国家人工智能安全战略：对大学的影响

克里斯·R·格拉斯、塞夫吉·卡亚-卡什克奇、埃格利斯·查孔·卡梅罗、叶卡捷琳娜·米娜耶娃

克里斯·R·格拉斯（Chris R. Glass）：美国波士顿学院（Boston College）教育领导与高等教育系（Department of Educational Leadership and Higher Education）教授

电子邮箱：glassch@bc.edu

塞夫吉·卡亚-卡什克奇（Sevgi Kaya-Kaşıkcı）：土耳其中东技术大学（Middle East Technical University）博士后研究员

电子邮箱：sewgikaya@gmail.com

埃格利斯·查孔·卡梅罗（Eglis Chacon Camero）：美国波士顿学院教育领导与高等教育系博士生

电子邮箱：chaconce@bc.edu

叶卡捷琳娜·米娜耶娃（Ekaterina Minaeva）：美国波士顿学院教育领导与高等教育系博士生

电子邮箱：minaeva@bc.edu

研究型大学正在应对一个由国家人工智能（AI）与技术安全政策深刻塑造的复杂且不断演变的国际合作格局。2020 年至 2024 年间，许多国家陆续出台或更新了本国的人工智能战略，明确要求大学在推动国家 AI 能力建设方面发挥关键作用。这一轮以 AI 为核心的政策浪潮，标志着大学与国家战略优先事项关系的新阶段——从冷战时期的科研限制到“9·11”事件后的安全监管。然而，如今 AI 监管框架的广度与深度，反映了政府对大学研究在国家竞争力与安全体系中核心作用的重新定位。

尽管 AI 研究首当其冲地受到政策审查，如《推进美国人工智能领导地位备忘录》（*Memorandum on Advancing the United States' Leadership in Artificial Intelligence*），但新的安全框架也正在影响从气候科学到公共卫生等多个领域的国际合作。大学领导者如今必须系统地评估国际合作中的多重风险因素——从数据敏感性到技术转移风险。这一趋势较以往的学术交流时期更为严格，学术活动虽从未完全不受限制，但过去享有的自主性和非正式监管已大幅减少。

学术开放性与国家安全

当下研究型大学面临的首要挑战，是学术开放性与国家安全考量之间日益突出的张力。虽然出口管制与科研监管早已存在，但当今的地缘政治环境使国际科研合作，尤其在欧美国家，受到更高强度的审查。

这种紧张关系在中美科研合作中尤为明显。美国的“中国行动计划”（China Initiative）以及针对高性能计算与半导体技术的出口限制，阻碍了联合研究与学术交流。西方政府对中国的“数字丝绸之路”（Digital Silk Road）倡议加强审查，担忧相关技术可

能被双重用途（dual-use applications），并涉及数据安全与知识产权风险，尤其是在与华为和中兴合作的 5G 网络和智慧城市项目中。

类似趋势在全球范围内也在蔓延。澳大利亚高校已根据政府防范外部干预的指导方针，调整科研安全框架；日本亦强化网络安全管理，设立专门机构以监督敏感科研合作。这些举措标志着高校国际合作管理方式的重大转变——从开放协作逐步过渡到系统性风险评估与制度化安全审查。这一变化反映出全球科研体系在平衡国际合作收益与安全风险方面的新格局。

为此，各高校普遍采用“有管理的开放性”（managed openness）模式，以在科研合作与安全要求间取得平衡。这类框架通常包括合作伙伴筛查、数据共享协议透明化，以及定期安全审计。与此同时，数据治理（data governance）成为新焦点，各机构需同时应对不同地区的合规要求，例如从欧盟《通用数据保护条例》（*General Data Protection Regulation*）到各国的本地法律框架。成功的应对策略通常依赖稳健的治理结构、明确的国际合作评估机制，以及强化的合规执行能力。

机构自主性承受压力

国家 AI 研究经费与大学机构自主性之间的关系，正成为全球范围内愈发突出的议题。各国政府在增加 AI 领域投资的同时，往往附加与国家战略目标相符的条件，从而对学术独立构成压力。这种动态在不同地区表现出差异，反映出多样化的高等教育治理体系与国家优先方向。

在亚洲，政府对科研议题的主导更为直接。中国的《新一代人工智能发展规划》（New Generation Artificial Intelligence Development Plan）即为典型，研究型大学须依照国家战略执行科研任务。印度的国家 AI 战略（National AI Strategy）旨在推动 AI 在各领域的开发与应用，以确立全球领导地位；然而，印度理工学院（IITs）需在追求国家 AI 目标与保持国际科研合作间取得平衡。

相比之下，西方国家在总体上保留了较多机构自主权。美国高校虽保持显著的学术独立性，但联邦科研经费的导向性仍可能间接影响研究方向。欧洲高校则面临多层次的治理体系：在享受欧盟“地平线欧洲”（Horizon Europe）计划资金支持的同时，必须兼顾欧盟范围的法规（如《通用数据保护条例》及人工智能伦理准则）与各成员国政策，形成复杂的跨国合作环境。

非洲高校呈现多元模式：有的侧重与西方大学合作，有的深化与中国的科研联系，也有高校通过“应用科学伙伴计划”（Partnership for Applied Sciences）推动非洲区域协作。拉丁美洲的“拉美人工智能研究网络”（Latin American AI Research Network）则以区域能力建设为导向，兼顾合作与自主。这些差异性体现了制度自主性在地方发展优先事项中的多重维度。

人才流动与招聘困境

全球 AI 人才竞争加剧，给大学的人才引进与留任带来挑战。顶尖研究型大学在维持国际科研团队方面遇到困难，原因包括签证限制、安全审查要求及来自产业界的激烈竞争。在部分国家，国家安全框架要求 AI 研究岗位必须由本国公民或永久居民担任，从而进一步缩小了人才来源。

这些因素正以复杂方式重塑全球人才

流动格局。中国正大力发展本土 AI 教育体系；印度推出“人人 AI”（AI for All）计划，并与全球科技企业合作建立能力建设平台；巴西及其他新兴经济体通过“拉美人工智能研究网络”等区域合作项目，培育 AI 人才；欧洲通过“欧洲 AI 奖学金计划”（European AI Fellowships）吸引人才；东盟（ASEAN）框架则推动区域内的跨国人才流动。

然而，尽管区域性努力不断推进，全球南方（Global South）的许多高校仍在基础设施、资金与人才流失方面面临长期困境。高性能计算与数据基础设施的高成本，使资源充足的大学与新兴经济体高校之间的差距进一步扩大。联合国教科文组织高等教育、创新与能力建设研究所（UNESCO IESALC）的比较政策研究表明，发展中国家正越来越多地以市场准入与数据资源为交换，换取 AI 技术能力的获取，这可能加深国际高等教育体系中“中心—边缘”（center–periphery）结构的不平等。

同时，地缘政治变动也影响了传统的学术流动模式。许多亚洲顶尖大学正致力于通过研究生项目与产业合作构建国内人才培养体系；欧洲高校则强调“可信赖 AI”（trustworthy AI）与伦理框架，吸引重视学术诚信与道德标准的研究人员。

探索“负责任国际化”

当下学术界普遍倡导的“负责任国际化”趋势，为高校带来根本性挑战——在保持开放科研交流的同时，应对日益增长的安全监管压力。这一紧张关系映射出国际高等教育的更广泛变迁：全球合作的传统理念正与国家安全优先事项产生竞争。欧盟提出的“尽可能开放、必要时关闭”（as open as possible, as closed as necessary）原则为高校提供了一种框架，但关键问题仍在于——谁来界定开放与限制的边界？这些界定又将如何影响全球知识生产？

这一形势要求高校领导者与更广泛的高等教育共同体采取切实行动：首先，高校领导层应与教师及国际合作伙伴协商，制定清晰的风险评估机制，在维护学术自由的同时确保安全合规，从被动遵守转向主动治理；其次，大学应强化区域科研网络，以维持在双边合作受限情况下的多边学术活力；最后，高校应积极倡导兼顾安全与公平的政策框架，既回应合理的安全关切，又防止削弱学术核心价值或扩大全球 AI 研究的不平等。