies, Renmin University of China (Beijing, 100872) and S. Rajaratnam School of International Studies, Nanyang Technological University (Singapore, 639798).

[Abstract] "Sovereign AI" refers to the governance of Artificial Intelligence (AI) led by sovereign states: domestically, it relies on the "supremacy" of sovereignty to strike a balance between industrial development and security risks; externally, it leverages the "independence" of sovereignty to pursue strategic autonomy and international influence. The theoretical implication of this concept derives from the technological characteristics of AI. The rapid iteration and inherent uncontrollable nature of AI compels states to assert their agency in technology governance. The general-purpose nature of AI requires state power to coordinate across multiple security domains. The cross-border mobility of technological factors of AI necessitates that "sovereign AI" pursue strategic autonomy premised on openness. To counter the monopolization of technical standards and governance rules, "sovereign AI" must assert its voice in international rule-making, thereby upholding the value of diversity in the global order. In recent years, an increasing number of Global South countries have been leveraging a

"sovereign AI" strategy to respond to constraints such as "inadequate technological elements," "vulnerability to security risks," "structural inequality," and "imbalanced governance discourse power." The cases of Brazil and Indonesia demonstrate that "sovereign AI" plays a constructive role in empowering the Global South countries to achieve technological autonomy, safeguard national security, and enhance their discursive power. As a natural member of the Global South, China adopts a cooperative response towards "sovereign AI," featuring a spirit of cooperation based on equality and mutual benefit, a capacity-building model integrating open-source strategies with localized deployment, and a solidarity approach to enhance global AI governance engagement.
[Keywords] sovereignty, artificial intelligence, national security, Global South, technology governance
[Authors] ZHANG Shuyan, Ph.D. Candidate, School of International Relations and Public Affairs, Fudan University; CHEN Zhimin, Professor, School of International Relations and Public Affairs, Fudan University (Shanghai, 200433).

[Abstract] Based on the dual analytical framework of "security status–security capacity," this article systematically examines points of consensus and divergence among Global South countries in their participation in global security governance. The findings reveal that, in terms of objective security status, the Global South confronts common challenges, including threats to sovereign independence, inadequate economic autonomy, and deficient discursive influence in security affairs. In terms of subjective perceptions of security governance, the Global South has forged a conceptual consensus centered on multilateralism and common security, advocating structural reforms of the global governance system while upholding a development-oriented approach. In the field of security capacity building, efforts are directed toward institutional integration, resource coordination, and norm development. However, within the Global South, there exist divergent orientations regarding identity construction and governance objectives, differences in the selection of security issues and development preferences, and varying modes of action, including embedded reform, parallel institution-building, and regionalized security approaches. To address these complex dynamics, the authors propose constructing a security architecture featuring hierarchical alignment and functional complementarity to meet differentiated demands, innovating mechanisms of issue linkage and resource integration to reconcile diverse preferences, promoting synergy among multiple pathways to accommodate varied action choices, and focusing on security capacity building to solidify the security foundations of the Global South. These efforts aim to provide theoretical insights and practical pathways for advancing the transformation of the global security governance system toward a more equitable, inclusive, and sustainable transformation.
[Keywords] Global South, global security governance, governance consensus, governance divergences
[Authors] HUA Minchao, Associate Professor, National Security College, Southwest University of Political Science and Law; CHEN Chen, M.A. Student, National Security College, Southwest University of Political Science and Law (Chongqing, 401120).

（本期英文编辑：张国帅）