

条约保护及投资仲裁（四） — 中东

作者：孙伟 | 赵宇先 | 段志超 | 陈湘林 | 刘隆 | 吕钧儒 | 魏姝昱 | 邹奕

一、简介

随着全球经济多极化趋势加速，中东地区，特别是沙特阿拉伯和阿拉伯联合酋长国（阿联酋），正处于历史性经济转型期。在“沙特 2030 愿景（Saudi Vision 2030）”与“阿联酋国家人工智能战略 2031（UAE National AI Strategy 2031）”等国家级战略驱动下，中东各国正以前所未有的速度向数字经济、人工智能（AI）、云计算转型¹。这一战略转向使得中东成为中国科技企业出海青睐的战略枢纽之一。

多项权威机构的调研数据显示：截至 2025 年，近 90% 的中国受访企业计划进入或扩大在中东的业务布局，87% 的受访企业已在沙特及阿联酋等核心市场开展实质性业务，战略重心已从早期设立代表处实质性转变为建立区域运营实体、研发中心乃至本地化数据中心²。以云计算、大数据分析、大语言模型（LLM）训练为代表的中国科技与 AI 企业，正迅速填补中东市场在底层数字基础设施与前端智能化应用方面的空白。

然而，机遇与风险并存。中东东道国为捍卫“数字主权（Digital Sovereignty）”，正密集出台严格的数据保护法规³、本地化存储强制要求以及基于“国家安全”的外商投资审查（FDI Screening）机制⁴。更为严峻的是，在中美科技脱钩背景下，美国通过长臂管辖、出口管制等手段频繁向中东国家施压，要求其在关键 AI 算力与数字基础设施领域剔除中国供应商，导致中国企业面临设备被强制替换、特许经营权被撤销乃至资产被变相征收的巨大风险。

在此背景下，国际投资条约（包括双边投资协定（BIT）与多边投资协定）及基于此建立的投资者 — 东道国争端解决机制（ISDS），构成了保护中国出海企业合法权益的重要防线。本文将剖析中国与沙特、阿联酋等中东热门东道国签署的主要国际投资条约，聚焦 AI 与科技公司面临的数据安全及国家安全审查风险，结合代表性国际投资仲裁案例的法理分析，为已经或计划出海中东的中国科技企业提供投资保护建议。

¹ The Middle East's Big Bet on Artificial Intelligence and Data Security | Crowell & Moring LLP, <https://www.crowell.com/en/insights/client-alerts/the-middle-east-s-big-bet-on-artificial-intelligence-and-data-security>.

² 中国企业加速布局中东市场，ENCOR Group 助力可持续出海增长路径 – China Daily, <http://ex.chinadaily.com.cn/exchange/partners/82/rss/channel/cn/columns/sz8srm/stories/WS6964ab10a310942cc499af42.html>.

³ 例如，参见沙特阿拉伯个人数据保护法（<https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf>）；阿联酋个人数据保护法（<https://ai.gov.ae/personal-data-protection-law>）；卡塔尔数据保护规章（https://www.qfc.qa/-/media/project/qfc/qfewebsite/documentfiles/resource-center/data-protection/regulations-and-rules/qfc_data_protection_regulations_2021.pdf）等。

⁴ 例如，参见 Foreign direct investment reviews 2025: Middle East（<https://www.whitecase.com/insight-our-thinking/foreign-direct-investment-reviews-2025-middle-east>）。

二、中国与中东热门东道国签订的主要投资条约解析

在国际投资法范畴内，外国投资者及外国投资在东道国拥有三个层面的法律保障：投资合同保障、东道国国内法保障以及国际法保障。国际投资条约是投资者用以规避东道国国内法修改与政策朝令夕改风险的重要依据。中国与中东核心国家在早年间已构建相对完善的双边投资条约网络，多边条约亦为复杂的跨国投资架构设计提供了广阔空间。

（一）《中国-沙特阿拉伯双边投资协定》（1996）的法律适用与局限

中国与沙特阿拉伯于1996年签署了《中华人民共和国政府和沙特阿拉伯王国政府关于相互促进和保护投资的协定》（“《中沙 BIT》”），该协定于1997年5月1日正式生效⁵。在实体保护标准方面，《中沙 BIT》第2条第1款规定了未附加条件的公平公正待遇（Fair and Equitable Treatment, FET）条款。这一条款未将 FET 明确限定在习惯国际法最低待遇标准之内，因此赋予了仲裁庭较大的自由裁量权。投资者可据此主张东道国未能提供稳定、透明、可预期的法律与商业环境，或违背了投资者的合理商业预期（Legitimate Expectations），甚至采取了不合理、专断及歧视性的干预措施。《中沙 BIT》第3条第1款确立了最惠国待遇（Most-Favored-Nation, MFN），确保中国投资者享受不低于任何第三国投资者的待遇。此外，《中沙 BIT》第4条第1款还规定了“充分保护与安全（FPS）”义务，并明确禁止未给予充分有效补偿的直接征收与间接征收行为。

在争端解决机制方面，《中沙 BIT》显现出历史局限性。根据协定第8条第2款，条约仅允许投资者将与东道国之间“涉及征收和国有化补偿数额的争议”单方面提交国际仲裁。这意味着，若中国科技企业因沙特数据合规新政或国家安全审查而遭受损失，但争议焦点涉及公平公正待遇或国民待遇而非征收，投资者在直接援引《中沙 BIT》启动 ICSID 仲裁时将可能面临较大的管辖权（Jurisdiction）障碍。

值得特别关注的是，《中沙 BIT》未明确包含“基本安全例外（Essential Security Exception）”条款，也缺乏类似 GATT 第21条的公共秩序或公共健康豁免条款。一旦沙特政府以国家安全为由采取损害中国投资者的措施，其在投资仲裁中可能难以直接通过条约例外条款获得免责，而必须诉诸门槛更高的习惯国际法“危急情况（State of Necessity）”进行抗辩。这一条约设置，客观上可以为中国投资者提供相对更有利的救济空间。

（二）《中国-阿联酋双边投资协定》（1993）的核心条款审视

中国与阿联酋于1993年签署、1994年生效的双边投资保护协定（“《中阿 BIT》”）同样构成了双方经贸往来的基石⁶。《中阿 BIT》第2条第2款及第3款分别规定了公平公正待遇及充分保护与安全义务。其中，第2条第3款进一步明确东道国不得采取“不合理或歧视性措施”损害投资者权利¹⁶。和《中沙 BIT》相同，《中阿 BIT》第3条确立了最惠国待遇，确保中国投资者享受不低于任何第三国投资者的待遇¹⁶。第9条明确了国际仲裁程序的适用，相较于《中沙 BIT》严格限定于“补偿数额争议”，《中阿 BIT》第9条第3款允许在投资者与东道国另行同意的情况下，将其他类型的投资争议提交仲裁。尽管如此，该等基于同意的仲裁机制依然使得投资者在直接援引《中阿 BIT》启动仲裁可能面临一定的管辖权障碍。

与《中沙 BIT》如出一辙，《中阿 BIT》文本中同样未包含明确的“基本安全例外”条款。在面对

⁵ <https://investmentpolicy.unctad.org/international-investment-agreements/treaty-files/3361/download>.

⁶ <https://investmentpolicy.unctad.org/international-investment-agreements/treaty-files/791/download>.

阿联酋近年来针对外资频繁启用的“战略影响活动”审查时，这一缺失降低了东道国在国际法层面的免责抗辩能力，使仲裁庭能够对其所谓“国家安全”干预进行更为实质性和侵入性的司法审查。

（三）多边条约的战略跳板：《伊斯兰合作组织投资协定》（OIC 协定）

《伊斯兰合作组织投资协定》（OIC Investment Agreement, “《OIC 协定》”）于 1981 年签署，沙特和阿联酋均系该协定的重要缔约国。尽管中国并非 OIC 成员国，但中国出海企业完全可以通过在法律体系较为完善的 OIC 成员国（如印度尼西亚）设立实际运营的控股子公司（SPV），并以该子公司作为投资主体向沙特或阿联酋进行投资，从而被纳入《OIC 协定》的保护伞之下。

《OIC 协定》第 17 条规定了具有约束力的投资者 — 国家仲裁机制，第 8 条提供了 MFN 条款。在具有深远影响的 Hesham Al-Warraq v. Indonesia 案中⁷，仲裁庭创先例地允许投资者利用《OIC 协定》MFN 条款，成功“引入（Import）”了印度尼西亚与第三国 BIT 中的公平公正待遇（FET）条款，填补了《OIC 协定》本身未明确规定 FET 的文本空白⁸。这一经典判例为中国科技企业通过精密的投资架构设计获取更强国际法保护，提供了极具价值的实证依据。

条约/协定名称	签署与生效年份	公平公正待遇（FET）	最惠国待遇（MFN）	国家安全例外条款	ISDS 覆盖范围
《中国-沙特 BIT》	1996 签署 1997 生效	包含（无条件，未设例外）	包含	文本中无明确安全豁免条款	主要限于征收补偿数额争议
《中国 - 阿联酋 BIT》	1993 签署 1994 生效	包含（明确禁止不合理或歧视性干预）	包含	文本中无明确安全豁免条款	包含征收补偿数额及经同意的其他争议
《OIC 投资协定》	1981 签署	可通过 MFN 条款引入	包含	包含维护公共秩序及安全的限制	包含（第 17 条明确支持国际仲裁）

三、AI 与科技公司出海中东面临的特殊数据与安全合规挑战

与传统行业投资截然不同，AI 大语言模型开发、底层算力中心建设、政务云服务及智慧城市项目具有高度的数据敏感性。中东各国政府正将“数据主权”提升至不可侵犯的国家战略高度，中国科技企业的投资行为正受到东道国前所未有的严苛审视。

（一）日趋清晰但依然严格的跨境传输强制约束

沙特阿拉伯新版《个人数据保护法》（Personal Data Protection Law, PDPL）于 2021 年颁布，经 2023 年重大修订后，于 2024 年 9 月全面进入强制执行阶段⁹。PDPL 由权力极大的沙特数据与人工智能局（SDAIA）主导监管，标志着沙特正式确立了对标欧盟 GDPR 的数据治理体系。尽管沙特此前在数据本地化（Data Localization）方面表现出比欧洲更为强烈的“数据主权”色彩，但是近期的监管动向体现其逐步对齐主流司法辖区的趋势。

⁷ <https://www.italaw.com/cases/1527>。

⁸ Hesham Talaat M. Al-Warraq v The Republic of Indonesia, Final Award dated 15 December 2014, UNCITRAL Arbitration, §§541-551。

⁹ <https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf>。

根据 PDPL 和 2024 年颁布的跨境传输实施条例¹⁰，沙特暂时没有普遍性的数据本地化存储要求，但是个人数据跨境传输依然需要满足严格的前置条件，包括确保不影响国家安全或重大利益、仅限于实现传输目的所必需的最小范围、确保数据得到同等保护水平。后者实现方式主要包括，签署 SDAIA 颁布的跨境传输协议（SCC）或者建立有约束力的规则（Binding Common Rules）并取得 SDAIA 批准，并开展数据跨境传输风险评估。

不过，特定行业如云计算服务，由于历史上存在较为明确的本地化存储要求¹¹，后续相关规定如何与最新的 PDPL 框架相互衔接依然有待监管部门进一步澄清。因此，对高度依赖全球云端协同、集中式算力调度以及需要汇聚多国数据进行大模型训练的中国 AI 企业而言，当地监管环境依然存在不确定性，需要提前进行规划、落实相关合规要求。否则，若违反 PDPL 开展数据出境，企业不仅面临警告、巨额罚款，更可能在极端情况下面临刑事处罚。

阿联酋的数据合规环境则呈现高度碎片化的复杂格局。在联邦层面，2021 年第 45 号联邦法令确立了全国性个人数据保护基准，并具有强力的域外效力，涵盖在阿联酋境外处理境内居民数据的外国科技企业¹²。同时，迪拜国际金融中心（DIFC）¹³和阿布扎比全球市场（ADGM）¹⁴均颁布并执行完全独立的数据保护法与监管标准。在人工智能方面，阿联酋人工智能办公室已经发布多项政策文件，倡导 AI 的合规应用¹⁵。特定行业（金融行业）则加强了对生成式 AI 系统的安全要求，要求相关受监管实体植入“隐私设计（Privacy by Design）”原则，且须向监管机构开放一定的算法透明度审核¹⁶，对中国 AI 企业形成多重平行的合规压力。

（二）外商投资审查中泛化的“国家安全”红线与负面清单壁垒

沙特于 2024 年 8 月颁布全新《投资法》（Investment Law），该法于 2025 年 2 月正式生效，全面取代实行二十余年的旧版《外国投资法》¹⁷。新法在表面上确立了内外资平等待遇原则，并用简化的“注册制”取代繁琐的“许可制”（第 7 条），然而《投资法》第 9 条赋予了沙特投资部（MISA）基于“客观理由”随时中止（Suspend）任何已获批外国投资的权力¹⁸。尽管 2025 年实施细则要求 MISA 在做出终止决定时给予投资者申请复议的权利¹⁹，但沙特依旧保留严密的“排除活动清单”，严格限制外资进入涉及国家安全、关键信息基础设施等敏感地带²⁰。从事云服务架构、底层网络安全防卫乃至具有军民

¹⁰ Regulations on Personal Data Transfers outside the Kingdom, <https://sdaia.gov.sa/Documents/RegulationonPersonalDataEN.pdf>.

¹¹ Cloud Computing Services Provisioning Regulations, https://www.dataguidance.com/sites/default/files/ccrf_en.pdf.

¹² UAE, Federal Decree by Law No.(45) of 2021 Concerning the Protection of Personal Data, <https://uaelegislation.gov.ae/en/legislations/1972/download>.

¹³ DIFC Data Protection Law, DIFC Law No.5 of 2020, <https://www.difc.com/business/laws-and-regulations/legal-database/difc-laws/data-protection-law-difc-law-no-5-2020>.

¹⁴ Abu Dhabi Global Market (ADGM) Data Protection Regulations 2021 (DPR 2021), <https://www.adgm.com/operating-in-adgm/office-of-data-protection>.

¹⁵ UAE's AI Ethics Principles and Guidelines (Dec 2022), <https://ai.gov.ae/wp-content/uploads/2023/05/MOCAI-AI-Ethics-EN.pdf>.

¹⁶ 例如，参见阿联酋央行对金融机构 AI 使用的有关要求：Data Quality, Privacy and Security, <https://rulebook.centralbank.ae/en/rulebook/5-data-quality-privacy-and-security>.

¹⁷ <https://investmentpolicy.unctad.org/investment-policy-monitor/measures/4800/new-investment-law-guarantees-equal-treatment-and-replacing-licensing-with-registration>.

¹⁸ <https://misa.gov.sa/activities/laws-regulations-copy/>.

¹⁹ Implementing Regulations of the Investment Law, Art. 23, <https://misa.gov.sa/app/uploads/2025/06/THE-INVESTMENT-LAW-IMPLEMENTING-REGULATIONS.pdf>.

²⁰ Business Setup in Saudi Arabia: The Ultimate Step-by-Step Guide for Foreign Investors (2025) – Iskan Marketing & Investment, <https://iskanco.com/starting-a-business-in-saudi-arabia/>.

两用潜力的前沿 AI 研发的中国企业，极易触碰此红线而面临被要求强制剥离资产的绝境。

阿联酋则依据 2021 年内阁第 55 号决议（Resolution No.55 of 2021），明确划定了 85 项“具有战略影响的活动（Strategic Impact Activities）”²¹，涵盖安全、国防、高保密级别的电信网络、核心金融服务等命脉领域。任何试图在这些战略领域进行绿地投资或 100% 外资控股的外国实体，均须经极其严格的跨部门审批，不仅需要经济发展部（DED）的许可，还必须获得国防部、内政部或中央银行等监管部门的特别豁免批准²²。相关部门拥有几乎不受司法审查约束的广泛裁量权，实务中常以隐性且模糊的“国家利益受损”为由予以一票否决，且不会出具详尽的书面拒批理由²³。

（三）地缘政治风险：强制脱钩与“微软-G42 事件”的警示

2024 年 4 月，微软与阿联酋顶级 AI 企业 G42 达成 15 亿美元战略投资²⁴，然而，这一合作的背后是美国政府的深度介入。多位阿联酋政府官员曾披露，在 AI 领域对华“脱钩”是与美国合作的关键条件。在此背景下，微软与 G42 的合作附加了严苛的排他性条件：其一，G42 被迫清仓剥离对字节跳动（ByteDance）、超聚变（xFusion）等中国科技企业总计超百亿美元的投资；其二，G42 被强制要求从核心数据中心全面拆除并销毁价值预估高达 17 亿至 20 亿美元的中国原产硬件设备（主要针对华为服务器及网络设备）；其三，微软接管运营的 G42 数据中心须接受严格的安全审查，并执行美国商务部工业和安全局（BIS）的出口管制与实体清单封锁审查²⁵。

这一标志性事件揭示了严峻现实：中东主权国家为获取最先进的美国芯片资源，完全可能在压力下做出地缘政治妥协。对于长久以来依托“工程总承包+融资（EPC+F）”等重资产模式²⁶深度扎根中东数字基础设施建设的中国企业（如华为、阿里云、腾讯云等），此类外部政治干预随时可能导致已签署的巨额商业合同被强行废止，前期投入的庞大硬件资产与智力成果因被迫“下架替换”而瞬间归零。

四、中东区域投资仲裁代表性案例浅析及法理启示

当严密的防范体系被地缘政治或东道国突发性政策摧毁，援引投资条约提起国际投资仲裁（Investor-State Arbitration）便成为出海企业挽回经济损失的重要手段。已有的判例及其法理逻辑，能为中国科技出海企业提炼出极具指导意义的实务启示。

（一）科技与电信行业争端破冰的管辖权博弈：P 公司 v. Saudi Arabia

在 P 公司 v. Kingdom of Saudi Arabia（ICSID Case No. ARB/22/20）案中，投资者 P 公司是某亚洲主要的综合通信服务公司的子公司。2022 年，投资者依据 1996 年《中沙 BIT》正式向沙特阿拉伯王国提起了 ICSID 仲裁程序。该案目前仍处于审理阶段，具体诉状主张尚未全面披露²⁷。

²¹ Cabinet Resolution No.(55) of 2021: Determining the List of Activities with a Strategic Impact, <https://uaelegislation.gov.ae/en/legislations/1520/download>。

²² Promising Sectors, <https://www.moet.gov.ae/en/promising-sectors>。

²³ United Arab Emirates | Lex Mundi, <https://www.lexmundi.com/guides/foreign-investment-restrictions-guide/jurisdictions/middle-east/united-arab-emirates/>。

²⁴ Microsoft Announces \$1.5 Billion Investment in G42 – CXO Insight Middle East, <https://www.cxoinsightme.com/news/microsoft-and-g42-partner-to-accelerate-ai-innovation-in-uae-and-beyond/>。

²⁵ The United Arab Emirates’ AI Ambitions – CSIS, <https://www.csis.org/analysis/united-arab-emirates-ai-ambitions>。

²⁶ Local Agency Is Shaping China’s Digital Footprint in the Gulf – Carnegie Endowment, <https://carnegieendowment.org/russia- Eurasia/posts/2025/01/local-agency-is-shaping-chinas-digital-footprint-in-the-gulf>。

²⁷ PCCW Cascade (Middle East) Ltd. v. Kingdom of Saudi Arabia, ICSID Case No. ARB/22/20 – itlaw,

本案是极为罕见的由中国背景科技/通信类投资者向中东核心主权国家发起正面仲裁挑战的案件，具有重要的风向标意义。核心看点在于仲裁庭将如何突破管辖权障碍——《中沙 BIT》第 11 条原仅允许将“涉及征收补偿数额的争议”提交国际仲裁²⁸。据此，沙特政府极有可能提出属事管辖权异议，主张仲裁庭仅有权审理补偿款额的争议，而无权管辖征收行为本身的合法性问题。若仲裁庭最终采纳投资者通过 MFN 条款引入沙特与其他国家缔结的近代 BIT 中更为宽泛的争端解决机制的法理路径，将对未来中国企业针对沙特等国家的维权路径产生深远影响。

（二）科技业务的“虚拟性”与属地投资的刚性门槛：S 公司 v. UAE

在 2024 年立案的 S 公司 v. United Arab Emirates (ICSID Case No. ARB/24/16) 案中²⁹，来自肯尼亚的申请人依据 2014 年《肯尼亚-阿联酋双边投资协定》，就其与阿联酋驻摩加迪沙大使馆签订的多项工程基建合同产生纠纷，指控阿联酋驻摩加迪沙大使馆官员存在涉腐败或不当干预行为，并据此对阿联酋提起 ICSID 仲裁。然而，在 2025 年 7 月作出的裁决中，ICSID 仲裁庭依据《ICSID 仲裁规则（2022 修订版）》第 41 条中针对“明显缺乏法律依据的诉求（manifestly without legal merit）”的简易驳回机制，以申请人未能提供确凿证据证明其将资金、设备或人员实际投入到了阿联酋“主权领土范围”内为由，驳回了全部诉求。仲裁庭认定，尽管合同受阿联酋法律管辖、部分准备活动在阿联酋进行，但投资的重心（centre of gravity）仍在索马里，不符合双边投资条约关于“位于领土内之投资（investments made in the territory）”的要求³⁰。

这一裁决对当前的数字出海大潮具有重要的警示作用：对于主营云计算服务、跨境电商平台、SaaS 软件分发及 AI 大模型 API 调用的科技企业而言，如果仅在中东设立无实质运营的数据节点或单纯通过互联网提供跨境服务，而未在该国境内进行实质性重资产投入（如建立实体数据处理中心、大量雇佣当地员工、投入研发资金进行在地技术转化），一旦与东道国发生合同违约或政策纠纷，在寻求投资仲裁救济时，极有可能因不符合双边投资条约关于“位于领土内之投资”的刚性定义，在管辖权阶段即遭仲裁庭拒之门外。

（三）司法程序不公与拒绝司法认定：K 某 v. Kuwait

在 K 某 v. State of Kuwait (ICSID Case No. ARB/20/53) 案中³¹，申请人 K 某是具有法国和叙利亚双重国籍的媒体企业家，通过控股公司间接持有科威特出版传媒集团 A 公司 45% 的股份。K 某与其商业伙伴、科威特前总理之子发生纠纷后，遭遇了一系列刑事和民事诉讼：因“将自己偷渡出科威特”这一逻辑上不可能成立的指控被缺席定罪；在对方提起的诽谤案中，上诉判决的模糊性使其无法获得有效救济；在合资公司股息纠纷中被判个人承担 1,400 万美元债务。K 某依据《法国-科威特双边投资协定》（France – Kuwait BIT (1989)）提起仲裁，主张科威特违反公平公正待遇（FET）和充分保护与安全义务，索赔 4.93 亿美元。2025 年 3 月 10 日，ICSID 仲裁庭作出最终裁决，认定科威特构成拒绝司法（Denial

<https://www.italaw.com/cases/9503>。

²⁸ Agreement Between the People’s Republic of China and the Kingdom of Saudi Arabia on the Reciprocal Promotion and Protection of Investments (1996) – Jus Mundi, <https://jusmundi.com/en/document/treaty/en-china-saudi-arabia-bit-1996-china-saudi-arabia-bit-1996-thursday-29th-february-1996>。

²⁹ Claims against UAE dismissed as ICSID arbitration tribunal manifestly lacked jurisdiction – Thomson Reuters, <https://uk.practicallaw.thomsonreuters.com/w-048-3564>。

³⁰ Kenyan Firm’s UAE Dispute Tests ICSID Investment Rules: What to Know – Radio Dalsan, <https://radiodalsan.com/united-arab-emirates/299284/kenyan-firms-uae-dispute-tests-icsid-investment-rules-what-to-know>。

³¹ Kiwan v. Kuwait – UNCTAD Investment Policy Hub, <https://investmentpolicy.unctad.org/investment-dispute-settlement/cases/1073/kiwan-v-kuwait>。

of Justice)，尽管仲裁庭认定存在条约违反，但因申请人未能独立量化损失，最终未裁定金钱赔偿。在费用承担上，仲裁庭拒绝了科威特提出的 660 万美元费用请求。仲裁庭指出，科威特“采取了战略性的对抗姿态”，仅“提供证据来反驳具体的指控”，而非“协助仲裁庭基于所有可用证据记录查明争议真相”，仲裁庭最终认定，由于科威特“也并非完全胜诉且被认定违反了公平公正待遇”，因此不应判给其费用³²。

该案表明，拒绝司法的认定标准已明确，东道国司法系统的严重程序不公、逻辑荒谬的定罪均可构成 FET 违反，企业应系统记录东道国司法程序全过程，尤其关注超期审理、剥夺辩论机会等异常情形。此外，需防范商业纠纷政治化风险，与权贵阶层合作时应尽可能约定国际仲裁，避免完全依赖东道国司法救济。最后，费用裁定可成为实质性胜利，即便无法量化损失，若能证明东道国程序不公且其“战略性的对抗姿态”导致程序冗长，仍可在费用层面获得有利结果，为商业和解积累筹码。

五、出海中东企业的投资保护建议

相较于其他海外市场，中东地区不仅拥有更雄厚的主权资本与购买力，也呈现出更强的政治自主性与更为暗流涌动的地缘政治环境。AI 与科技企业在规划出海中东蓝图时，必须在战略层面建立系统性、前瞻性的投资防御机制。

（一）准入合规：筑牢投资保护的第一道防线

正如多起败诉的投资仲裁案例所揭示的，若外国投资者的投资行为自始违反东道国核心公共政策或强制性限制清单，将从根本上丧失依据 BIT 寻求国际法保护的权利。对此，建议中国出海企业须采取如下应对措施：

其一，穿透数据合规审查体系。以出海沙特为例，在正式注入重资产前，AI 企业对其核心 AI 应用的数据生命周期进行严苛合规审计，确保物理服务器选址、相关合规机制安排等符合沙特 PDPL 的跨境传输要求，从根源上避免高额行政处罚以及极端情况下的刑事责任。

其二，规避负面清单刚性限制。投资决策前须确认业务是否落入东道国负面清单范围，如沙特“排除活动清单”或阿联酋“战略影响活动清单”的覆盖范围。切忌通过违规代持安排、隐性控制权协议等手段规避外资准入限制。国际仲裁实践表明，任何蓄意规避东道国强制性法律规范的投资行为，仲裁庭均可能基于“净手原则（Clean Hands Doctrine）”认定其为非法投资并予以驳回。

（二）投资架构：投资条约规划（Treaty Planning）

鉴于《中沙 BIT》和《中阿 BIT》等条约在争端解决条款及实体保护标准上存在历史局限性，科技企业应将投资架构规划前置设计：

其一，战略性引入第三地跳板架构。除通过中国香港或新加坡设立特殊目的实体（SPV）以外，出海中东的中国科技企业可重点考量《OIC 协定》这一多边保护伞。通过在政治环境相对中立、法律体系成熟稳定的 OIC 成员国（如马来西亚）设立实质性运营的子公司，并以该子公司作为核心投资主体向沙特或阿联酋投资，可在面临政策风险时越过受限的 BIT，援引《OIC 协定》主张权利，实现合法权益保护的最大化。

³² ICSID Tribunal Confirms Denial of Justice and Due Process Violations in *Bachar Kiwan v. Kuwait – Aceris Law*, <https://www.acerislaw.com/icsid-tribunal-confirms-denial-of-justice-and-due-process-violations-in-bachar-kiwan-v-kuwait/>.

其二，确保“实质性商业活动”以抵御“利益拒绝”抗辩。为防范东道国在仲裁程序中抛出“利益拒绝条款（Denial of Benefits Clause）”抗辩，设立在第三国的 SPV 须在注册国具备真实的商业实质：包括租赁实际办公场所、雇佣具备专业技能的当地员工、开展真实的业务运营并产生连续合规的纳税记录，方能顺利通过仲裁庭对“合格投资者”身份的穿透式审查。

（三）多维风控：防范“国家安全”被泛化滥用

G42 事件表明，中东国家为获取美国先进技术可能在压力下妥协。与主权基金或政府背景企业合作时，须提前考虑多维度构建风险防御体系：

其一，合同层面可考虑嵌入地缘政治变故条款。与主权基金或政府背景企业合作时，应在不可抗力、根本性法律变更基础上，增加“非归责提前终止”机制，明确因外部干预（如美国次级制裁）导致合同终止的补偿计算方式。这将为日后主张东道国“违背投资者合理商业预期”提供关键证据。

其二，技术层面可建立商业数据与国家安全信息的物理与逻辑防火墙。一方面必须清晰界定企业在日常运营中收集与积累的数据产权归属、使用授权及流转边界。另一方面，对涉及敏感隐私数据的 AI 核心模型进行有效的权限管控和日常监测，这不仅能切断数据违规外流通道，更可在东道国发起安全审查时提供技术实证，证明运营未对“国家安全”构成威胁，瓦解东道国动用相关行政权力干预经营的合法性。

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国或其他相关司法管辖区法律及实务的最新动态和发展，仅供参考，不应被视为任何意义上的法律意见或法律依据。

如您对本期《汉坤法律评述》内容有任何问题或建议，请与汉坤律师事务所以下人员联系：

孙伟

电话： +86 21 6080 0399

Email: wei.sun@hankunlaw.com

赵宇先

电话： +86 21 6080 0272

Email: yuxian.zhao@hankunlaw.com

段志超

电话： +86 10 8516 4123

Email: kevin.duan@hankunlaw.com

陈湘林

电话： +86 10 8516 4166

Email: xianglin.chen@hankunlaw.com

刘隆

电话： +86 10 8516 4212

Email: long.liu@hankunlaw.com