全球治理与国内挑战：印度网络安全战略多元主义路径研究*

张舒君

（中共江苏省委党校世界经济与政治教研室，江苏　南京　210000）

摘　要：印度的网络安全战略在全球治理与国内挑战影响下呈现多元主义路径。从印度信息技术政策的演变切入，揭示历史竞争与国际战略选择中的多元考量形成其网络安全战略的基础。其次，剖析印度国内意愿与能力错位、国际治理压力及大国博弈等因素对其战略调整的影响。最后，聚焦数字化进程中的数据安全，阐述印度在“数据民族主义”、国际合作及人工智能与数据一体化平台建设方面面临的机遇与挑战。面对网络安全应对能力不足、高端技术创新不够等局限，印度试图通过政策立法和技术布局强化网络安全防护体系，并在国际竞合中寻求灵活战略空间。

关键词：印度；多元主义；网络安全；人工智能；数据安全

中图分类号：D81　　**文献标识码**：A　　**DOI**：10. 19358/j. issn. 2097 - 1788. 2025. 01. 005

引用格式：张舒君. 全球治理与国内挑战：印度网络安全战略多元主义路径研究［J］. 网络安全与数据治理，2025，44(1)：30 - 36.

Global governance and domestic challenges: a study of India′s cybersecurity strategy through a pluralistic approach

Zhang Shujun

(World Economy and Politics Research and Teaching Department,
Jiangsu Provincial Party School of the Communist Party of China, Nanjing 210000, China)

Abstract: India′s cybersecurity strategy exhibits a pluralistic approach influenced by global governance and domestic challenges. This paper begins by examining the evolution of India′s information technology policies, revealing that diverse considerations in historical competitions and international strategic choices underpin the formation of its cybersecurity strategy. It then analyzes the impact of factors such as the misalignment between domestic intentions and capabilities, pressures from international governance, and great power rivalries on the strategic adjustments undertaken by India. Finally, focusing on data security within the digitalization process, the study elucidates the opportunities and challenges India faces in areas including data nationalism or international cooperation, and the development of integrated artificial intelligence and data platforms. Confronted with limitations such as inadequate capabilities, limited high - end technological innovation, and insufficient understanding of cybersecurity complexities exposed by cybersecurity threats, India endeavors to strengthen its cybersecurity defense system through policy legislation and technological deployment, while seeking flexible strategic space in international competition and cooperation.

Key words: India; pluralism; cybersecurity; artificial intelligence; data security

0　引言

“过去城市沿河而建，如今它们的旁边是高速公路。未来它们将会建在光纤网络和新基建的基础之上。”印度总理莫迪在决意推进“数字印度”的设想后，以富有诗意的方式向印度和世界展望其未来的发展蓝图。

作为较早实现信息化的国家，印度在网络安全战略的制定上一直秉持相对谨慎而渐进的态度，并且这一战略的形成与其对外战略息息相关：在应对国内发展的同时，不断进行策略上的调试，逐步形成了具有印度特色的网络安全战略。总体而言，印度网络安全战略呈现多元主义路径，主要体现在两个层面：其一，国内层面以政策、法律、多方治理为抓手，尤其重视数字化进程中所涉及的数据安全；其二，国际层面，面对国际治理规则缺失、大国网络霸权等结构性张力时，主张通过多元

*基金项目：国家社科基金青年项目（21CGJ036）

合作开展共同治理。

当前，关于印度网络安全战略的研究主要集中在以下几个方面。一是印度网络空间安全产业的发展状况，探讨印度网络空间产业内的安全技术和服务提供情况[1]。二是网络安全法律与政策，关注印度反网络暴力的法律现状与困境[2]。三是国际合作与挑战，特别是研究印太战略框架下日本和印度网络空间合作的现状和前景，揭示网络安全治理国际合作的进程、逻辑和面临的挑战[3]。四是美国和印度的网络安全关系，主要从美印网络安全竞争[4]与合作两个方面入手，分析了合作的外在转变、内生动力及矛盾增生[5]。五是印度网络空间能力建设情况综述，包括技术发展与政策制定等方面[6]，包括印度参与网络空间国际治理的进程[7]。六是数据本地化与网络安全体系建设是新近关注的重点领域，其中涉及印度数据本地化政策遇到的难题及机遇[8]、印度网络安全体系建设[9]等研究。

目前，我国有关印度网络安全问题的研究呈现三大趋势。一是研究视角由内而外，从关注印度本身的网络安全产业发展逐步拓展到与世界主要国家的合作与竞争。二是研究维度更加丰富，不仅关注技术层面的能力建设，还涉及法律、政策和战略层面的制定与实施。三是研究领域不断扩大，从单一的网络安全问题转向多领域、多层次的综合分析，囊括了经济、政治、社会等多个领域。总体而言，国内研究大多侧重理论分析，缺少对实际案例的深入挖掘与实证研究，部分研究使用的数据无法反映最新的研究进展。同时，对印度与其他国家在网络安全方面的比较研究较少，限制了对其战略有效性的全面评估。

印度网络安全领域的研究正在逐步深化，需紧密关注其在国内外面临的结构性矛盾与战略压力。事实上，印度国际战略选择已从传统的“不结盟”转向了“多向结盟”，在中美战略竞争中亦呈现出一定的对冲意图[10]。随之而来的关键问题在于，印度整体战略转向是否会对其网络安全战略产生投射及影响。由于印度在网络安全核心能力与高端技术创新方面的不足，以及政府意愿与实际能力之间的错配、对网络安全复杂性与国内政治挑战的低估等因素，其政府在网络安全战略选择中不断进行调整，最终趋向于一种多元主义的路径。本文正是基于此视角，结合印度网络安全治理的实践与理论，以期在已有研究的基础上进一步探讨印度网络安全战略的形成逻辑、演进特征及现实影响。

1　印度网络安全战略的基石

作为全球软件外包基地，印度的信息技术“奇迹”一度享誉国际。自莫迪政府提出“数字印度”以来，不断出台并完善相关法律法规，以应对快速演变的内外网络环境。值得注意的是，后殖民主义历史在塑造印度互联网生态方面呈现出两面性。面对波谲云诡的国际战略形势，印度在网络安全领域稳步推进，并在网络安全治理规则的制定过程中积极发声，为自身争取最大化利益。

1.1　信息技术奇迹与“数字印度”

2010 年《经济学人》杂志对印度的“经济奇迹”发出了赞叹，“奇迹”来源于上世纪八十年代印度本土信息技术产业的飞速发展，当时印度的家庭小作坊式经济逐渐被现代企业经济所取代。信息技术企业家们从西方带回了先进技术和全球视野，成为印度“新经济”的代言人和意见领袖，推动了印度国家治理方式的转变。得益于坚实的信息技术基础，第四次工业革命在印度获得了成长的土壤。曾经享誉世界的“信息技术奇迹”和印度已有的信息技术基础，为世界信息技术初级市场提供了数量庞大的初级技术人才。

印度的网民群体成为全球社交媒体第二大注册及使用者，仅次于美国，年轻人对新技术和科技生活趋之若鹜。据世界卫生组织统计，印度的人口结构呈现出年轻化趋势，35 岁以下的年轻人已成为印度社会的主要人口构成。在全球主要发达国家和新兴经济体普遍面临人口老龄化困境的情况下，印度巨大的人口红利已经并将持续成为其在网络安全治理竞争中核心竞争力因素之一。

印度的信息技术产业自上世纪六十年代建立后，于八十年代忽然起飞，年均 30% 的增长率为印度经济做出了可观贡献。印度的信息技术产业为全球 75 个国家的 580 多家机构提供服务[11]，印度塔塔咨询公司市值更是在当年超过了脸书、百度、领英等全球知名互联网企业。这一经济奇迹是如何在印度发生的呢？有一种意见占了主流，即信息技术产业的发展超过了印度政府的传统监管范畴，初期甚至都没有相关法律去规范它。因此，为早期互联网公司提供了近乎“野蛮生长”的空间，并使其能够依托极低的人力成本获利。印度信息技术部部长早在 2000 年便直言不讳“印度之所以能在信息技术领域成为领头羊，是因为政府没有涉足这一领域”[12]。

莫迪总理上台后，从国家战略角度提出的“数字印度”开启对于互联网空间治理的努力。印度电子信息技术部称“数字印度”将把印度转变为“数字社会与知识经济”加持的国家。尽管该战略自发布实施以来颇受质疑，但新冠疫情的全球大流行无形中为其提供了新的推力与国内外契机。就内容而言，“数字印度”涉及内政与外交多个层面，且不断扩充，包括以下关键要素：其一，创建“数字基础设施”，为民众建立终身数字身份，并提

供安全可靠的网络访问；其二，“政府与服务”，通过在线及移动端为公众提供实时服务，并在各级政府或司法管辖区之间实现数字化的无缝衔接；其三，“公民数字赋权”，使公民全面获得数字化资源与相应的数字权利。

自“数字印度”提出以来，印度政府大力推进网络安全与数字信息技术教育，建立各式政府机构，不断制定与完善相关法律法规，鼓励私人企业在互联网领域的发展。印度网络安全战略政策文件的出台经历了提出、打磨、修正、退回与最终颁布的重重考验，至今仍在完善过程中。其中，政策框架以 2013 年颁布的《国家网络安全政策》以及印度“十二五规划”中有关网络安全的部分为主。2015 年发布的《加密政策草案》在公布两天后即因严苛条款引发公众抗议而被撤回。2000 年颁布的《信息技术法》是印度处理技术和网络安全的重要法规，《2008 信息技术法》（修正案）是对 2000 年版的重要补充，印度议会通过后，次年开始实施。治理参与方首先是政府部门，总理办公室于 2015 年设立了国家网络安全协调办公室，并建立国家网络安全研究基金。印度电子与信息技术部是印度政府网络安全治理的核心部门，承担主要的政府治理职责。内政部负责印度国内网络安全，国防部则是传统上负责印度国际网络安全的部门。国防部旗下的国防研究与分析研究所（IDSA）和国防研究与发展组织（DRDO）主要参与网络安全、国家安全研究工作。行业机构参与网络安全治理是印度网络安全治理的一大特色，其中最有名的便是印度数据安全委员会（DSCI），一家从事数据保护的公司，由印度全国软件和服务公司协会（NASSCOM）成立。除此之外，民间社会组织、智库、技术类与非技术类的学术机构也都积极参与到印度的网络安全治理之中，各自发挥着积极作用[4]。

回顾印度网络安全体制机制的形成过程可见，印度基于政策、法律、多方治理等多重角度，通过政策引领、法律约束与多方参与的方式，逐步探索并确立了自身的网络安全战略框架。后殖民主义的历史遗产与日益紧绷的国际战略环境，从内部与外部两方面共同加速了印度网络安全战略的制定与实施。随着印度在网络领域的不断扩张，如何平衡国内外的多重压力，进一步完善并稳固其多元主义战略路径，已成为未来印度网络安全治理的核心议题。

1.2 历史之殇与国际战略选择

后殖民主义历史对印度科学技术与网络安全的发展具有深远影响。尼赫鲁在其著作《人类的历史》中谈及对英国人的感受时写道“从某个方面看，英国对印度还是功莫大焉。英国人精力充沛的生命对整个印度造成巨大震动，也给印度带来了民族感。受过英语教育的新阶层开始出现……他们注定要在民族运动中居于领导地位”[13]。正是这群在西方接受前沿技术教育的人士，在后殖民主义语境下，一方面发挥着技术教育与经营的关键作用，另一方面也通过话语形态与媒介表征，塑造了当代印度互联网生态的核心面貌。互联网在推动印度社会的发展进程的同时，也带来消极影响，如孟买恐怖袭击及大选干预等，都与互联网传播密切相关。

外界对印度的相对忽视为其提供了相对宽松的发展环境。当世界的目光主要集中于美、中、俄等网络强国时，印度网络空间的发展反而获得了新的机遇。与印度国内信息技术最初的“脱管式”快速扩张相似，印度在国际竞争中同样面临较少的外部限制和干预。印度通过本国印度裔技术专家与国际组织管理人士，在网络安全治理规则的制定过程中为印度争取到了更多利益。2014 年 10 月，印度提出由国际电信联盟（ITU）主导并履行互联网治理职能，试图将互联网治理重新纳入政府间的多元主义框架，而不再主要由美国主导的技术机构掌控。这一网络安全多元主义的构想与印度对外战略的指导方针可谓一脉相承。

2 印度网络安全战略的调试

随着全球安全局势持续紧张，印度的对外战略已从“不结盟”逐步转向“多向结盟”，在中美战略竞争格局中也展现出明显的对冲意图。总体来看，印度的网络安全战略架构相对完整，但在国内层面仍面临政府意愿与实际能力之间的显著落差；在国际层面，则遭遇结构性张力的多重挑战。因此，印度在网络安全战略的早期选择并不多，而是通过策略性摇摆不断进行调试，并未贸然采取激进对冲策略。这一做法与印度建国之初所确立的大国战略目标相一致，也与多重内外因素交织相关。

2.1 国内困境：意愿与能力

网络安全问题首先是一种内在的主权和治理议题，网络安全战略的制定需要从本国实际出发，划定在可承担的人力、物力、财力范围内的安全底线，然后再与国际参与相互协调，最终确立适合本国国情的网络安全战略。尽管战略构想往往宏大，但其具体挑战却极为切实。

对于印度政府而言，最为突出的症结具体可归纳为以下几方面。首先，基础设施更新速度过缓，当前全球普遍推进新型基础设施建设，而印度要“迎头赶上”仍显力不从心。其次，网络安全教育缺乏，效能远远不足，这不仅体现在政府层面，企业与个人也缺乏足够的宣传与培训。第三，网络安全维护能力薄弱，缺少匹配当下网络安全形势的应对手段，外部势力易渗透印度国内网络，导致印度网络安全事件频发。第四，印度网络安全

各行为体之间缺乏有效协同。政府内部的网络安全治理组织机构混乱，职能重叠且协调不足；军方各自为政，军民融合推进困难；私营部门则多依赖自我管理。尽管印度是全球第 12 个通过网络安全法的国家，其国家网络安全战略的完善进度却依旧缓慢。

印度虽然在信息技术领域起步相对较早，但其后续创新动力始终不足。与其将此归咎于“安于现状”的国民性格，不如说印度国内政治体制和社会环境的复杂性才是更关键的掣肘因素。首先，“低端服务提供者”这一身份认同长期困扰着印度网络技术产业的发展。印度的软件服务行业外包属性浓厚，境内大多数软件企业仅在全球网络体系内充当分包商角色，承担离岸或项目层面的次级分包业务。其次，印度网络信息技术的高质量发展因缺乏政府政策背书而举步维艰，在高端信息技术掌握与应用层面落后于全球主流发展水平。印度数据安全理事会（DSCI）报告提出，印度网络安全产业到 2025 年计划实现 350 亿美元（约合 2 345 亿元人民币）产值的增长目标，将持续推动网络安全初创企业发展，并在政府支持下开展研究与开发项目，涵盖加密、密码分析、隐写术、网络与系统安全保障、网络监控、网络取证以及能力建设等多个领域。第三，民族主义倾向正从传统物理空间延伸至网络空间。由于数据的控制与存储涉及国家安全、社会公共道德、公共秩序、个人隐私、消费者权益、国内执法及产业发展等多重议题，“数据民族主义”这一概念随之出现[14]。印度政府强调数据本地化的重要性，主张对开放与滥用数据的行为进行有效遏制，以维护本国数据安全，也成为印度国内网络安全治理在国际层面的投射。

2.2 国际困境：结构性张力

全球网络安全治理面临的结构性张力主要源于缺乏一套普遍适用且具有约束力的国际法律框架，用以规范各国在网络空间的行为。目前较为公认的条约是《布达佩斯公约》，而印度并非该公约的签署国。

2.2.1 数据获取与跨境执法的分歧

印度与西方国家在跨境数据获取的问题上存在显著差异。以跨境数据执法为例，印度主要依靠司法协助条约（MLAT）获取所需信息。截至目前，印度已与 42 个国家签署了该条约，其中 6 个国家的条款纳入了国际公约的相关内容。相比之下，美国通过《云法案》对联邦法律进行修订，赋予美国政府机构在不受数据存储位置限制的情况下访问由美国境内服务商控制的数据的权力，并同时允许美国政府与其他国家签订行政协议，让相关服务提供商可直接共享数据。由于《云法案》降低了数据访问的门槛，因此招致了严厉批评。

《布达佩斯公约》是目前国际上较常被引用的处理数据获取争议的法律基础。该公约强调相互司法协助的原则，并为已经签有司法协助条约的国家设立了补充合作机制。仅在两种特定情况下，允许缔约方单方面获取数据而无需另一方授权：其一，可公开获得的数据；其二，在某一缔约方的境内计算机系统上访问存储于另一地点的数据，但需得到该数据合法持有者的“自愿同意”。欧盟内部也在积极推动电子证据机制立法，以为成员国执法机构跨境获取数据提供统一的法律依据。例如，2019 年 11 月欧洲议会公民自由、司法和内政委员会（LIBE）提出的报告草案，对该提案进行了大幅修改，明确了服务提供商的更多义务，并着重强调对基本权利的保护。然而，该草案尚待进一步审议与批准。

2.2.2 争议与执行

在跨境数据的执行层面，各国及相关个人在接收请求通知方面的权利也存在较大争议。由于适用领域不同，各类法律文书在保障措施和保护范围上各异。例如，《布达佩斯公约》第二附加议定书草案虽为通知另一缔约国预留了空间，但并非强制性规定；欧盟的电子证据提案仅在“数据请求可能影响豁免和特权或对另一方根本利益造成影响”时才需告知该方。为应对这类局限，欧盟司法和内政委员会的报告草案提出了“自动通知机制”，但仍须进一步研讨才能落地实施。相比之下，《布达佩斯公约》第二附加议定书草案主要规定可在命令中写明“特别程序指示”，包括禁止通知用户或其他第三方，以防止信息走漏。然而，各方利益相关者普遍呼吁应要求执法部门向个人发出通知，并仅在特定情形下允许延期发布禁言令，且此类延期应经司法裁决程序批准。

由于印度并非《布达佩斯公约》的签署国，无法参与对第二附加议定书的谈判与制定；同理，欧盟内部的电子证据法规对印度并不适用。然而，一旦越来越多国家加入这些协定，势必会对印度未来的网络空间策略产生间接影响。

2.2.3 国际法缺失与网络空间犯罪问题

此外，国际法在应对网络空间的恶性事件上缺乏统一的法律框架，各国通常依靠国际刑警组织或双边、多边的司法协助条约来进行合作，难以形成有效的全球共识。传统国际法律对网络犯罪的指导作用依然有限，尽管犯罪行为可能发生在某一具体国家，但发起攻击的一方却未必是主权国家，甚至可以通过各种技术方式伪造攻击源，导致攻击行为难以溯源，从侧面凸显了网络安全国际共识的脆弱性和复杂性。

3 新关切：数字化进程中的数据安全

面对国内外网络安全的多重困境，印度愈发意识到

网络主权对于国家发展的重要性。印度网络安全战略所呈现的多元主义路径，正是基于这一对网络主权的基本认知。数据安全问题是网络安全治理的核心基石，决定着网络安全战略的合理性、完整性与可持续性。“数据民族主义”的标签化表达恰恰映射出印度在国际合作中对数据安全的高度关注；同时，这一立场并未阻碍印度在多元主义理念下积极参与国际协作。基于此，印度正加快人工智能与数据一体化平台的建设。

3.1 数据民族主义

“数据本地化”的政治表达形式即“数据民族主义”，它在实际的数据安全治理中以多元化的话语手段呈现。坚决推进数据本地化不仅是印度对于网络主权的明确宣示，也代表着其现实条件下的自我保护选择。在美国、中国、俄罗斯、欧盟等主要国家或地区的网络攻防实力快速提升的背景下，印度通过推动数据本地化、通过“内敛化”路径来对抗外部强势力量，成为其自我防御的重要策略。。

当前，印度已成长为仅次于美国和中国的全球第三大互联网用户拥有国，年均增速超过 30%，面临着如何保护用户隐私与信息安全的严峻挑战。自莫迪执政以来，印度政府日益凸显的民族主义色彩在印度网民群体中获得广泛认同，并进一步从物理空间延展至网络空间。莫迪的连续当选与他熟练运用网络媒介和社交媒体密不可分。对印度政府而言，网络舆论与社交媒体的引导不仅关系到舆论走向，更可能成为民族情绪的“催化剂”，譬如孟买恐怖袭击事件酿成重大悲剧，巴基斯坦武装圣战组织“虔诚军”（LeT）在本世纪初就开始招募电信工程师、技术人员和运维人员，甚至自行设计应用程序及开发软件，并在穆斯林青年群体中展开招募。网络安全事件倒逼印度出台并完善《信息技术法》等相关法规。

2024 年 3 月 1 日，印度电子和信息技术部（MeitY）公布《人工智能建议》（AI Advisory），要求在印度运营的所有网络平台必须向印度政府提供运营报告。这份报告涵盖脸书（Facebook）、照片墙（Instagram）、谷歌视频（YouTube）、推特（Twitter）、微软（Microsoft）、领英（LinkedIn）等拥有海量用户的数据平台。“数据民族主义”构成了印度数据安全保护的独特底色，推动其网络安全战略多元主义路径逐步走向成熟。

3.2 国际合作中的数据安全

美国是印度在网络安全领域最主要的合作伙伴，两国在合作中面临的核心挑战之一就是数据安全。早在 2006 年，美印就发起“网络安全论坛”，致力于解决涉及关键网络信息系统外包、知识管理、软件开发、数据处理以及源于两国日益互赖所引发的国家安全问题，旨在强化两国政府间的互动[15]。当时，印度侧重于进行能力建设的研究与发展，而美国则最关注数据保护。由于印度在信息技术创新方面的发展相对迟缓，导致印度关键的网络信息基础设施（包括银行体系、高科技公司以及电网等）仍然陈旧，印度关键基础设施的数字化却远未达到同等水平，难以适应数字时代的需求。尽管如此，美印两国依旧迫切需要在网络安全领域展开探讨与合作，原因不仅在于印度大量承接了美国的低端互联网业务，还与其他多重因素相关——例如，世界最大的两家海底光缆公司（信实电信和塔塔通信）均为印度企业，承担了全球大量互联网流量，同时印度许多网站也托管在美国服务器上。

为有效遏制网络犯罪，美国与印度均认识到实时反应与信息共享的重要性。然而，两国现行的合作渠道主要仍依赖国际刑警组织和司法互助条约。在反恐领域，由于美国的中南亚战略与印度在中亚地区的政策主张相契合，两国在打击恐怖主义上拥有较大的合作意愿和共识。除此之外，联合研发本应成为另一潜在的合作领域，但需要建立在开放的学术环境和科研平台基础之上。拦截和破解加密通信是重要网络安全手段之一，在美国政府对加密技术实施出口管制的情况下，美印双方在技术共享方面依旧障碍重重。当前，两国对待数据持截然不同立场：美国主张数据共享，以确保其在网络世界的无阻通行；印度则坚决反对大范围的数据共享，奉行“数据民族主义”，并将数据保护视为优先事项，这与印度网络安全保护能力相对薄弱和其追求自我防御的现实需求密不可分。

印度在医疗保健领域原本享有一定声誉。然而，由于印度在数据保护能力方面依然欠缺，如何保护医疗健康信息已成为重大难题。此外，电子货币的普及为印度民众提供了更多样化的支付手段，个人财务风险也随之显著攀升。

3.3 人工智能与数据一体化平台建设

智能化时代数据安全问题成为印度政府关注的核心议题。早在 2018 年，印度政府便已着眼于人工智能可能带来的潜在风险，并着手制定相应的对策。当年 2 月 1 日，时任印度财政部长阿伦·贾伊特利在年度预算报告中指出，全球经济正因数字空间尖端技术的应用而转型为数字经济，其中包括机器学习、人工智能、物联网和 3D 打印等前沿技术。为此，印度国家研究院（NITI Aayog）将启动一项国家项目，引导印度在人工智能领域的研究与应用。2020 年 1 月，该智库再次发布《人工智能云计算特定基础设施建设》方法报告，提出建设人工智能研究、分析与数据一体化平台（AIRAWAT）的目标。

“数字印度”的推进使印度社会顺利由信息化外包产业时代向互联网时代过渡，并进一步迈向全面数字化。然而，数据分析对硬件基础设施提出了更高的算力需求，而印度诸多互联网应用仍依托美国高性能服务器提供支撑。因此，人工智能研究、分析与数据一体化平台成了印度在新一轮全球技术浪潮中“迎头赶上”的关键环节，其中能否真正补齐技术迭代的短板尤为重要。为应对计算基础设施开发、培训与部署方面依旧面临高成本与低可用性的困境，印度国家研究院（NITI Aayog）基于《人工智能国家战略》向政府提交了《AIRAWAT：为印度建立的人工智能云计算基础架构》等系列方法报告。该报告建议构建一个底层的基础云服务，以促进印度人工智能研究和解决方案的开发，并采用高性能、高吞吐量的超级计算技术。这一系统旨在推动医疗、教育、农业和交通等领域的效率提升，同时在计算能力、数据存储和数字数据规模三方面提供强有力的支撑，为印度政府及其网络治理需求带来全新的解决方案。一体化平台框架结构如图 1 所示。

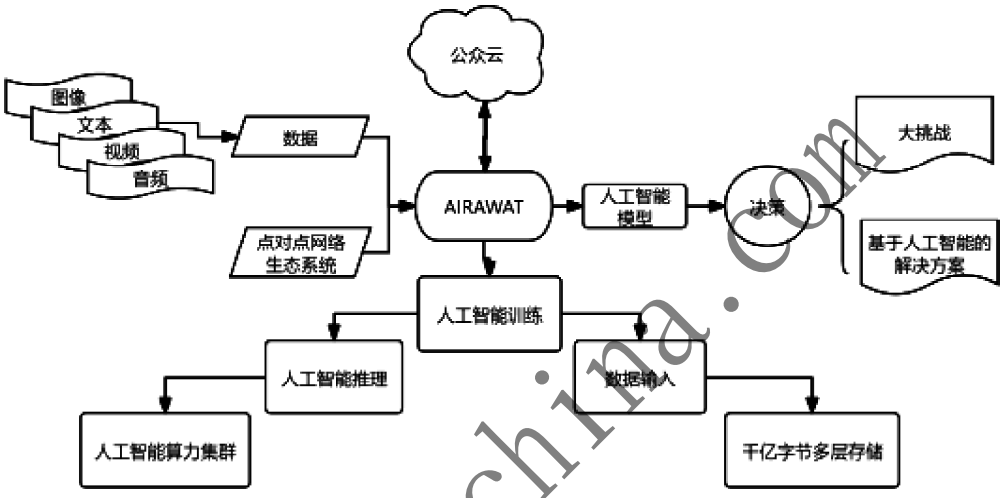

图 1　一体化平台框架结构图

AIRAWAT 平台计划构建高性能数据存储空间及领先的数据处理能力，实现数据自主化与更完善的数据分析功能。目前，AIRAWAT 平台仍处于设计阶段，实施者、经费来源、监管机构以及智力支持等方面尚未敲定，平台未来能够达成的规模亦存不确定性。从技术逻辑上看，印度的网络治理正逐步由立法引导转向更注重数据自主与数据安全。管理重心的转移意味着治理能力随之改变。尽管印度数据安全的支撑手段及治理模式尚需时日加以实践和检验，但 AIRAWAT 平台的提出无疑具有里程碑意义，为印度网络治理的具体实施提供了实质性方案。

4　结论

上世纪信息技术浪潮驱动了印度国家现代化与经济的高速增长，“数字印度”不仅是莫迪个人的施政口号，更是印度的战略雄心。回望历史之殇与国际战略选择，可以发现印度展现出了独特的国家智慧。然而，国家意愿与技术能力之间的错配为国内治理带来显著挑战；在国际层面，印度同样面临多重困境所引发的结构性张力。印度对网络安全治理的战略与方法设计，始终以其自身能力为基准。即便印度欲跻身世界网络大国的意愿强烈，却也不可避免地受到不平衡合作关系、国际治理规则缺失、区域政治错综复杂以及自身网络安全核心能力不足等诸多内外因素的限制，只能不断调试并奉行多元主义路径。

在网络安全国家战略的持续演进中，印度率先意识到数据安全在国家数字化进程中的关键地位，在国际电信联盟与西方国家的规则制定博弈中格外主动。印度外交战略由“不结盟”转向“多向结盟”[10]，同样体现在印度网络安全战略的变迁中。印度的网络安全战略选择并未依附任何具体联盟，这既与印度的实际能力紧密相关，也体现其独特理念。印度政府在网络安全战略中选择了多元主义，而非单纯对冲的方式。与此同时，印度积极出台人工智能国家战略并制定具体的路径方案，为下一阶段的发展奠定了基础，其在国防领域带来的变革，为应对可能的外部冲突赢得先机，并进一步巩固其在南亚地区的主导地位。

参考文献

[1] 罗仙. 印度网络空间安全产业发展研究 [J]. 信息安全与通信保密，2023，(12)：27－34.
[2] 何晖，杨倩倩. 印度反网络暴力现状与困境 [J]. 现代世界警察，2023 (7)：60－65.

[3] 毕世鸿，林友洪，耿鑫. 印太框架下日印数字合作的进程、逻辑及挑战［J］. 印度洋经济体研究，2023（6）：81－98.
[4] 张舒君. 印度网络安全治理视域下的美印网络安全竞合［J］. 信息安全与通信保密，2019（8）：63－74.
[5] 王业超，宋德星. 美印网络安全合作：外在转变、内生动力及矛盾增生［J］. 南亚研究，2023（1）：70－96.
[6] 张兆祺. 印度网络空间能力建设情况综述［J］. 中国信息安全，2022（9）：79－83.
[7] 荣国郡. 印度参与网络空间国际治理的进程分析［D］. 北京：外交学院，2020.
[8] 戴永红，陈思齐. 印度数据本地化：网络利益边疆的碰撞与机遇［J］. 南亚研究季刊，2022（2）：93－112.
[9] 华佳凡. 印度网络安全体系建设［J］. 信息安全与通信保密，2022（6）：21－31.
[10] 李莉. 从不结盟到“多向结盟”——印度对外战略的对冲性研究［J］. 世界经济与政治，2020（12）：21.
[11] DAS C P. Make in India-an analysis of IT sector［J］. Splint International Journal of Professionals，2017：69.
[12] KAPUR DEVESH. The causes and consequences of India′s IT boom［J］. India Review 2002，1（2）：91－110.
[13]［印］尼赫鲁. 人类的历史［M］. 高原，译. 北京：北京大学出版社，2016.
[14] 毛维准，刘一燊. 数据民族主义：驱动逻辑与政策影响［J］. 国际展望，2020，12（3）：20－42.
[15] SAMUEL C. Prospects for India-US cyber security cooperation［J］. Strategic Analysis，2011，35（5）：770－780.

（收稿日期：2024－11－21）

作者简介：

张舒君（1988－），女，博士，讲师，研究员，主要研究方向：美国对外关系、网络安全、冷战史。

（上接第8页）

[4] 郭光灿. 量子信息技术研究现状与未来［J］. 中国科学：信息科学，2020，50（9）：1395－1406.
[5] 慕慧娟，丁明磊，顾成建. 我国量子信息科技创新发展面临的挑战及建议——基于中美对比视角的分析［J］. 科技管理研究，2024，44（3）：11－19.
[6] 李静，高飞，秦素娟，等. 量子网络系统研究进展与关键技术分析［J］. 中国工程科学，2023，25（6）：80－95.
[7] 王敬. 量子信息技术产业发展概况及建议［J］. 通信世界，2024（6）：28－31.
[8] 王琦，李蒙，沈兴中，等. 量子测量技术内涵与发展［J］. 中国测试，2024，50（2）：1－6.
[9] 宋姗姗，钟永恒，刘佳，等. 量子信息领域的国家战略布局与研发态势分析［J］. 世界科技研究与发展，2024，46（1）：21－35.
[10] 周君璧，董瑜. 美国量子研发布局对我国的启示［J］. 世界科技研究与发展，2023，45（6）：661－669.
[11] 秦庆，汤书昆. 国外典型量子产学研联盟案例研究及对中国的启示［J］. 世界科技研究与发展，2023，45（2）：243－253.
[12] 邹丽雪，刘艳丽. 欧盟量子技术战略研究及启示［J］. 世界科技研究与发展，2022，44（1）：25－34.

（收稿日期：2024－09－05）

作者简介：

林浩（1990－），男，博士，工程师，主要研究方向：量子信息、密码学、网络空间安全。

姜伟（1979－），通信作者，男，博士，研究员，主要研究方向：网络空间安全、数据安全、网络综合治理。E-mail：jw@bjut. edu. cn。

王普（1992－），男，博士，助理研究员，主要研究方向：网络安全、数据安全、个人信息保护、大型平台数字治理。

（上接第14页）

[13] 郭晓亚. 基于联邦学习的加密流量分类研究［D］. 西安：西安电子科技大学，2022.

（收稿日期：2024－07－05）

作者简介：

崔又文（2003－），男，本科，主要研究方向：密码学、联邦学习。

冯千烨（2003－），女，本科，主要研究方向：网络入侵检测、联邦学习。

何云华（1987－），男，博士，教授，主要研究方向：网络空间安全、区块链。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部