

海合会国家数字治理的路径、挑战 与对华合作^[1]

梁玉红 罗林

【内容提要】随着全球数字化进程的加速，数字治理已成为国家现代化转型与全球竞争力塑造的关键领域。一方面，海合会国家将数字化转型视为推动经济发展和社会治理现代化的新契机，并通过建立健全制度法规、强化教育和培训以及加强区域和国际合作，积极提升数字治理能力。但这些国家长期对美西方技术与基础设施的依赖，使其在实现数字主权、数字治理话语权、网络和数据安全等方面面临国际、区域与国内层面的多重挑战。另一方面，为加速推进数字经济“跨越式发展”，海合会国家也积极加强与中国在数字领域的合作；同时，中国提出的全球治理倡议等主张也为中国同海合会国家在数字领域的合作提供了重要引领。海合会国家的探索实践为全球南方国家推动数字化转型和参与全球数字治理提供了重要参照。

【关键词】海合会国家 数字治理 人工智能 中阿合作 全球南方 全球治理倡议

【作者简介】梁玉红，广东金融学院外国语言与文化学院讲师，北京语言大学2024级博士研究生；罗林，北京语言大学国别和区域研究院院长、教授。

【中图分类号】D815

【文献标识码】A

【文章编号】1006-6241 (2025) 06-0138-28

[1] 本文系国家社会科学基金重大项目“阿拉伯史学经典《历史大全》的汉译与研究”（项目编号：19ZDA238）的阶段性成果。作者感谢《和平与发展》匿名评审专家及编辑部对本文提出的宝贵修改意见，文中错漏概由本人负责。

当今世界，信息技术创新日新月异，以人工智能、大数据、云计算、区块链等为代表的数字技术快速迭代发展，大大拓展了人类的经济社会活动范围和认知边界，成为重塑全球产业结构和要素资源、改变全球竞争格局的重要力量。与此同时，数字技术的发展也给各国的国家安全、网络和数据安全等带来诸多挑战——个别国家凭借其数字霸权，搞“小院高墙”式的技术封锁，严重侵害他国主权、安全和发展利益；少数大型科技企业垄断全球数字经济资源和产业，甚至通过断供断链等方式在地缘政治冲突中“选边站队”；伴随数字技术快速发展出现的“算法黑箱”“深度伪造”“信息茧房”等问题，对经济社会发展构成风险，等等。^[1]所有这些都使得数字治理的重要性日益凸显。就数字治理的定义而言，欧美国家主要强调对数字环境中出现的新问题的监管，以及制定相应的规则、规范和制度。^[2]中国所倡导的数字治理通常包括两方面的含义，一是运用数字化、智能化手段提升既有治理体系效能，提高治理的科学性、精准度和有效性，即“数字赋能治理”；二是针对数字化进程中平台经济、技术应用等带来的新问题建立相应的响应和规范机制，从而构建起有效的控制、协调、激励与信任体系，即“对数字化的创新治理”。^[3]

作为治理体系现代化的核心组成部分，数字治理不仅涉及信息基础设施建设、数据安全与网络秩序维护，还直接关系到国家主权的延伸、经济的发展和运行的稳定。哈佛商学院名誉教授肖莎娜·祖博夫（Shoshana Zuboff）认为，数字技术带来的数字治理挑战将会引发一场“认知革命”，

[1] 周靖、孙南翔：《让数字技术更好造福全人类 汇聚完善全球数字治理的强大合力》，载《人民日报》2025年11月27日，第9版。

[2] 参见 Digital Government of United States, “An introduction to digital governance,” <https://digital.gov/resources/an-introduction-to-digital-governance/>; Council of Europe, “Digital Governance,” <https://www.coe.int/en/web/digital-governance/overview%20>; David Zamora et al, “Case: Digital Governance Office,” *Journal of Business Research*, Vol. 69, No.10, 2016 等。

[3] 参见李韬、冯贺霞：《数字治理的多维视角、科学内涵与基本要素》，载《南京大学学报（哲学·人文科学·社会科学）》2022年第1期，第76页；魏礼群、顾朝曦、倪光南等：《数字治理：人类社会面临的新课题》，载《社会政策研究》2021年第2期，第3—12页；张鸿：《数字治理》，北京：清华大学出版社2023年版，第6—11页等。

并将重新定义 21 世纪的社会秩序。^[1] 欧洲左翼和马克思主义学者更是认为这种数字技术带来的治理挑战已经不再属于资本主义范畴,而是一种“技术封建主义”。^[2] 由此可见,数字治理问题在近些年已经成为被高度关注的焦点议题,而围绕数字治理模式的竞争博弈也日趋激烈。许多国家相继提出了不同的数字治理方案和路径,使得关于数字主权、数字发展权的博弈成为数字时代国际竞争的核心场域。例如,美国凭借科技优势,主张建立开放式的“数据自由流动”模式,方便其利用技术优势对外进行“超主权垄断”,以维护其数字霸权。欧盟以维护“基本权利”为名,通过产业政策和数字监管来推进相关议程^[3],以增强其在全球数字治理中的规范塑造能力。中国则强调数字主权和公平正义,主张统筹发展和安全,构建网络空间命运共同体。^[4]

近年来,以沙特阿拉伯(以下简称沙特)、阿拉伯联合酋长国(以下简称阿联酋)等海湾阿拉伯国家合作委员会(以下简称海合会, GCC)国家为了摆脱对能源经济的高度依赖,实现经济的多元化转型,开始着手将数字化发展作为实现“后石油时代”经济可持续发展的核心支柱。总的看,海合会国家经济持续稳步增长,人均 GDP 超过 3.6 万美元^[5],人口规模较小且比较年轻,一半以上人口在 25 岁以下^[6],受教育特别是高等教育程度

[1] Shoshana Zuboff, “The Coup We Are Not Talking About,” *The New York Times*, January 29, 2021, <https://www.nytimes.com/2021/01/29/opinion/sunday/facebook-surveillance-society-technology.html>.

[2] [法]雅德里克·朗迪:《技术封建主义》,陈荣钢译,北京:中国人民大学出版社 2024 年版,第 176—178 页。

[3] Benjamin Farrand, Helena Carrapico, “Digital Sovereignty and Taking Back Control: From Regulatory Capitalism to Regulatory Mercantilism in EU Cybersecurity,” *European Security*, Vol.31, No.3, 2022, pp.435–453.

[4] 参见《中国关于全球数字治理有关问题的立场(就制定“全球数字契约”向联合国提交的意见)》,外交部网站,2024 年 1 月, https://www.mfa.gov.cn/wjb_673085/zjg_673183/jks_674633/zclc_674645/qt_674659/202305/t20230525_11083602.shtml。

[5] 参见 General Secretariat of GCC, “HE GCCSG: The Allocation of a Gulf Dialogue Session Within the Asian Financial Forum 2025 Highlights the Economic Standing of The GCC Countries in Regional and International Arenas,” January 14, 2025, <https://www.gcc-sg.org/en/MediaCenter/News/Pages/news-2025-01-14-4.aspx>。

[6] PwC, “Middle East Youth Outlook 2024,” August 26, 2024, <https://www.pwc.com/m1/en/publications/middle-east-youth-outlook-2024.html>。

较高，加之君主制有利于提升顶层设计的效率，这些因素共同构成了这些国家实现数字化转型得天独厚的优势。一方面，它们积极推进数字化转型，使其从数字领域的“追随者”转变为“领先者”和“探索者”，并成为全球南方国家数字化发展的标杆；另一方面，这些国家在数字技术、基础设施和信息生态等方面对外部具有较强的依赖性，既使其在网络和数据安全等领域面临较大的脆弱性，也使其成为对国际数字竞争博弈具有重要潜在影响的“中间地带”。因此，提高自身数字治理水平和能力已经成为海合会国家亟待解决的问题，它们力图在发展数字经济和抵制数字霸权之间求得平衡，努力探索符合自身特点的数字治理路径。

本文将尝试分析海合会国家因数字化转型而产生的治理问题，解析这些国家数字化“跨越式发展”的路径，以及其在数字治理领域面临的挑战，并探讨海合会国家与中国在数字治理领域的合作实践，揭示这些国家相关探索对全球南方推动构建开放、包容、公平和普惠的全球数字治理体系的启示，为学界和实务界相关研究提供参考。

一、海合会国家的数字化转型

从海合会国家发展和治理的数字化转型历程来看，大体可以分为三个阶段。第一阶段是20世纪90年代末至本世纪初的“政府上网”，海合会各成员国政府建立官方网站，将互联网技术作为提供信息发布等基础服务的工具；第二阶段是本世纪初至本世纪10年代初的“电子政务和商务”，域内各国利用网络空间从信息发布转向提供在线交易等服务；第三个阶段是本世纪10年代中期至今的“数字化转型”，各国政府都注重发挥数据驱动和人工智能（AI）在国家发展和社会治理中的作用。事实上，在上述的前两个阶段，海合会各国政府仅是将网络技术作为处理日常事务的辅助手段，而第三个阶段的数字技术赋能则在其国家发展和社会治理中发挥了核心功能。特别是在当前全球数字化加速推进的背景下，海合会国家的数字化转型不仅是推动其国家发展转型的重要战略抓手，也是其应对全球竞争与区域安全挑战的必然选择。

（一）将数字化转型作为国家发展战略的基石

为应对全球能源格局变化和内部社会经济转型的双重挑战，以及推动经济发展多元化与社会治理现代化，海合会国家近些年来均制定了长期国家发展战略。^[1] 这些战略均将数字化作为实现经济多元化和提升国家竞争力的重要方案，其核心内容包括：一是国家数字化战略。海合会国家的数字化战略都是由国家层面主导并上升到国家宏观战略层面，被视为提升政府效能、推动经济增长和增强企业韧性的重要引领。例如，早在2013年，卡塔尔就将打造“数字政府”列为优先事项，提出《卡塔尔数字政府战略2020》，该战略旨在通过数字技术来打造一个更高效、更便捷、更透明的政府。^[2] 此后，其他海合会国家也相继制定了各自的数字化战略，包括阿曼的《阿曼数字社会与数字政府国家战略》、阿联酋的《阿联酋数字政府战略2021—2025》、沙特的《国家转型计划》、巴林的《2022 数字政府战略》和科威特的《数字转型战略》。近年来，各成员国的数字战略已在原有基础上陆续升级：阿曼发布《政府数字转型计划2021—2025》，阿联酋推出新版数字化转型与数字经济战略，沙特对《国家转型计划》持续迭代，巴林在2022战略基础上扩展数字经济规划，总体呈现从数字政府向数字国家与数字经济拓展的趋势。

二是国家人工智能战略。近年来，基于大数据的人工智能技术迅猛发展，已成为推动全球经济发展的新引擎。正如英国谢菲尔德大学学者克莱夫·亨比（Clive Humby）所言，“数据是新的石油”。^[3] 海合会国家将发展人工智能视为摆脱对石油资源依赖、重构国家经济体系的新动力，并制定了各自

[1] 这些战略包括巴林的“2030 经济愿景”、科威特的“2035 愿景”、阿曼的“2040 愿景”、卡塔尔的“2030 国家愿景”、沙特的“2030 愿景”以及阿联酋的“2031 愿景”。

[2] Ministry of Information and Communications Technology, *Qatar e-Government 2020 Strategy*, <https://hukoomi.gov.qa/assets/documents/qatare-government-2020-strategy-executive-summary>. Pdf.

[3] 参见谢菲尔德大学网站的克莱夫·亨比个人简介, <https://sheffield.ac.uk/cs/people/academic-visitors/clive-humby>。

的国家人工智能战略。^[1]其中，阿联酋和沙特已成为区域 AI 发展的核心驱动者与制度引领者。根据国际金融论坛（IFF）2025 年 2 月发布的全球人工智能竞争力指数报告，在每百万人口拥有 AI 公司最多的前十个国家和地区中，阿联酋排名第九，凸显了该国致力于成为 AI 和数字化转型全球领导者的雄心。^[2]根据波士顿咨询集团（BCG）2025 年 4 月发布的一份专门评估海湾地区人工智能发展状况的报告，阿联酋、沙特等国被列入了“人工智能竞争者”类别，仅次于美国和中国等顶级“先驱者”水平的国家。^[3]

（二）着力推进经济发展的数字化转型

数字化是海合会国家实现经济多元化转型的核心抓手与战略支撑，大力发展数字经济已成为这些国家经济发展战略的首要目标。

一是加强数字经济基础设施建设。海合会各国着力加大在数字基础设施领域的资金投入，强化支撑数字经济运行的物理基础和技术平台建设。例如，在阿联酋，诸多人工智能与技术基础设施企业，如 G42、AIQ、THI、Etisalat 等，不仅致力于国内人工智能研发能力的建设，同时在全球范围内部署数据基础设施、提供模型应用及相关电信与技术服务，形成了跨国技术能力网络。^[4]科威特联合华为等中国企业及其国内三大运营商

[1] 例如，2019 年以来卡塔尔颁布《国家人工智能战略》、科威特颁布《2025—2028 国家人工智能战略》、阿曼制定《人工智能与数字未来计划 2024—2026》、巴林制定《人工智能战略》。

[2] International Finance Forum, “IFF Global AI Competitiveness Index Report Highlights UAE's Achievements in AI,” February 24, 2025, <https://www.ifforum.org/index.php/show/7430>.

[3] Akram Awad et al, “The GCC AI Pulse: Mapping the Region's Readiness for an AI-Driven Future,” Boston Consulting Group, April 22, 2025, <https://www.bcg.com/publications/2025/the-gcc-ai-pulse-mapping-the-regions-readiness-for-an-ai-driven-future#:~:text=In%20this%20inaugural%20study%2C%20we%20assess%20the%20development%20Policy%2C%20Investment%2C%20Research%2C%20and%20Ecosystem%20across%2030%2B%20indicators>.

[4] Kristina Fort, Nikhil Mulani, “AI Oases: Leveraging Gulf AI Ambitions for U.S. Strategic Objectives,” *SSRN 5344463*, 2025, p.13.

(Ooredoo、Zain 和 Stc) 等公司大力推动 5G-A 技术的全国性部署, 成为在全球最先推进 5G-A 技术商业应用的国家之一, 并以此强化数字经济技术设施。阿曼电信监管局已向其国内运营商分配相关频谱, 用于开展免费的 6G 技术创新试验。^[1]

二是推进数字产业发展。海合会国家积极推动为数字化发展提供技术、产品、服务和基础设施的基础产业发展。沙特和阿联酋将构建完整数字产业生态作为重要目标。沙特通过公共投资基金 (PIF) 主导数字产业体系建设, 推动人工智能、云计算与网络安全协同发展。2025 年成立的 Humain 公司是落实沙特国家人工智能战略的关键平台; 沙特阿美 (Aramco) 在能源数字化与智能管理方面发挥龙头作用; DataVolt 公司承担数据中心建设任务, 为“2030 愿景”提供基础设施支撑。阿联酋在推动数字商务发展方面取得了显著进展。早在 1996 年, 迪拜机场自由区便开始运营, 随后在 2005 年成立了迪拜硅谷绿洲, 致力于科技创新与企业孵化。2021 年, 迪拜商业城成立, 进一步推动了数字商务生态的发展。卡塔尔和巴林则致力于打造区域性数字经济枢纽, 寻求合作和差异化发展之路, 与沙特和阿联酋市场形成互补, 并通过数字产业平台建设和数字人才培养, 提高自身吸引力。

三是加快产业数字化。海合会国家通过将数字技术、数据资源与传统产业深度融合, 推动了传统产业的产出增加和效率提升。在第一产业层面, 沙特和科威特已着手推进精准农业与水资源管理的数字化, 开始逐步扭转海合会国家农业数字化程度普遍较低的局面。在第二产业层面, “智慧能源”成为这些国家工业数字化转型的核心方案。该方案包含实现油田的数字化管理和提升先进数字技术嵌入水平。例如, 阿联酋的阿布扎比国家石油公司将数字孪生与人工智能等技术深度融合, 有效预测设备停机, 提高可靠性和安全性, 并节省了高额维护成本。^[2] 在第三产业层面, 海合会国

[1] “The evolution of 5G: the Gulf’s path to an ultra-connected future,” Mobile World Congress Doha, September 26, 2025, <https://www.mwcdoha.com/articles/the-evolution-of-5g-the-gulf-path-to-an-ultra-connected-future>.

[2] The Abu Dhabi National Oil Company, “ADNOC Completes First Phase of Artificial Intelligence Predictive Maintenance Project,” November 10, 2020, <https://www.adnoc.ae/en/news-and-media/press-releases/2020/adnoc-completes-first-phase-of-artificial-intelligence-predictive-maintenance-project/>.

家在金融服务、数字支付及政府服务的数字化等方面已处于全球领先水平。在央行数字货币领域，沙特和阿联酋率先启动了“Aber”试点项目，旨在评估两国央行联合发行数字货币用于金融结算的可行性；而卡塔尔和巴林等国则采取了相对谨慎的态度，通过小范围试点的方式，稳步推进金融改革。同时，得益于数字基础设施的完善以及物联网技术的应用，海合会国家的电子商务也增长迅猛，并成为新的经济增长点。据相关专业机构预计，截至2025年末，海合会国家企业的电子商务规模将超过500亿美元。^[1]

（三）积极推进国家治理的数字化转型

在全球南方，海合会国家是运用数字赋能国家治理的积极实践者和领跑者，它们利用大数据、云计算和人工智能等新一代信息技术，对治理理念和治理结构等层面进行全方位、系统性变革，并取得了引人瞩目的成绩。

一是公共治理数字化程度明显提高。海合会国家的数字化公共治理平台在整合社会资源和提升效率方面表现出色，加快了政府数字治理的步伐。特别是在新冠疫情期间，这些国家广泛利用人工智能等技术进行公共场所人流识别、病例预测、医疗物资调配与虚假信息监测^[2]，在疫情预防、治疗药品研发和医疗管理等领域都发挥了重要作用。在后疫情时代，数字化同样为公共治理提供了强有力的技术支撑，例如，迪拜推出“无警警务”（Police Without Policemen）、“Oyoon”人脸识别等系统，并部署人工智能安全机器人以提升城市治安管理能力。^[3]总的看，海合会国家在数字连接（digital connectivity）方面成就斐然。据全球移动通信系统协会（GSMA）预测，到2030年海合会国家5G普及率平均可达95%，不仅高于亚太发达地区和北美，

[1] Competenza Innovare, “Enterprise E-Commerce in the GCC: A Complete Guide for 2025,” September 1, 2025, <https://competenza.ae/blog/enterprise-e-commerce-in-the-gcc/>.

[2] Rahaf AL Khazraji, “Utilizing Artificial Intelligence against COVID-19,” Trends Research and Advisory, August 26, 2020, <https://trendsresearch.org/insight/utilizing-artificial-intelligence-against-covid-19/>.

[3] “Dubai Police proposes tech-based ‘Police without Policemen’ project,” OpenGov Asia, March 14, 2018, <https://archive.opengovasia.com/2018/03/14/dubai-police-proposes-tech-based-police-without-policemen-project/>.

更

色杜系等绸年该总化发济

改通用例訪20室的在在

3, 1
eco

在
202

建设中引入了智能冷却系统，通过实时监测与自动化调节机制实现能源使用的最优配置。阿联酋则通过“Smart Dubai”计划整合交通、安防、能源与政务系统以及多类智能设备数据，实现对城市运行与公共服务的更精准管理。^[1]

二、海合会国家数字治理的路径

海合会国家的数字化进程也伴随着一系列结构性挑战与潜在隐忧。本土数字创新生态的培育尚处于初级阶段，数据安全和隐私保护问题在日益频繁的网络交互中愈发凸显，而依赖外部技术平台所带来的主权风险也不容忽视，这使得如何有效加强数字治理成为这些国家亟需解决的关键问题。围绕立法、制度建设、教育与国际合作，域内各国正在探索多维度的治理路径，以在全球竞争与区域合作中塑造更加稳固、自主的数字治理格局。

（一）完善数字治理制度

维护数字主权已成为海合会各国实现现代化和经济多元化的关键。为此，这些国家普遍通过完善数字安全管理与监管体系，为数字治理提供制度保障。

一是设立专门机构，强化数字安全监管。根据美国 IBM 公司 2024 的研究，中东地区网络安全事件的平均成本已达到每次 693 万美元，显著高于全球平均水平的 424 万美元。^[2] 网络和数据安全是数字治理的基础，也是海合会国家关注的焦点。沙特于 2017 年设立了国家网络安全局（NCA，旨在取代 2013 年成立的国家电子安全中心），其职责包括“保护王国的网络空间免受网络威胁、应对网络安全事件以及提供网络态势感知”。^[3] 2019 年，

[1] Government of Dubai Media Office, “RTA’s Traffic Signal Upgrade Boosts Flow 37%,” September 4, 2025, <https://www.mediaoffice.ae/en/news/2025/september/04-09/rta-traffic-signal-system-upgrade>.

[2] International Trade Administration of U.S. Department of Commerce, “United Arab Emirates Country Commercial Guide: Digital Economy,” September 20, 2024, <https://www.trade.gov/country-commercial-guides/united-arab-emirates-digital-economy>.

[3] “(يناربيسلا نم ألال ةينطولا ةئيهلا) ءاشناب يكلم رمأ رودص”（发布关于建立（国家网络安全局）的王室法令），*أيديوعسلا ءابنألا قلأكو*（沙特通讯社），10-31, 2017, <https://www.spa.gov.sa/1683043>.

沙特在“2030 愿景”框架下成立了国家数据与人工智能管理局 (SDAIA)，负责统筹沙特国家层面的数据治理与人工智能战略，推动数字基础设施建设与公共服务智能化。该局还与沙特国防部签署谅解备忘录，为军方提供数据管理与人工智能领域的技术咨询服务。^[1] 阿联酋于 2019 年成立了电信与数字政府监管局 (TDRA)，并于 2020 年成立了网络安全委员会。为此，阿联酋设立了国家电子安全局 (NESA)，负责制定并实施国家网络安全法规。阿曼于 2020 年 6 月宣布在交通、通信和信息技术部下成立综合电子防御中心^[2]，而巴林、卡塔尔和科威特则分别于 2021 年和 2022 年设立了国家网络安全中心。

二是设立数字监管机制，建立长期稳定的治理框架。为维护数字主权，海合会国家顺应数字技术发展，不断迭代监管规则，构建完善机制以应对新挑战。在数字化转型与数字主权监管体系的建设上，沙特已成为区域内发展最为迅速、布局最为系统的国家之一。沙特通信、空间与技术委员会 (CSTC，2022 年由通信和信息技术委员会 CITC 改名而来) 负责监管沙特的信息与通信技术基础设施，并于 2019 年发布云计算和物联网的新监管框架。^[3] 此外，沙特还制定了一系列的网络监管框架，如沙特货币管理局网络安全框架 (2017 年)、基本网络安全控制措施 (2018 年)、物联网监管框架 (2019 年)、国家密码标准 (2020 年)、云计算监

[1] “The Ministry of Defence and ‘SDAIA’ Sign Memorandum of Understanding for Digital Industry,” Saudi Press Agency, November 2, 2022, <https://www.spa.gov.sa/viewfullstory.php?lang=ar&newsid=2397663>.

[2] 参见“مماظن رادصإو ينورتكلإلإ عافدلا زكرم ءاشنإب ينأطلس موسرم” (阿曼苏丹国法令：设立电子防务中心并颁布其规章制度)，نامع ءابنأ قلأكو (阿曼通讯社)，6-10, 2020, <https://omannews.gov.om/topics/ar/112/show/378291>; Staff Report, “HM the Sultan Issues 28 Royal Decrees”, Oman News Agency, August 18, 2020, <https://omannews.gov.om/topics/en/102/show/1458> 等。

[3] 参见“Saudi Arabia: CITC Publishes IoT Regulatory Framework,” Data Guidance, October 14, 2019, <https://www.dataguidance.com/news/saudi-arabia-citc-publishes-iot-regulatory-framework>; “Saudi Arabia: Cloud Computing Regulatory Framework Enters Into Force,” Data Guidance, March 12, 2018, <https://www.dataguidance.com/news/saudi-arabia-cloud-computing-regulatory-framework> 等。

临 2 年监禁。^[1] 二是数字基础设施与安全立法。根据世界银行的最新数据，海合会国家都拥有先进的电信网络，其中 5G 网络覆盖率超过 90%，并将数据中心和高速计算系统等设施项目视为投资的重中之重。^[2] 为此，海合会国家制定了相关法律，确保数字基础设施的安全和稳定，甚至将其纳入了相应的国家网络安全战略。^[3] 这一系列法律规范相互支撑，共同发挥着维护网络安全、强化数字保护、激励数字创新的支柱性作用。^[4]

（二）强化数字治理教育与培训

海合会国家普遍将数字人才的培养和数字安全培训视为实现数字本土化和自主化的重要前提，并将教育体系视为培育本土数字能力和提升数字竞争力的重要平台。首先是重视数字技能在基础与高等教育中的嵌入。以沙特为例，其在 2016 年制定的“2030 愿景”整体框架下，将教育改革置于国家战略的核心位置，启动了“塔特维尔教育发展项目”（Tatweer）。该项目建立了 50 所智能学校，它们不仅是沙特教育创新的试点，更成为政府将教育改革与经济转型紧密联系的关键基础数字人才“制造厂”。为此，沙特政府投入的教育预算高达 408 亿美元，占其公共支出的比例超过 20%。^[5]

[1] *Kingdom of Saudi Arabia Personal Data Protection Law*; March 27, 2023, <https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf>.

[2] World Bank, “GCC Economies Demonstrate Resilience, Advance Diversification, and Accelerate Digital Transformation,” December 4, 2025, <https://www.worldbank.org/en/news/press-release/2025/12/04/gcc-economies-demonstrate-resilience-advance-diversification-and-accelerate-digital-transformation>.

[3] 巴林、卡塔尔和科威特分别于 2014 年、2017 年和 2017 年制定了国家网络安全战略，阿曼、沙特及阿联酋则分别于 2010 年、2013 年和 2019 年完成相关战略的更新。参见 Bassant Hassib and James Shires, “Cybersecurity in the GCC: From Economic Development to Geopolitical Controversy,” *Middle East Policy*, Vol.29, No.1, 2021, p.99.

[4] “نمّال اليمقرلا لوححتلا ساسأ: جيلخل لود يف ةينقتلا تاعيرشتلا و ةمظنألا”（海湾国家的技术法规与立法：安全数字化转型的基础），Singleclic, 9-2, 2025, <https://singleclic.com/ar/خلالود-يف-ةينقتلا-تاعيرشتلا-و-ةمظنألا>.

[5] Tayan Bilal M, “The Saudi Tatweer Education Reforms: Implications of Neoliberal Thought to Saudi Education Policy,” *International education studies*, Vol.10, No.5, 2017, p.63.

2025 年 2 月，沙特教育部又发布了《人工智能在数字教育中的应用能力》框架，旨在构建教师与学习者的系统性 AI 能力标准，通过技术赋能与伦理规约的双重路径，推动沙特教育体系在数字化转型中实现包容性发展与全球竞争力提升。^[1]

其次是通过推广网络和数据安全教育及培训提升国民数字主权意识。海合会国家的大学已相继开设涵盖网络安全技术与组织管理的本科与研究生课程，学生群体参与课程的人数不断增长。在网络安全教育方面，沙特、阿联酋尤为突出。2021 年 3 月，沙特教育部与国家通信管理局签署合作协议，共同开展网络安全培训与研究项目。2022 年 8 月，国家通信管理局启动“网络安全创新中心”计划，目标是推动 60 余家网络安全初创企业的设立，并为超过一万名沙特公民提供系统化培训。^[2]此外，沙特国有企业与孵化机构在人才培养和产业支持中也发挥了关键作用。例如，塔克尼亚网络公司（Taqlia Cyber）专注于培训与能力建设，而巴迪尔（Bader）技术孵化加速计划则通过为初创企业提供融资与孵化支持，激发民间的网络安全创业活力。阿联酋网络安全委员会与战略合作伙伴共同推出“Cyber Pulse”项目，向社会公众普及数据保护与网络风险意识，截至 2025 年 11 月已覆盖数十万名参与者。^[3]

第三是积极推动与跨国企业和国际学术机构在数字技术教育领域的合作。巴林理工学院与微软合作建立了中东首个人工智能学院；巴林大学与英国 Benefit 公司合作推出人工智能和先进计算专用实验室，标志着巴林在网络安全、大数据、量子技术、工程与可持续能源等领域的研究和创新方面迈出了重要一步；巴林信息与电子政务管理局（iGA）和纳赛尔人工智能

[1] “میل عتلا یف یغان طصالء الفذل راطل”（《人工智能在数字教育中的应用能力》框架），ینورتکلل إل میل عتتل ینطول زکفرمل،（沙特国家电子教育中心），<https://nelc.gov.sa/en/node/2929>.

[2] National Cybersecurity Authority, “The National Cybersecurity Authority (NCA) Launches the ‘CyberIC’ Program for the Development of the Cybersecurity Sector in the Kingdom of Saudi Arabia,” August 8, 2022, <https://nca.gov.sa/en/news?item=234>.

[3] UAE Government, “Cyber safety and digital security,” November 12, 2025, <https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security>.

研究与发展中心 (NAIRDC) 签署了一份谅解备忘录, 旨在加强人工智能和技术创新领域的合作和知识交流。^[1] 近年来, 沙特的网络安全、人工智能与先进技术学院先后与美国卡内基梅隆大学及英国贝宜系统公司 (BAE) 等西方实体建立合作伙伴关系^[2], 并开设了由美国“铁网” (IronNet, 由美国网络司令部前司令和国家安全局前局长 Keith Alexander 等创办) 网络安全公司主导的“网络战”课程, 积极发挥跨国合作在沙特数字高端技能培养中的重要作用。^[3] 阿联酋建立世界上第一所致力于人工智能的研究型大学——穆罕默德·本·扎耶德人工智能大学 (MBZUAI), 并与 IBM 开展战略合作, 以进一步提升其在人工智能领域的创新能力。^[4] 总之, 海合会国家将国际教培合作视为培养数字技术和治理领域专业人才和实现赶超式发展的重要途径。

(三) 加强国际和地区数字治理合作

一方面, 海合会国家积极加强数字治理国际协商。一是致力于通过现有国际架构推动多边治理合作。沙特、阿联酋等成员国深度参与联合国信息安全政府专家组 (UNGGE) 及开放式工作组 (OEWG) 的磋商, 并在联合国互联网治理论坛 (IGF) 中积极发声。海合会各国还通过率先采纳国际互联网协会 (ISOC) 制定的《阿拉伯国家互联网基础设施安全指南》等区域规范, 不仅实现了内部数字主权与安全标准的协同, 更通过这类安排为国际网络安全治理贡献了力量。^[5] 二是通过创新多边合作机制, 推动数字领

[1] Government of Bahrain, “Artificial Intelligence Leveraging Artificial Intelligence (AI) for Bahrain,” November 13, 2025, <https://www.bahrain.bh/wps/portal/en/BNP/ExploreBahrain/ArtificialIntelligence>.

[2] “Saudi College, BAE Sign Cybersecurity Agreement,” *Arab News*, September 7, 2019, <https://www.arabnews.com/node/1550756/saudi-arabia>.

[3] “Mohammed bin Salman Cyber Security College Signs Deal with IronNet Cybersecurity,” *Alarabiya*, July 4, 2018, <https://english.alarabiya.net/business/technology/2018/07/04/Mohammed-bin-Salman-Cyber-Security-College-signs-deal-with-IronNet-Cybersecurity>.

[4] “IBM and MBZUAI Join Forces to Advance AI Research with New Center of Excellence,” IBM, May 25, 2022, <https://newsroom.ibm.com/2022-05-25-IBM-and-MBZUAI-join-forces-to-advance-AI-research-with-new-center-of-excellence>.

[5] Bassant Hassib, James Shires, “Cybersecurity in the GCC: From Economic Development to Geopolitical Controversy,” *Middle East Policy*, Vol.29, No.1, 2021, p.104.

域包容性对话。特别是沙特作为二十国集团（G20）中唯一的阿拉伯国家，扮演了十分积极的角色。2020年，沙特利用担任G20轮值主席国的契机，先后发起了全球网络安全论坛（GCF）、全球人工智能峰会（GAIN）等对话平台，积极引领数字治理前沿议程，促进国际交流协作；作为5个发起国之一推动在利雅得成立数字合作组织（DCO，现有16个成员国，包括5个海合会国家），旨在通过跨境协作消除全球数字鸿沟。GCF每年举办一次，海合会国家借此汇聚了全球60多个国家和地区的千余名专业人士资源。^[1] GAIN峰会每两年举行一次，2022年的第二届峰会通过《利雅得人工智能行动宣言》，提出消除技术发展不平等、构建包容性数字未来等倡议^[2]；2024年第三届峰会上，沙特宣布成立人工智能研究与伦理中心，进一步推动了跨国界的技术伦理对话。^[3] 另外，2024年12月，沙特承办了第19届联合国互联网治理论坛，聚焦“多方共治的数字未来”议题^[4]；2025年9月，沙特还通过与国际电联（ITU）联合主办全球监管者峰会，积极向国际社会分享海合会国家人工智能监管的实践案例。^[5]

另一方面，积极加强网络安全与数据保护国际合作。面对网络安全威胁的跨境性特征，海合会国家积极参与域内外网络安全合作项目、制定统

[1] يملا ع ريب خو لوؤسم 100 نم رثكأ، “كشك دمحم فرشأ (阿什拉夫·穆罕默德·卡什克)”，“نمألل يلودل ىدتنملا يف نوعمتجي (超过100位全球官员和专家齐聚国际网络安全论坛)”，“ةيموكحل تامدخلل ءدحوملا ءينطول ءصنملا (沙特国家政务服务平台)”，14-2، 2020，<https://my.gov.sa/ar/news/8272>.

[2] “Digital Cooperation Organization Adopts Riyadh AI Declaration at the Global AI Summit,” Saudi Press Agency, September 13, 2022，<https://www.spa.gov.sa/2383673>.

[3] “يف يعان طصلال ءالكذل ءيملا علأ ءمقل .. ده علأ يل وسم ءياعرب / تاي نقت و مولع” “شذحتم 300 نم رثكأ ءكراشمب يعان طصلال ءالكذل تاي نقت تاروطت ضرعتست ءثل ائلا اهتخسن ءلالكو، (在王储殿下赞助下，第三届世界人工智能峰会展示了人工智能技术的发展成果，吸引了来自100个国家的300多位演讲者和全球与会者参与)”，“ةلدود 100 نم يملاع روضحو ءي دوعسل ءابنأل (沙特通讯社)”，8-21، 2024，<https://www.spa.gov.sa/N2158322>.

[4] 《互联网治理论坛：构建安全与公平的数字未来》，联合国网站，2024年12月16日，<https://news.un.org/zh/story/2024/12/1134401>。

[5] Mohammed Al-Kinani Ghadi Joudah, “Saudi Arabia pushes global connectivity, AI rules at regulators’ summit,” Chatham House, September 2, 2025，<https://www.arabnews.com/node/2613873/business-economy>.

一的安全标准，并着力建设区域网络安全平台。一是积极参与区域网络安全合作项目，包括海湾合作委员会计算机应急响应小组（GCC-CERT）、伊斯兰合作组织计算机应急响应小组（OIC-CERT）以及阿拉伯联盟相关机制。此外，还定期召开海合会网络安全部长级会议，并参与国际电信联盟、国际刑警组织（INTERPOL）以及事件响应与安全团队论坛（简称 FIRST）等国际协作项目。^[1]二是致力于与国际标准接轨，如海湾合作委员会标准化组织发布了 ISO27001 网络安全标准的阿拉伯语版本等^[2]，这些国际标准不仅有助于在中东地区构建强健的网络安全基础设施，也有助于国际合作伙伴和投资者建立对其数字环境的信心与信任。^[3]三是着力加强网络安全平台建设。2024 年 11 月，海合会国家在多哈举行的网络安全部长级会议上发布了《海湾网络安全战略》，该战略搭建了成员国间信息与网络威胁评估交流平台，进一步深化了在网络安全领域的区域合作。^[4]海合会国家将数据保护视为维护网络安全的重点，通过数据保护立法等举措，着力保护企业、消费者及关键基础设施免受日益增长的网络攻击威胁。^[5]

[1] “HE GCCSG: It's Important to Raise Cybersecurity Level to Protect our Countries & Ensure their Cybersecurity, by Confronting Cybercrimes, which are Among the Most Important Security Challenges whose Severity has Increased Regionally and Internationally,” GCC News, November 3, 2024, <https://www.gcc-sg.org/en/MediaCenter/News/Pages/news2024-11-3-1.aspx>.

[2] James Shires and Joyce Hakmeh, “Is the GCC Cyber Resilient?” Chatham House, March 2020, <https://www.chathamhouse.org/sites/default/files/CHHJ8019-GCC-Cyber-Briefing-200302-WEB.pdf>.

[3] Srbaz Nidham Othman et al, “The Impact of Cybersecurity Law in the Middle East,” *Encuentros*, Vol.23, 2025, p.415.

[4] “يناربي سلا نم ألل ةيجيلخ ةيجيتارتسا نال ع” (海湾网络安全战略发布), قرشلا طسؤال (《中东报》), 11-3, 2024, <https://aawsat.com/الابرعل-الاعل/جيلخل/يبرعل-الاعل/5077718-يناربي سلا نم ألل-ةيجيلخ-ةيجيتارتسا نال ع>.

[5] “ةيولوا تانايبلا ةيامح: يناربي سلا نم ألل جيلخل ةيجيتارتسا” (海湾网络安全战略: 数据保护是优先事项), ويفير موكيليت (《电信评论》), 4-3, 2025, <https://www.telecomreviewarabia.com/articles/reports-coverage/4190-cybersecurity-strategy-in-gulf-data-protection-a-priority>.

三、海合会国家数字治理面临的挑战

近年来，以数字经济为重要动力的新型经济全球化不断向纵深拓展，加速了数据跨境流动，凸显了技术对外依赖风险，模糊了国家领土和网络空间之间的界限，对海合会国家维护数字主权和完善数字治理体系等层面构成了全新的挑战。海合会国家的数字治理模式和路径选择往往与技术依赖、规则碎片化和地缘政治竞争等因素交织在一起，要在数字技术上的自主与依赖、应对数字领域风险上的开放与安全、数字治理上的规则借鉴与本土化之间达成脆弱的平衡，并非易事。

（一）国际层面：数字治理话语权与技术依赖的双重挑战

首先，海合会国家在全球数字生态中所处的弱势地位制约其数字治理话语权。现有的国际数字治理规则中，西方在跨境数据流动、网络安全、人工智能伦理等方面一直占据主导话语权。^[1]值得注意的是，在特朗普 2.0 时代开启后，美国与海合会国家在数字领域的关系出现了新的变化。一是双方加强了在人工智能领域的合作。在 2025 年 5 月特朗普访问沙特、阿联酋和卡塔尔期间，美国与三国签署了多项人工智能与数字技术协议。阿联酋深度参与由 OpenAI、甲骨文等科技巨头发起的美国“星际之门”（Stargate）AI 基础设施发展计划，而该计划的首个国际部署项目就是将落户在阿布扎比的总容量 5 吉瓦的“星际之门阿联酋”（Stargate UAE）数据中心综合体项目。^[2]二是美国加快其数字技术标准在海湾地区的确立和渗透。新一届特朗普政府废除了拜登政府时期的《人工智能

[1] Milton Mueller, *Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace*, Cambridge: Polity Press, 2017, p.10.

[2] Stephen Nellis, “Stargate UAE AI datacenter to begin operation in 2026,” Reuters, May 22, 2025, <https://www.reuters.com/business/media-telecom/stargate-uae-ai-datacenter-begin-operation-2026-2025-05-22/>.

扩散规则》^[1]，积极推动美国企业向沙特和阿联酋等国出口先进人工智能芯片，力图使这些国家融入美国主导的数字生态系统。三是以“数字杠杆”增强美国的地缘政治影响力。美国放宽对海湾地区芯片等技术出口限制，实质也是进一步通过数字技术渗透，重塑区域地缘政治格局，而美国的谷歌和 Meta 等科技企业是实现这一目标的重要力量。^[2] 海合会国家的国家级云和数据中心多依赖这些跨国公司，缺乏自主可替代能力，往往只能被动接受外部制定的标准。

其次，对西方的技术依赖问题进一步加剧了海合会国家在数字治理领域的脆弱性。一是相关国家战略愿景与现实依赖的反差。尽管沙特、阿联酋等国在其国家发展战略中强调数字产业自主，但在基础硬件、云服务和软件生态等关键环节上仍严重依赖西方的技术供应。二是资本投入向技术提供方回流。沙特和阿联酋的主权财富基金以及本地数字企业（如 G42、STC）虽预计投入数百亿美元用于建设人工智能集群与云平台，但这些投资大多流向美西方的技术供应商。三是美国政策与地缘政治格局的牵制。半导体产业分析机构 Semi Analysis 的研究认为，在人工智能模型和基础设施建设方面，海湾国家若无美国支持，几乎无法独立推进。^[3] 四是数字自主性面临结构性风险。美国在半导体、人工智能基础模型和云平台等方

[1] 新一届特朗普政府废除拜登政府时期《人工智能扩散规则》后，美国对海湾国家的人工智能政策取向出现了明显调整：一是在以全球许可制度取代分级许可制度后，美国强化了与海合会国家间的双边协议，海合会国家以对美投资换取先进智能芯片出口限制；二是在最大程度降低美国国家安全风险前提下，依据美国技术与监管框架，与海合会国家加强云计算和数据中心建设等方面的合作；三是由“技术选边”转向条件性容忍，只要不触及美国核心技术优势，海湾国家多轨并行的数字合作空间明显扩大；四是美国减少对规则主导型治理的制度性投入，转而强调灵活的双边与项目型合作，从而客观上为海湾国家提供了更大的实操回旋空间。

[2] “أي دأصتقأو أي مقر مألعل الكيرمأ بقاءعت فيك.. أي جولونكتلأ بورح”（技术战争：美国如何从数字和经济上惩罚世界？），سكلفببر (Brieflex)，7-3, 2025, <https://brieflex.com/عأل الكيرمأ بقاءعت فيك.. أي جولونكتلأ بورح/أي عانطصلأل الكذل>.

[3] Dylan Patel et al, “AI Arrives in The Middle East: US Strikes a Deal with UAE and KSA,” Semi Analysis, May 16, 2025, <https://newsletter.semianalysis.com/p/ai-arrives-in-the-middle-east-us-strikes-a-deal-with-uae-and-ksa>.

面的主导地位,使海合会国家在数字技术供应链中长期处于“被动输入者”的位置。尽管海合会国家在国际资本市场和能源市场具有重要影响力,但一旦外部技术供应因地缘政治紧张或经济制裁而受阻,其数字基础设施也将面临系统性风险。

最后,跨国科技巨头在海合会国家的深度布局,也给这些国家带来数据主权方面的隐忧。全球科技巨头如同殖民帝国的铁路网络一样日益强化在全球数字经济领域的“殖民统治”,控制着数据流和数字基础设施。GAMAM (Google、Apple、Meta、Amazon、Microsoft 5 个美国公司) 占据全球前五大企业席位,2024 年总收入超过 1.5 万亿美元。^[1] 尽管目前谷歌、甲骨文和思科等美国科技公司同意加大大地生产、技术本地化和技能转移,但这些公司仍对与其合作的海合会国家提出诸多限制条件,如要求这些国家的安全法规与美国标准保持一致。^[2] 美国企业通过提供高精尖芯片并将专有软硬件人工智能等生态系统植入该地区,致使海湾国家难以摆脱长期依赖美国技术及维护服务的局面。此外,技术转移风险依然存在,这些公司与海合会国家签署的协议在治理权限方面缺乏透明度,如美方仍保留对海湾地区中心运营的根级访问权或实时监控权。^[3] 同时,海合会国家数据应用和监管依旧需要在不同程度上遵循这些数据来源国的法规。这种“准域外管辖”削弱了海合会国家对本土数据的完全掌控权,从而在数字主权层面留下隐患。

(二) 区域层面: 地缘政治竞争与治理碎片化的双重压力

一方面,地缘政治竞争下网络渗透对海湾国家数字治理的潜在威胁上

[1] “Google, Amazon, Meta, Apple, and Microsoft (GAMAM)—Statistics & Facts,” Statista, July 4, 2025, <https://www.statista.com/topics/4213/google-apple-facebook-amazon-and-microsoft-gafam/?srsltid=AfmBOopHTDmIm5KAVU7E7kMghRhspIzIQ19RNvHjoeVWoleNf15INTtn#topicOverview>.

[2] Kristina Fort, Nikhil Mulani, “AI Oases: Leveraging Gulf AI Ambitions for U.S. Strategic Objectives,” *SSRN 5344463*, 2025, p.26.

[3] Ferial Saeed, “America’s AI Pivot to the Gulf,” The Stimson Center, July 18, 2025, <https://www.stimson.org/2025/americas-ai-pivot-to-the-gulf/>.

升。近年来，中东地区的地缘政治对抗和冲突日益向数字空间领域扩散，成为影响海合会国家数字主权的重要威胁。以色列在网络安全领域初创公司数量众多、技术领先，使得以色列成为中东地区网络安全产品和解决方案的主要输出国。阿联酋等海湾国家引进以色列公司开发的可对智能手机进行远程监控的“飞马”间谍软件等技术，既是这些国家应对日益复杂网络威胁的现实选择，也使其面临敏感信息泄露的危险。^[1] 沙特学者玛达维·拉希德（Madavi Rashid）指出，以色列监控技术公司不仅威胁巴勒斯坦人，更危及所有海湾公民。^[2] 此外，美国通过云设施主导权、网络安全架构标准、社交媒体等多层面对海合会国家进行“数字渗透”，使数字空间成为地缘竞争的新战场。为了排挤其他大国在海湾地区的影响力，美国及其欧洲盟友持续向区域国家施压，要求它们在数字基础设施建设等方面减少与中国等其他国家的合作。^[3]

另一方面，海合会内部缺乏有效的制度整合。虽然海合会在多个议题上推进区域合作、制定海湾联合行动方案及框架性协议和公约，但在数字治理领域，各国在发展水平、利益诉求和政策法规等方面差异显著。例如，阿联酋积极吸引跨国科技企业并成立网络安全委员会制定相对开放的政策，而沙特则强调数据本地化与国家安全优先。^[4] 沙特积极推进未来智能城市 NEOM 的建设，并主要着眼于构建本地化而非区域性的网络安全框架。卡

[1] Schindler Max, “Israeli companies talking to Saudi Arabia about \$500b. ‘Smart City’,” *The Jerusalem Post*, October 25, 2017, <https://www.jpost.com/business-and-innovation/israeli-companies-likely-talking-to-saudi-arabia-about-500-bil-smart-city-508429>.

[2] Mawadi al-Rasheed, “Pegasus Project: Why I was Targeted by Israeli Spyware,” *Middle East Eye*, July 20, 2021, <https://www.middleeasteye.net/opinion/pegasus-israel-saudi-arabia-why-targeted-spyware>.

[3] J Mohammed Soliman, “The Middle East in an era of great tech competition,” *Middle East Institute*, February 6, 2023, <https://www.mei.edu/publications/middle-east-era-great-tech-competition>.

[4] Nadin Hassan, “Saudi Arabia emerging as global cybersecurity guardian: digital experts,” *Arab News*, December 20, 2024, <https://www.arabnews.com/node/2583733/business-economy>.

塔尔提出《2030 数字议程》，也不包含区域合作的内容，而是强调通过本土的数据中心和云基础设施的商业化，将卡塔尔建成领先的数字经济体。这种政策不协调导致区域内缺乏统一的数字治理机制，使得海湾阿拉伯国家整体难以形成有效合力应对跨国网络威胁与外部数据渗透。

（三）国家层面：数字产业自主不足与制度建设滞后的双重短板

一方面，数字产业自主性不足。海合会国家严重依赖外国技术是最突出的短板，这在核心产业环节表现得尤为突出。如在硬件方面，海湾国家严重依赖外部供给。全球约 90% 的最先进半导体由台积电制造^[1]，而海合会国家几乎没有本土高端芯片研发和生产能力。仅 2023 年一年，沙特就通过公共研究机构阿卜杜拉国王科技大学（Kaust）购买了至少 3,000 颗英伟达的 H100 芯片。^[2]从人力资源再生产角度来看，专业人才的结构性短缺也是影响数字主权的重要因素。长期以来，海合会国家在经济和科技发展上高度依赖外籍劳动力。根据美国高级网络安全管理学院（ACSMI）2025 年发布的统计数据，海合会国家一线企业的本土网络安全人才不到 10%^[3]，其主要原因是数字技术的快速扩张与专业人才培养不足的矛盾造成的。硬件环节严重依赖进口，软件生态依赖跨国公司，本土企业缺乏在全球市场上的竞争力，这意味着海合会国家即便投入巨额资金，其数字化发展依然是“进口驱动型”，缺乏真正的自主可控性。

另一方面，法律制度建设相对滞后。欧美国家在数字治理立法方面虽然也存在分歧和矛盾，但在立法的系统性上要更为完善。例如，欧盟建立了统一的数据传输法律框架《通用数据保护条例》（GDPR），消除了内部

[1] Helen Davidson and Chi-hui Lin, “How Taiwan secured semiconductor supremacy – and why it won’t give it up,” *The Guardian*, July 19, 2024, <https://www.theguardian.com/world/article/2024/jul/19/taiwan-semiconductor-industry-booming>.

[2] Madhumita Murgia, “Saudi Arabia and UAE race to buy Nvidia chips to power AI ambitions,” *Financial Times*, August 15, 2023, <https://www.ft.com/content/c93d2a76-16f3-4585-af61-86667c5090ba>.

[3] ACSMI, *Cybersecurity Workforce Shortage: A Comprehensive 2025 Study*, July 12, 2025, <https://acsmi.org/blogs/cybersecurity-workforce-shortage-a-comprehensive-2025-study>.

数据流动的障碍，并通过倡导欧洲数据主权开始影响全球数据政策。与之相比较，海合会国家却存在三方面的问题：一是数字立法执法系统性不足。例如，科威特在2021年《数据隐私保护条例》颁布以前尚无专门的数据保护法律，立法滞后导致法律与相关部门之间缺乏有效的协调，且执行和监管机制也不健全。^[1]二是公众立法参与度较为有限。例如，2025年4月沙特通信、空间与技术委员会正式发布《全球人工智能中心法》草案，尽管也通过调查问卷了解民众对该草案的意见，但民众总体上对数据保护规则制定缺乏实质性参与。^[2]三是缺乏网络数字安全立法的区域统筹协调。网络安全威胁的动态化特征，以及海合会各君主国相对垂直封闭的行政体制，对于协调配置资金、技术和人力等各种资源构成一定制约，增加了区域内构建统一网络安全监管和立法的难度。因此，网络安全立法往往只是在国家层面存在，缺乏统一的区域性数字监管立法框架。

四、全球治理倡议下中国与海合会国家的数字基础设施 与数字治理合作

中国是数字经济大国，在数字治理方面也拥有技术优势和先进经验，提出的“数字丝绸之路”“网络空间命运共同体”等数字合作框架和理念，扩大了中国在包括海合会国家在内的全球南方的影响力，也为各国提升数字治理能力带来了机遇。根据中国外交部发布的《中国关于全球数字治理有关问题的立场》，中国致力于帮助发展中国家提高数字能力，特别是通过资金支持、技术培训、基础设施建设等方式，促进共同发展。这既尊重发

[1] “White Paper on the Data Protection Regimes in the GCC: A Comprehensive Overview and Comparative Analysis,” International Institute of Communications, March 24, 2025, https://www.iicom.org/wp-content/uploads/IIC-Whitepaper-Data-Protection-Regimes-in-the-GCC-10-March-2025-review75294981.1-combined_1.pdf.

[2] “فيصخششلا تانايبل اةيامح ماظن حئاول لوح ممتايئرم ءادبال مومعلا وعدت ”ايادس”
(沙特数据与人工智能管理局邀请公众就个人数据保护体系的相关规定表达意见)，
فلالكو، <https://www.spa.gov.sa/e3f6ba66afg>. (沙特通讯社)

展中国的数字主权,又倡导通过国际合作建立更加公平的全球数字秩序。^[1]近年来,中国先后提出了《全球数据安全倡议》《全球人工智能治理倡议》《全球数据跨境流动合作倡议》等重要倡议,为完善全球数字治理贡献中国智慧、中国方案,充分体现了大国担当。^[2]特别是2025年9月中方提出的全球治理倡议,主张全球治理要坚持主权平等、国际法治、多边主义、以人为本和力求实效的五大核心理念,并突出人工智能与网络空间等领域治理的紧迫性与现实挑战^[3],为各方共同完善全球数字治理体系以及构建开放包容、公平普惠的数字秩序提供了重要指引和强大动力。

中华文明与阿拉伯文明交流互鉴的历史源远流长。在阿拉伯历史学家和地理学家所撰写的《历史大全》《中国印度见闻录》《道里邦国志》等著作中,均折射出古代阿拉伯世界对中国精湛的制品工艺、完善的典章制度和安定的社会秩序的景仰。^[4]新中国自1949年诞生以来,一直不遗余力坚定支持阿拉伯人民争取国家独立和民族解放,赢得了广大阿拉伯国家的尊重和信任。中阿传统友谊为双方共建“一带一路”、加强包括数字经济在内的各领域交流合作奠定了深厚基础。以海合会国家为代表的阿拉伯世界的数字治理观念与中国数字治理范式在理念和实践层面表现出深度的契合,而双方在数字领域的合作则共同塑造了一种兼具区域特色与全球视野的数字治理模式。

[1]《中国关于全球数字治理有关问题的立场(就制定“全球数字契约”向联合国提交的意见)》,外交部网站,2024年1月,https://www.mfa.gov.cn/wjlb_673085/zzjg_673183/jks_674633/zclc_674645/qt_674659/202305/t20230525_11083602.shtml。

[2]《汇聚完善全球数字治理的强大合力》,新华网,2025年11月27日,<http://www.xinhuanet.com/politics/20251127/f35797db0b98478d804b75ba12882b08/c.html>。

[3]参见《全球治理倡议概念文件》,外交部网站,2025年9月1日,https://www.fmprc.gov.cn/wjbxw_new/202509/t20250901_11699909.shtml。

[4]参见伊本·艾西尔·伊兹丁·阿布·哈桑·阿里·伊本·穆罕默德(《历史大全》第5卷),《中国印度见闻录》,穆根来、汶江、黄倬汉译,中华书局出版社,1983年版,第10页;[阿拉伯]伊本·胡尔达兹比赫:《道里邦国志》,宋颀译注,华文出版社,2017年版,第62页等。

一是加强数字基础设施合作，打造新型“数字纽带”。2017年，沙特通信与信息技术部（MCIT）与中国国家发展和改革委员会签署了一项协议，旨在通过中国“数字丝绸之路倡议”（DSRI）与沙特“2030愿景”之间的对话协同，在智能城市 and 智能能源电网管理、数字基础设施（如光纤通信）以及电子政务等技术领域深化合作。2022年12月，习近平主席在首届中国—海合会峰会上发表主旨讲话时强调，中国愿同海合会国家共建大数据和云计算中心，加强5G和6G技术合作，共建一批创新创业孵化器，围绕跨境电商合作和通信网络建设等领域实施10个数字经济项目。^[1]2023年以来，海合会国家加速与“数字丝绸之路”倡议对接，形成互利共赢的产业共同体。华为公司已与沙特国家人工智能中心及沙特数字学院合作，共同培养沙特本土人工智能人才；阿里巴巴等中国科技企业则正在助力利雅得实现智慧城市愿景。截至2025年12月，阿里巴巴在中东建成的数据中心都分布在海合会国家，其中，在沙特和阿联酋各建有2个。^[2]

二是推进数字技术转移，架起中阿“数字桥梁”。2023年以来，华为一直在沙特运营云数据中心^[3]，并在2023年宣布再投资4亿美元支持沙特云计算发展。^[4]在华为等中国企业的支持下，科威特有了中东首个覆盖全国的商用5G网络，阿联酋也成为全球首个启动全国5G-A网络商用的国家。^[5]阿里

[1] 《习近平出席首届中国—海湾阿拉伯国家合作委员会峰会并发表主旨讲话》，中国政府网，2022年12月10日，https://www.gov.cn/xinwen/2022-12/10/content_5731120.htm。

[2] 参见“阿里云全球基础设施”，https://www.alibabacloud.com/zh/global-locations?p_lc=1。

[3] “China’s Huawei Opens Cloud Data Centre in Saudi Arabia in Regional Push,” Reuters, September 4, 2023, <https://www.reuters.com/technology/chinas-huawei-opens-cloud-data-centre-saudi-arabia-regional-push-2023-09-04/>。

[4] Catherine Sbeglia Nin, “Huawei to Invest \$400 Million in Saudi Arabia Cloud Region,” RCR Wireless, February 13, 2023, <https://www.rcrwireless.com/20230213/telco-cloud/huawei-to-invest-400-million-in-saudi-arabia-cloud-region>。

[5] 参见 Rajiv Pillai, “du launches region’s first live 5G-Advanced network in UAE with Huawei,” Gulf Business, August 13, 2025, <https://gulfbusiness.com/du-launches-regions-first-live-5g-advanced-network-in-uae-with-huawei/>; 《驻科威特大使张建卫在科威特媒体发表署名文章〈中科战略合作伙伴关系进入新阶段〉》，外交部网站，2023年9月21日，https://www.mfa.gov.cn/web/gjhdq_676201/gj_676203/yz_676205/1206_676620/1206x2_676640/202310/t20231004_11154746.shtml 等。

云在阿布扎比和迪拜建立了主要数据中心和混合云，推动数据本地化。在人工智能方面，沙特主权财富基金一直在投资中国人工智能生态系统。沙特人工智能公司（SCAI）宣布通过合资企业与中国商汤科技集团共同建设尖端人工智能实验室。^[1]2024年5月，沙特与中国两国财长在北京举行会谈，就深化人工智能、可再生能源及智慧城市领域合作达成共识。

三是加强数字治理对话，塑造安全“数字生态”。2020年9月，中国提出《全球数据安全倡议》，旨在为数字发展创造一个开放、公平、非歧视的环境，并帮助发展中国家在全球治理中发出自己的声音。在2021年3月的中阿数据安全视频会议上，东盟对该倡议表示欢迎，并与中方共同签署和发表《中阿数据安全合作倡议》，阿拉伯国家由此成为全球首个与中国共同发表数据安全倡议的地区。^[2]参与该倡议的共有14个阿拉伯国家，包括所有海合会成员国。在2025年5月的首届东盟—中国—海合会峰会的联合声明中，包括促进数字经济发展、开展数据安全合作、确保数字时代包容性参与等在内的数字化转型与创新是三方对话的六大主题之一。^[3]

四是加强数字治理合作，构建公平“数字秩序”。事实上，中国与海合会国家在数字经济、数字治理领域的合作充分体现了全球治理倡议所倡导的五大核心理念。近年来，中海跨境贸易电子商务蓬勃发展，以SHEIN、AliExpress、TikTok Shop为代表的中国跨境电商，共同竞逐这一新兴电商“蓝海”，不仅促进了海湾地区数字经济强劲增长^[4]，而且让域内民众更多、更方便地共享互联网和数字技术发展成果。同时，中海平等开展数字领域的跨国合作，有助于降低全球南方国家对西方数字技术和规则体系的依赖，

[1] “SCAI invests \$206.54m with SenseTime to deliver AI-powered solutions,” Trade Arabia, September 13, 2022, [https://www.tradearabia.com/News/400635/SCAI-invests-\\$206.54m-with-SenseTime-to-deliver-AI-powered-solutions](https://www.tradearabia.com/News/400635/SCAI-invests-$206.54m-with-SenseTime-to-deliver-AI-powered-solutions).

[2] 《中阿这份倡议，为全球数字治理打了个样》，新华网，2021年4月1日，http://www.xinhuanet.com/world/2021-04/14/c_1211110822.htm。

[3] 《东盟—中国—海合会峰会联合声明》，中国政府网，2025年5月28日，https://www.gov.cn/yaowen/liebiao/202505/content_7025574.htm。

[4] 《全球跨境电商竞逐中东市场》，新华网，2024年5月17日，<https://www.news.cn/tech/20240517/3fe4c700f4c44289bd2e41159acbed39/c.html>。

推动数字治理格局的均衡化与多元化。阿联酋学者法拉赫·阿布赖亚 (Farah Aburaya) 指出,中国的科技公司为海合会国家提供更具吸引力的定制化方案,既契合这些国家的需求与优先发展方向,又以优惠价格回应了各国在数字安全与主权自主方面的关切。^[1]更重要的是,中海双方都主张在全球数字治理中扮演更积极主动的参与者和引领者角色,正如《中阿数据安全合作倡议》所强调的,推动各方“在相互尊重基础上,加强沟通交流,深化对话与合作,共同构建和平、安全、开放、合作、有序的网络空间命运共同体”。^[2]总之,中海双方加强数字治理合作,有助于启迪和赋能全球南方在数字转型中掌握发展和治理主动权。

结 语

在数字技术驱动的新一轮产业革命浪潮下,全球产业链、供应链、价值链与创新链的分布形态正加速重构,世界经济数字化转型已是大势所趋。面对数字技术所带来的数据跨境流动、数字主权界定、技术伦理以及网络安全、数据安全等复合性挑战,国际社会亟需构建协同普惠的数字治理框架。这也正是联合国于2024年9月通过《全球数字契约》的历史背景与核心使命——该契约致力于在全球范围内弥合数字鸿沟、推进包容性发展,并强化数字治理领域的多边合作机制,标志着数字空间的规则建构进入新一轮全球协商周期。^[3]

在不可逆转的全球数字化转型进程中,海合会国家敏锐地捕捉到数字技术所蕴含的跨越式发展机遇,将其视为推动经济结构转型、国家治理模

[1] Farah Aboraya, “The Future Role of China in the GCC’s Tech Transition,” Al Habtoor Research Centre, October 20, 2025, <https://www.habtoorresearch.com/programmes/the-future-role-china-gcc/>.

[2] 《中阿数据安全合作倡议》, 外交部网站, 2021年3月29日, https://www.mfa.gov.cn/web/ziliao_674904/1179_674909/202103/t20210329_9180823.shtml。

[3] 参见《全球数字契约》, 联合国网站, 2024年9月22日, <https://www.un.org/zh/documents/treaty/A-RES-79-1-Annex-I>。

式现代化的战略抓手。这些国家力图通过系统性的数字能力建设，降低对传统能源经济的路径依赖，进而重塑其在全球数字生态中的角色与影响力。一方面，海合会国家积极布局数字基础设施、推进数字化发展、培育本土数字产业，加强与中国等国家的数字领域的合作，展现出从“能源大国”向“数字枢纽”转型的雄心壮志。另一方面，这些国家的数字化转型战略和政策实践也深刻体现了其对数字主权和数据安全的重视，即在积极参与全球数据流动与合作的同时，致力于构建本土化的数据治理体系与网络、数据安全防线，力求在“开放性”与“自主性”之间实现平衡。这种探索不仅反映了海湾国家试图借助数字化转型实现“弯道超车”式发展的内在逻辑，也揭示了全球南方国家参与全球数字治理体系改革的普遍诉求与独特路径。

展望未来，海合会国家的数字治理仍面临内外多重张力，包括技术本土化与全球化之间的平衡、传统治理模式与数字开放需求的调适，以及在地缘政治竞争加剧背景下数字技术标准和应用规范选择所隐含的战略风险。然而，对数字治理的探索绝不仅仅是提升效率的工具性议程，而是深刻关乎全球南方国家在数字时代能否实现主权自立与公平发展。对于这些国家而言，数字治理是构建适应未来社会经济结构、打破传统发展瓶颈的关键。一个审慎、开放且注重本土需求的数字治理框架，能够赋能全球南方国家在数字经济价值链、数字规则制定中争取更有利的地位，避免沦为技术规则或“数字殖民”的被动接受者。因此，海合会乃至整个全球南方的探索与实践，有助于推动全球数字治理理念与路径超越西方的经验范式，真正导向一个更公正、更平衡和命运与共的未来数字世界。

【收稿日期：2025-09-19】

【修回日期：2025-12-22】

（责任编辑：王霄巍）