大国关系

中印网络空间安全合作:机遇、挑战与应对*

于大皓　蔡翠红

[内容摘要]　随着数字时代和“大变局”时代的同时到来,中国和印度均面临严峻的网络空间安全态势,两国携手弥合全球网络空间安全赤字的意义凸显。在安全诉求契合、发展诉求契合、治理诉求契合和战略诉求契合四大动力的驱动下,中印网络空间安全合作已在双边和多边两个层面取得部分实际成果。但与此同时,这种合作关系也仍面临较大挑战,这既是两国在现实空间的矛盾所致,也由网络空间的自身特点形塑。若想化解挑战,唯有采取多种措施,力争以多边助推双边,以行动促进战略,以经济带动安全,以威慑倒逼互信,以斗争求取和平。中印如能围绕网络空间治理相向而行、求同存异,将不仅有利于塑造良好的网络空间安全态势,也有利于将合作延伸至现实空间,缓解全球地缘紧张局面。

[关键词]　网络空间治理　网络安全合作　中印关系　国际安全

[作者简介]　于大皓,复旦大学国际关系与公共事务学院博士研究生;蔡翠红,复旦大学美国研究中心教授

[中图分类号]D822.3　[文献标识码]A　[文章编号]2095-5715(2024)05-0116-20

随着数字时代和“大变局”时代的同时到来,世界面临多重治理困境和复合治理赤字。[①] 其中,信息通信技术的“泛安全化”应用与认知,导致网络空间安全

* 本文系国家社会科学基金重点项目“总体国家安全观视阈下的数字主权研究”(项目编号:23AZZ002)的阶段性研究成果,并得到复旦大学“卓博计划”资助。

① 蔡翠红、于大皓:《中国“三大倡议”的全球治理逻辑及实践路径—基于国际公共产品供给视角的分析》,《东北亚论坛》2023年第5期,第3~18页。

风险上升,网络空间安全赤字扩大。[①] 在这一背景下,中国所面临的网络空间安全态势复杂多变。中国受到诸如网站攻击、分布式拒绝服务攻击、高级持续性威胁攻击、恶意代码等网络安全问题困扰,其中仅在 2023 年,中国就遭受高级持续性威胁攻击 1200 余次,[②]遭受分布式拒绝服务攻击 146 万余次。[③] 鉴于此,中国亟需加强与关键信息基础设施、新技术新应用、企业海外合规、网络金融、供应链等相关的网络空间安全保障,推动网络空间治理体系的完善,维护国家网络空间安全和国际网络空间的和平与稳定。[④] 近年来,随着数字技术和数字经济的迅猛发展,印度也开始面临诸多网络空间安全问题。[⑤] 印度是全球网络攻击的主要目标之一,占所有此类事件的 13.7%,[⑥]仅在 2022 年印度就发生了高达 139.1 万起网络安全事件。[⑦] 印度的网络安全问题呈现多元特征,涵盖网络犯罪、网络攻击、数据泄露、网络恐怖主义、网络安全漏洞、网络安全法律滞后、网络安全人才匮乏、网络安全国际合作不足等诸多领域。[⑧] 其中,印度在网络安全国际合作方面的严重不足影响了其在全球网络安全治理中的地位和作用。[⑨]

中国和印度同为重要的地缘政治和网络空间力量,均面临严峻的网络空间安全态势,双方的良性网络安全互动不仅有助于解决两国面临的现实问题、改善双边战略互信、弥合网络安全赤字,而且能够引导区域乃至世界的网络安全态势向好的方向发展,进而还能将网络空间安全合作延伸至现实空间,缓解全球地缘紧张局面。基于此,中印理应携手共同应对网络空间安全挑战。然而,目前两国

---

① 沈逸、孙逸芸:《威胁认知重构与战略互信重建—第四次工业革命背景下国家网络空间治理能力建设》,《中央社会主义学院学报》2019 年第 5 期,第 101 ~ 109 页。

② 安恒研究院:《2023 全球高级威胁态势研究报告》,https://www.dbappsecurity.com.cn/news/down2166.html?utm_source=gzh。

③ 华为:《2023 年全球 DDoS 攻击现状与趋势分析》,https://e.huawei.com/cn/material/networking/security/333e0bdd9694437e80aac4b436781fe3。

④ 中国网络空间安全协会:《2023 年网络安全态势研判分析年度综合报告》,https://www.cybersac.cn/detail/1760575360354787330。

⑤ 张兆祺:《印度网络空间能力建设情况综述》,《中国信息安全》2022 年第 9 期,第 79 ~ 83 页。

⑥ CYFIRMA, "India Threat Landscape Report 2023," https://www.cyfirma.com/whitepaper/the-changing-cyber-threat-landscape/.

⑦ Shruti Sharma, "Securing India's Digital Future: Cybersecurity Urgency and Opportunities," https://thediplomat.com/2024/01/securing-indias-digital-future-cybersecurity-urgency-and-opportunities/.

⑧ 华佳凡:《印度网络安全体系建设》,《信息安全与通信保密》2022 年第 6 期,第 21 ~ 31 页。

⑨ 鲁传颖:《印度正成为区域网络稳定的破坏者》,《环球时报》2021 年 11 月 23 日,第 15 版。

间相关合作并不充分,亟待加强。当下,国际行为体间强化网络空间的信息共享、对话沟通和规则制定,建构信任措施,[①]以避免战略误判和管控冲突升级愈发重要,通过建构信任措施防范网络空间安全冲突不仅可能而且必要。[②] 总之,中印网络空间安全合作存在机遇,但也面临较大挑战,如能抓住机遇、化解挑战,对于塑造良好的中印网络空间安全态势、弥合全球网络空间安全赤字大有裨益。

一、动力叠加成果:中印网络空间安全合作的机遇

目前中印之间并没有全面的网络空间安全合作路线图,但双方由于安全诉求契合、发展诉求契合、治理诉求契合和战略诉求契合而保有持续合作的动力。在四大动力的驱动下,两国网络空间安全合作已在双边和多边两个层面取得部分实际成果。动力叠加成果,说明两国存在网络安全合作的机遇。

(一)中印网络空间安全合作的动力

中印在网络空间安全领域的安全诉求、发展诉求、治理诉求和战略诉求均有一定程度的契合,分别成为驱动中印推进网络空间安全合作的直接动力、间接动力、深层动力和上层动力。

其一,安全诉求契合是中印推进网络空间安全合作的直接动力。安全合作的第一目标便是解决安全威胁。数字革命重塑了国际权力结构,是大变局时代的一个关键变量。[③] 随着数字权力日益被视为国家权力的关键组成部分,网络空间亦成为地缘政治博弈的前沿阵地。中印两国是高速发展的数字大国,都高度依赖信息通信技术及其衍生应用,但相比于西方发达国家,两国的网络基础设施、网络管理规范、网络安全风控尚处于发展中阶段,因而均面临着网络攻击、网

① 建构信任措施(CBMs)并无统一定义,通常指在紧张局势下,对手国家之间为预防可能因误会而导致的冲突升级、消解双方对攻击的恐惧而采取的致力于加强信任的任何政策措施。目前,CBMs 正从传统安全领域(如核安全等)向新兴安全领域(如网络、太空、人工智能等)拓展。参见 UN,"Military Confidence-Building Measures,"https://disarmament.unoda.org/convarms/military-cbms/。

② 张明:《国际安全视角下的网络空间"建立信任措施"态势、模式及展望》,《信息安全与通信保密》2022 年第 2 期,第 58~70 页。

③ 阎学通:《超越地缘战略思维》,《国际政治科学》2019 年第 4 期,第 4~7 页。

络犯罪与网络恐怖主义的威胁,且由于网络空间重要性的上升,相关安全问题的危害性也随之扩大。印度计算机应急响应小组在其《2022 年印度勒索软件报告》中指出,包括关键基础设施在内的多个部门遭勒索软件攻击的数量在一年内便增加了 51%。[①] 中国亦然,根据国家信息安全漏洞库发布的《2022 年度网络安全漏洞态势报告》,2022 年新增漏洞近 2.5 万个,达到历史新高,保持连年增长态势。[②] 面对这一现实,中印均对网络空间存在安全诉求,且双方安全诉求大致契合,即避免与外国发生网络安全冲突,同时寻求合作保护本国网络安全。[③] 两国在网络安全标准、网络安全技术、网络犯罪惩治、网络军控、网络反恐等具体议题上存在较大合作空间,因而中印携手推进网络空间安全合作以应对网络安全威胁符合双方的共同安全利益。

其二,发展诉求契合是中印推进网络空间安全合作的间接动力。当前全球经济形态正由传统工业经济向数字经济转型,数字经济已成为人类社会发展的重要引擎。[④] 数字经济作为一种新型经济形态,其生产要素为数据,其载体为网络,其驱动力为数字技术。[⑤] 2022 年全球数字经济总规模达 41.4 万亿美元,占全球 GDP 的 46.1%。在未来较长时间里,数字经济在世界经济中的比重仍将持续上升。[⑥] 全球发展离不开和平稳定的国际环境,[⑦]数字经济发展亦离不开和平稳定的网络环境。由于数字经济具有跨国界、跨部门的特征,其发展需要受信任的、安全的数据跨国流通。然而,网络空间的“泛安全化”趋势阻碍了国家间围绕发展数字经济开展的必要交流,国家间的互不信任导致数据要素流通不畅。数

① Rajeswari Pillai Rajagopalan, “The AIIMS Cyberattack Reflects India's Critical Vulnerabilities,” https://www.orfonline.org/expert-speak/the-aiims-cyberattack-reflects-indias-critical-vulnerabilities.

② 国家信息安全漏洞库:《2022 年度网络安全漏洞态势报告》,https://www.cnnvd.org.cn/home/report。

③ 杨路:《印度网络安全机制:内涵、现状与未来》,《南亚研究季刊》2019 年第 3 期,第 9~16 页。

④ 蔡翠红,于大皓:《美国“印太战略”背景下的中国与东盟数字经济合作及其挑战》,《同济大学学报(社会科学版)》,2023 年第 2 期,第 26~39 页。

⑤ 国家统计局:《数字经济及其核心产业统计分类(2021)》,http://www.stats.gov.cn/sj/tjbz/gjtjbz/202302/t20230213_1902784.html。

⑥ 中国信息通信研究院:《全球数字经济白皮书(2023 年)》,http://www.caict.ac.cn/kxyj/qwfb/bps/202401/P020240109492552259509.pdf。

⑦ 习近平:《共迎时代挑战 共建美好未来——在二十国集团领导人第十七次峰会第一阶段会议上的讲话》,http://www.gov.cn/xinwen/2022-11/15/content_5727057.htm。

字经济在中印两国的国民经济中均占据重要地位,中国数字经济总规模为 7.47 万亿美元,占全国 GDP 比重已逾 40%,印度数字经济总规模占全国 GDP 比重亦超过 20%。[①] 中印两国是全球最大的数字经济市场,印度具备庞大的人口规模,中国更拥有先进的技术经验,双方发展数字经济本有很强的互补性。然而,两国网络空间安全信任的缺失使得两国难以从数字经济合作中得到发展红利。[②] 故而,中印目前在减少数字经济要素流动障碍、加强数字基础设施互信、制定共同数字经济和贸易规则、管控冲突、促进数字经济与技术人才交流等具体议题上存在较大合作空间,两国携手推进网络空间安全合作以释放数字经济红利符合双方的发展利益。

其三,治理诉求契合是中印推进网络空间安全合作的深层动力。网络空间安全治理模式事关网络空间的深层安全逻辑,是大国权力博弈的一大关键。同为发展中网络大国,面对全力护持网络霸权的美国,中印处境相似,治理立场相近。在模式的选择上,虽然印度支持以数据自由流通为基础的美式多利益攸关方模式,但也认同中国主张的多边模式中关于联合国和政府应在网络空间治理中发挥重要作用的内容,且中印均重视保卫数字主权,支持公平治理。由此,双方具备一定的治理取向的共通性。[③] 中国在《全球安全倡议概念文件》中提出,希望推动达成反映各方意愿、尊重各方利益的全球数字治理规则,共同应对各类网络威胁,构建开放包容、公平合理、安全稳定、富有生机活力的全球网络空间治理体系。[④] 而印度早在 2014 年的全球利益攸关方大会上便表示互联网治理应是有代表性的、透明的、民主的、负责的,互联网治理机制的结构应国际化,应发展立

① 《〈亚洲数字经济报告〉:中国数学经济规模遥遥领先》,http://www.news.cn/fortune/2023-12/21/c_1130039769.htm。

② 李来孺:《印度对华外资政策调整及中国的应对策略》,《印度洋经济体研究》2022 年第 2 期,第 134~150 页。

③ Colin Agur, Ramesh Subramanian and Valerie Belair Gagnon, "Interaction and Policy-making: Civil Society Perspective on the Multistakeholder Internet Governance Process in India," https://www.researchgate.net/publication/313568193_Interactions_and_Policy-Making_Civil_Society_Perspectives_on_the_Multistakeholder_Internet_Governance_Process_in_India.

④ 《全球安全倡议概念文件(全文)》,https://www.gov.cn/xinwen/2023-02/21/content_5742481.htm。

足于本土语言的信息、设施和服务,使发展中国家同样享受到互联网时代的利益。[①] 这些表述反映了其对美国单边监管互联网关键资源的不满。在2017年于新德里举行的第五届全球网络空间大会上,印度则主张通过政策框架推动构建更具包容性的网络空间,实现网络空间的稳定性、安全性和自由度。[②] 可见,中印的网络空间安全治理取向都有反霸权、重视政府作用、强调缩小数字鸿沟、提升发展中国家话语权等特点。因此,两国在数字主权维护、数据流通标准制定、网络空间治理机制建构等具体议题上存在较大合作空间,双方携手推进网络空间安全合作以塑造网络空间善治符合共同治理意愿。

其四,战略诉求契合是中印推进网络空间安全合作的上层动力。作为数字时代的关键新疆域,中印均重视网络空间的安全维护,各自出台了众多关于网络空间安全的法律法规与战略文件。截至2024年7月,中国已发布了《互联网信息服务管理办法》《关键信息基础设施安全保护条例》《网络安全法》《数据安全法》《个人信息保护法》等一系列涉及网络空间安全的法律法规,并提出了《国家网络空间安全战略》《网络空间国际合作战略》《全球数据安全倡议》等网络空间安全战略或规划,同时在相关重要国家政策方针(如总体国家安全观、网络强国战略、全球安全倡议等)阐述中,也突出强调网络空间安全的攸关性。[③] 印度则形成了以《信息技术法》《信息技术(修正)法》《个人数据保护法案》《数字个人数据保护法》《国家网络安全政策2013》《国家网络安全战略2020》等官方文件为支撑的网络安全治理架构,并多次呼吁加强网络空间安全国际合作。[④] 可见,中印在很大程度上已经将网络空间安全上升到国家战略的高度,而要在战略层面达成目标,

① Ministry of External Affairs of India, "Government of India's Initial Submission to Global Multistakeholder Meeting on the Future of Internet Governance," https://www.mea.gov.in/Images/pdf/official_submission_to_the_conference.pdf.

② Ministry of External Affairs of India, "External Affairs Minister's Speech at the Valedictory Function of Global Conference on Cyber Space," https://www.mea.gov.in/Speeches-Statements.htm?dtl/29136/external+affairs+ministers+spy+function+of+global+conference+on+cyber+space+november+24+2017.

③ 袁赫杰、张祺好、唐刚、邓若杨:《我国网络安全法治体系现状、问题及完善路径》,《信息安全与通信保密》2023年第12期,第83~93页;赵瑞琦:《中国网络安全战略:基于总体国家安全观的特色建构》,《学习与探索》2019年第12期,第57~65页。

④ 华佳凡:《印度网络安全体系建设》,《信息安全与通信保密》2022年第6期,第21~31页。

则离不开与其他网络大国的合作。中印政府也都认识到了这一点,并在战略和政策阐述中加以表达。例如,中国在《网络空间国际合作战略》中提出:“中国致力于与国际社会各方建立广泛的合作伙伴关系,积极拓展与其他国家的网络事务对话机制,广泛开展双边网络外交政策交流和务实合作。”[①]而印度数据安全委员会则直言:“尽管加强自身能力以保护国家关键基础设施的举措具有积极意义,然而,为了确保网络空间安全,更为关键的在于进行广泛而深入的国际合作。”[②]网络空间安全合作已经成为了两国诸多相关战略与政策规划的重要组成部分,双方在各级战略对接、不同领域对话、政策要旨传达等具体议题上存在较大合作空间,因而中国和印度携手推进网络空间安全合作以实践网络空间规划符合共同战略方向。

(二)中印网络空间安全合作的成果

尽管有利益冲突、领土纠纷和外部干扰等因素的存在,但中印两国在前述四大动力的驱动下,已在双边和多边层面尝试推进网络空间安全合作,并取得了一定成果。

在双边层面,中印已达成了部分网络空间安全合作成果(见表 1)。首先,在政府机构方面,早在 1988 年,中印就成立了由两国商务部领导的联合经济小组,目前该小组的经济安全协调机制已延伸到数字经济领域。2010 年,中印建立战略经济对话框架下的高技术联合工作组,由中国国家发改委高技术产业司司长与印度电子和信息技术部联合秘书共同主持,涉及网络安全互信与管控相关内容。[③] 2015 年,两国发布《中华人民共和国公安部与印度共和国内政部联合声明》,决定建立交流合作机制以共同打击跨境网络犯罪、电信诈骗犯罪等,维护网络空间共同安全。[④] 2019 年 1 月,两国启动“中印数字化合作机会平台”,旨在促

① 中华人民共和国国家互联网信息办公室:《网络空间国际合作战略》,https://www.cac.gov.cn/2017-03/01/c_1120552617.htm。

② Data Security Council of India, “International Cooperation,” https://www.dsci.in/content/international-co-operation.

③ 《中印战略经济对话各工作组举行工作组会议》,https://www.gov.cn/xinwen/2019-09/09/content_5428580.htm。

④ 《中印将建立高级别安全和反恐会晤机制》,https://www.gov.cn/xinwen/2015-11/21/content_5015161.htm。

进中国本土企业和印度信息技术企业的对话以避免政策性误判。[①] 其次,在企业商务方面,中兴通讯与印度电信运营商展开合作,在印度市场提供网络基础设施和网络安全服务;阿里巴巴与印度支付和金融技术公司展开合作,在印度投资了Paytm 等多家电子商务和支付技术公司,阿里巴巴的技术支持在确保交易安全性方面发挥着重要作用。再次,在学术研究方面,在智库和学者参加的如“中印网络外交圆桌会议”“中印网络安全研讨会”等双边二轨外交对话机制下,两国网络安全专家定期进行交流,对于加强安全沟通有一定效果。在如清华大学与印度理工学院合作等高校间学术交流机制下,中印高校共同举办学术研讨会、联合研究项目和学生交换项目,在网络安全领域进行学术合作,共同研究网络安全技术和政策,这有利于促进知识和技术的传播以及加强互信。

表 1　　中印网络空间安全合作双边成果概览

双边框架	合作成果
商务部联合经济小组	双边数字经济安全协调合作
战略经济对话高技术联合工作组	双边网络安全风险管控合作
跨境网络犯罪打击合作机制	双边公安部门网络犯罪协作合作
中印数字化合作机会平台	双边公私部门交流合作
中印企业间合作平台	双边企业直接商务合作
二轨外交对话机制	双边智库、学者对话合作
高校间学术交流机制	双边高校、学生交流合作

资料来源:笔者自制。

在多边层面,中印共同参与和推进部分区域或全球网络空间安全合作(见表2)。第一,在联合国框架下,中印在相关议题的政府专家组和不限成员名额特设工作组中协力就全球网络空间稳定议程进行协调,在互联网治理论坛中相互配合,在关于网络犯罪定义和立法的谈判中持相近立场。[②] 第二,在亚太地区计算

① Press Information Bureau of India Ministry of Commerce and Industy, “Launch of Sino-Indian Digital Collaboration Plaza,” https://pib.gov.in/Pressreleaseshare.aspx? PRID=1559382.

② 张蛟龙:《联合国与全球网络安全治理》,《国际问题研究》2023 年第 6 期,第 98~118 页。

机应急响应组织[①]框架下,两国遵循相关规则推进网络空间应急合作。[②] 第三,在互联网名称与数字地址分配机构框架下,两国共同采取行动与美国在互联网关键资源管理问题中展开博弈。[③] 第四,在 77 国集团框架下,两国就数字经济安全管控相关问题强化交流与沟通。[④] 第五,在二十国集团框架下,两国都是数字经济工作组和全球人工智能伙伴关系的成员,就网络治理、数字包容、安全信任等数字经济和人工智能关键问题进行积极协调。[⑤] 第六,在世界贸易组织框架下,两国就数字贸易安全管控相关问题增进互信与互谅。[⑥] 第七,在中俄印三边对话框架下,两国与俄罗斯就网络安全问题进行定期磋商。[⑦] 第八,在金砖国家框架下,两国就优化网络空间安全治理共同发声,共同探讨和制定网络安全合作的政策和措施,强化跨国网络安全防御能力和应对策略。[⑧] 第九,在上海合作组织框架下,两国在网络反恐联合演习中并肩作战,并共同签署了合作打击信息技术犯罪的协议,有利于加强上合成员国间在网络安全领域的合作和信息共享。[⑨]

中印网络空间安全合作在双边和多边两个层面的实际成果,为两国可以推进合作提供了清晰的证明。中印之所以能够搁置既有矛盾推进安全合作,是因为双方在网络空间安全领域存在展开合作的四大动力,动力叠加成果,两国应抓住这一机遇,协力塑造良好网络空间安全态势。

---

① 亚太地区计算机应急响应组织(APCERT)成立于 2003 年,是亚太地区计算机应急响应组织的联盟。APCERT 现有成员 30 个,来自中国、澳大利亚、日本、韩国、马来西亚等 21 个经济体,其目标是通过国际合作帮助建立亚太地区安全、干净、可信的网络空间。APCERT 按照其制定的运行原则和规章开展工作,对其成员的组织运行等不存在任何控制权力。参见“APCERT Annual Report 2022,”https://www.apcert.org/documents/pdf/APCERT_Annual_Report_2022.pdf。

② 关培凤、畅爽:《中印网络空间合作:现状与前景》,《印度洋经济体研究》2023 年第 4 期,第 79 ~ 93 页。

③ 沈逸:《ICANN 治理架构变革进程中的方向之争:国际化还是私有化?》,《汕头大学学报(人文社会科学版)》2016 年第 6 期,第 61 ~ 68 页。

④ Group of 77,“Statement by the G-77 and China at the Fifth Session,” https://www.g77.org/vienna/wp-content/uploads/2023/04/G77-and-China-statement-5th-session-AHC-website.pdf.

⑤ 高晓雨:《二十国集团峰会及其数字经济议题探析》,《中国信息化》2020 年第 7 期,第 5 ~ 8 页。

⑥ 参见张建平:《世界贸易组织改革与“全球南方”的作用》,《当代世界》2024 年第 1 期,第 30 ~ 34 页。

⑦ 王世达:《印太战略背景下印度参与中俄印三边合作的动因与局限》,《俄罗斯东欧中亚研究》2019 年第 2 期,第 59 ~ 71 页。

⑧ 徐朝雨:《金砖国家的网络恐怖主义治理:机制、挑战与应对》,《中国信息安全》2023 年第 5 期,第 20 ~ 23 页。

⑨ 邓浩、李天毅:《上合组织信息安全合作:进展、挑战与未来路径》,《中国信息安全》2021 年第 8 期,第 73 ~ 76 页。

表 2　　中印网络空间安全合作多边成果概览

多边框架	合作成果
联合国	1. 在相关议题的政府专家组和不限成员名额特设工作组中协力就全球网络空间稳定议程进行协调。 2. 在互联网治理论坛中相互配合。 3. 在关于网络犯罪定义和立法的谈判中持相近立场。
亚太地区计算机应急响应组织	遵循相关规则推进网络空间应急合作。
互联网名称与数字地址分配机构	采取行动与美国在互联网关键资源管理问题中展开博弈。
77 国集团	就数字经济安全管控相关问题强化交流与沟通。
二十国集团	就网络治理、数字包容、安全信任等数字经济和人工智能关键问题进行积极协调。
世界贸易组织	就数字贸易安全管控相关问题增进互信与互谅。
中俄印三边对话	就网络安全问题进行定期磋商。
金砖国家	就优化网络空间安全治理共同发声、探讨和制定网络安全合作的政策和措施、强化跨国网络安全防御能力和应对策略。
上海合作组织	在网络反恐联合演习中并肩作战、签署合作打击信息技术犯罪的协议。

资料来源:笔者自制。

二、虚拟交织现实:中印网络空间安全合作的挑战

中印两国存在推进网络空间安全合作的机遇,但是相关合作仍相当薄弱,面临着共识有限且落实困难的挑战。

(一)中印在现实空间的矛盾

中印网络空间安全合作的挑战根植于中印两国在现实空间的既有矛盾及全球地缘政治态势。

其一,中印历史纠葛夹杂现实摩擦导致信任危机蔓延。一方面,两国历史纠葛复杂。中国和印度都是文明古国且在近代相对衰落,逐渐滑入西方主导的资本主义世界体系的边缘,印度直接沦为殖民地,中国虽保有主权但也饱受压迫。两国本应相互信任并共同追求复兴,但由于两国长期存在边界争端,并有过一次战争和数次冲突,这使得两国间形成了复杂的历史纠葛。历史认知阻力造成双方难以甩开包袱,推进网络安全合作。另一方面,两国现实摩擦较多,这主要是

因为印度长期视中国为竞争对手。印度长期试图追求南亚地区甚至印度洋区域霸主地位,与中国的全球治理和外交理念不合。印度是一个保护主义倾向较强的内需驱动型经济体,在经济发展中习惯于规避向外国资本开放市场,尤其是向被其视为对手的中国资本开放市场,故而高频率打击中国高科技企业在印经营。[①] 印度在各方面国际规则制定谈判中也经常因维护自身利益而与中国立场相左。中印两国在全球治理、地区影响力、数字产业链、国际规则制定等各个领域均存在一定利益冲突和战略对抗,削弱了两国在网络安全问题上合作的意愿。历史纠葛夹杂现实摩擦,使中印之间的互疑氛围蔓延到网络空间。印度多次无端指责中国进行网络攻击和间谍活动。如印度智库网络和平基金会无端指责称仅在 2020 年 10 月至 11 月之间,就有数百万印度电子商务客户成为“中国黑客”的目标;2021 年印度孟买发生大规模停电事件,印方也有意引导民间舆论将其归咎为中国的网络攻击。此类论调之所以能在印度大行其道,正是由于双方信任的缺失。相应地,中国亦难以在网络空间安全领域完全信任印度。

其二,印度自身的民粹化倾向导致合作难以达成。2014 年莫迪政府上台以来,印度民粹政治不断发酵,并愈发展现出走向极端民族主义的趋势。[②] 印度民粹思潮的重要特征之一就是倾向于将中国树为假想敌。在印度民粹主义势力及媒体的大肆渲染下,部分印度民众对中国产生敌意,选举中各党派也常常煽动和利用民众反华情绪以达到政治目的,对于和中国有关的一切都加以怀疑和抨击,对于网络空间安全等议题更是敏感。对印度政府来说,当前印度社会矛盾严重,因而政府常借“国家安全”之名实施一系列针对中国的措施以宣泄民间情绪,转移民众关注,转嫁国内经济、政治和舆论危机。[③] 然而,民粹是把双刃剑,在民粹思维与行为方式的裹挟下,印度政府在诸如网络空间安全等需要与中国加强合作的领域,要么难以理性决策,要么受到民间压力而不敢理性决策。此外,由于网络和社交媒体的“去中心化”特征降低了民众参与政治与外交事务的门槛,负

① 张家栋、何雪倩:《印度退出 RCEP 谈判的原因与影响因素》,《印度洋经济体研究》2022 年第 6 期,第 17 ~ 33 页。

② 谢超:《论印度人民党的右翼民粹主义动员策略及效果》,《南亚研究》2021 年第 4 期,第 110 ~ 135 页。

③ 王蕊、潘怡辰、朱思翘:《印度对华经济脱钩的动因及影响》,《国际贸易》2020 年第 10 期,第 12 ~ 18 页。

面的网络行为失去缓冲阀门,网络空间更是成为民粹政治的高地。[①] 民粹政治在网络空间安全领域裹挟印度政府,形塑了印度朝野对网络空间安全现实的错误认知或错误决策,这种结构性的国内政治性因素难以在短时间内改变,这给中印网络空间安全合作带来了较大困难和不确定性。

其三,美西方等外部因素的离间导致中印网络空间安全合作进程饱受干扰。近年来,以中美博弈为代表的地缘政治交锋日益激烈,国际体系与秩序面临重塑,现实主义的战略思维方式开始回归。2022 年,美国更是在其发布的新版《国家安全战略》中直接将中国定位为"最大地缘政治挑战"。[②] 为在网络空间制衡中国以护持自身网络霸权,美国不断渲染来自中国的网络威胁,试图建构起全方位的全球网络安全联盟,极力拉拢印度作为非传统盟友协助其在网络空间围堵中国,欲使印度充当其在印太地区牵制中国网络力量的支点。在美国所主导的"排他性"地缘战略框架下,美国、印度与日本、澳大利亚之间形成了紧密的合作关系,美日印澳四方安全对话机制不断强化在网络安全领域的合作,定期举行磋商会晤,并针对中国实施了一系列网络安全相关措施。[③] 在 2021 年 3 月的线上"四国峰会"中,四方安全对话机制关键和新兴技术工作组明确提出,要致力于建立技术标准,并深入探讨关键科技供应链的合作机制。同年 9 月,于线下举行的"四国峰会"上,网络安全合作被再次置于重要位置,四国提议成立高级网络小组,专注于网络标准的采纳与实施、安全软件的开发、非中国硬件的推广,以及网络抗灾能力的增强。[④] 2022 年 5 月的四方安全对话机制《2022 年东京峰会备忘录》则宣称,四国为应对网络安全漏洞和网络威胁寻求建立韧性,其中供应链韧性和安全合作交由印度领导,同时还将加强四国计算机应急小组之间的信息共

① 于大皓:《数字国际传播的机遇与挑战》,《东南传播》2023 年第 5 期,第 91 ~ 93 页。

② The White House, "National Security Strategy," https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

③ The White House, "Joint Statement of the Quad Senior Cyber Group," https://www.whitehouse.gov/briefing-room/statements-releases/2023/12/15/joint-statement-of-the-quad-senior-cyber-group/.

④ 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》,《南亚研究》2023 年第 1 期,第 70 ~ 96 页。

享。[①] 这些合作议程的展开,明显针对中国。而印度在一定程度上也将美国视为“靠山”,积极寻求与美、日、澳以及北约网络防御中心合作,[②]希望借中美博弈之机,在网络空间塑造自身优势,吸引美国、欧洲、日本、韩国等国家或地区的数字技术与资本向印度转移,并参与制定网络空间规则,以实现“弯道超车”。虽然中印两国推进网络空间安全合作存在四大动力,但印度和美西方在网络空间安全问题上的利益也很契合,美西方对印度的拉拢极大干扰了中印网络空间安全合作。

(二)中印在网络空间的分歧

除了现实空间中的矛盾,中印网络空间安全合作的挑战也受到网络空间自身特点的影响。

其一,技术民族主义强化了网络空间的斗争色彩。技术二元论认为,任何理论从国家合作与竞争的角度看待科技相关议题时,都同时包涵技术民族主义与技术全球主义两个基础概念。[③] 这两个基础概念的区别在于,技术民族主义强调技术的国家属性,技术全球主义则强调技术的公共属性。[④] 技术民族主义认为:“在激烈竞争的世界中,技术实力是国家实力的决定性因素,因此国家应当采取一切措施保护本国科技发展机会和科技利益,且国家应对外国科技发展采取主动干预措施。”[⑤]技术民族主义者认为保障技术安全,尤其是新技术安全,是国家安全的核心,[⑥]因而应管控对外国技术的依赖,减少相关合作。[⑦] 受新地缘政治形势的影响,技术民族主义思潮开始在包括印度在内的许多国家占据上风。与此

① The White House, “Fact Sheet: Quad Leaders’ Tokyo Summit 2022,” https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/23/fact-sheet-quad-leaders-tokyo-summit-2022/.

② 张力、常睿哲、梁刚:《“四方安全对话”机制的网络空间安全合作及其影响》,《国际关系研究》2022 年第 1 期,第 81~98 页。

③ Robert Reich, “The Rise of Techno-nationalism,” *The Atlantic Monthly*, No. 5, 1987, pp. 63~69.

④ Pak Nung Wong, *Techno-Geopolitics—U. S. -China Tech War and the Practice of Digital Statecraft*, London: Routledge, 2022, p. 19.

⑤ Joan Johnson-Freese and Andrew Erickson, “The Emerging China-EU Space Partnership: A Geotechnological Balancer,” *Space Policy*, Vol. 22, No. 1, 2006, pp. 12~22.

⑥ Leonard Lynn, “Japan and the Politics of Techno-Globalism,” *The Journal of Japanese Studies*, Vol. 31, No. 1, 2005, pp. 188~191.

⑦ William Keller and Richard Samuels, *Crisis and Innovation in Asian Technology*, Cambridge: Cambridge University Press, 2003, p. 10.

同时,印度教的传统宗教哲学思想概念“司瓦拉吉”在经过民族主义先驱们的改良后,进一步为今天印度的技术民族主义行为提供了来自宗教思想的理论支持。[①] 此外,通过技术自主创新来推动经济改革并最终让印度成为大国的蓝图也是印度人民党能够取得选举成功的重要基础,故而技术民族主义就成为当下印人党政府吸引选民、整合社会的有力抓手。在地缘政治、宗教思想和党派方针三大因素的共同作用下,莫迪政府的网络空间安全政策带有强烈的技术民族主义色彩,其大肆宣扬“去中国化”,频繁通过修改投资审查程序、调整公共财政规则、出台离岸中心政策等措施限制中资高科技企业在印投资,还将“国家安全”“数据隐私”当作借口打压华为、小米、中兴等中方高科技公司,并封禁部分中国手机应用。[②] 随着莫迪第三任期到来,印度政府在网络空间的技术民族主义政策取向短期内预计很难得到调整。

其二,全球网络空间缺乏国际安全制度规范。在网络空间发展早期,安全问题尚不突出,故而网络空间安全立法并未引起重视。随着在网络空间的利益深化和对自身脆弱性的理解的加深,各国开始积极引导网络空间国际安全制度和规范的健全。经过国际社会数十年的磋商,当前各国已初步同意将以《联合国宪章》为代表的现有国际法框架运用于网络空间安全治理,[③]但关于国际法具体应如何适用于网络空间安全治理,各方仍然存在很大的分歧。例如,围绕“非武力”原则以及由其衍生的自卫权、自卫程度、自卫还击对象等问题,各国仍争议不断。[④] 包括中印在内的各国对国家在网络空间的负责任和可接受的行为有不同的理解和期待,在网络制度和规范方面也有不同的做法和预案。全球网络空间治理缺乏共同的制度规范造成了网络安全领域行为的模糊性和相异性,放大了各国本就存在的不安全和不信任感,不利于国家间的安全合作。中国与印度虽

---

① “司瓦拉吉”出自公元前16世纪的印度教经典《梨俱吠陀》,意为自主、自治、自我管理。参见欧东明:《浅析印度民族主义意识的确立》,《南亚研究季刊》2013年第3期,第73~74页。

② 李来孺:《印度对华外资政策调整及中国的应对策略》,《印度洋经济体研究》2022年第2期,第134~150页。

③ Harold Hongju Koh, “International Law in Cyberspace,” https://harvardilj.org/wp-content/uploads/sites/15/2012/12/Koh-Speech-to-Publish1.pdf.

④ Nicholas Tsagourias and Russell Buchan, eds., *Research Handbook on International Law and Cyberspace*, Cheltenham: Edward Elgar Publishing, 2015, pp. 236~237.

然在网络空间立法上存在相近立场,但关于具体的网络空间安全议题也有不同利益和观点。莫迪政府上台后,印度自诩为“网络民主国家”,在网络空间治理规范的多个领域向西方国家靠拢,[①]接受美国的所谓价值规范,并在 2016 年《印美网络关系框架》下进一步强化两国在网络空间规范上的共同价值观。[②] 共同国际安全制度规范的缺失使得各方矛盾难以在统一评判标准下解决。同时,各方对规范的不同理解也容易导致既有矛盾的扩大以及新矛盾的产生。例如,印度对中国企业实施打压的其中一个理由就涉及数据跨境流动的管理标准和规范问题。

其三,中印网络空间安全政策均缺乏透明度。信息传递的畅通是安全合作建立的基础,但目前中印都没有公开详细阐述自身的网络安全战略、理论和能力。“信息迷雾”的存在加深了双方对于对方网络空间安全行为意图的怀疑,也使核实或归因网络安全行为变得困难。例如,双方尚不清楚对方是否明确区分进攻性和防御性网络行动,也不清楚对方是否为网络冲突升级设定了门槛或红线,这些模糊性可能导致战略误判和冲突升级。同时,中印也缺乏网络空间安全问题的制度化、专业化沟通渠道,这进一步降低了一方对另一方政策的感知度。两国现有关于网络空间安全的信息交流渠道基本都依附于其他议题,缺乏专门化的、深入的对话和协商机制。

三、多措并行推进:加强中印网络空间安全合作的建议

中印网络空间安全合作的挑战“虚实相生”。因此,若想化解挑战,唯有多措并行推进,同时发力、相互作用。针对中印网络空间安全合作的挑战,中国或可从以下五方面加以应对。

其一,多边建构为先,以多边助推双边。当前中印双边网络空间安全合作面临较大阻力,但有机会在多边形式下,特别是在联合国机制下进行合作,通过多

① 鲁传颖:《印度正成为区域网络稳定的破坏者》,《环球时报》2021 年 11 月 23 日,第 15 版。

② 童宇韬:《科技竞争背景下印美“下一代防务合作伙伴关系”评析》,《和平与发展》2024 年第 1 期,第 183 ~ 205 页。

边平台推动全球网络空间共同行为规范的制定,为建构双边安全信任寻找共同的国际法框架。首先,中国可加大与印度在当前主流多边机制下的合作。比如,中印有条件在联合国2021~2025年信息通信技术安全和使用问题不限成员名额工作组下展开合作。该工作组致力于为探讨全球网络空间安全问题提供平台,其一大重点工作是确定国际法的网络空间适用问题。目前为止,第二任工作组已经举行了四轮实质性会议,其内部对国际法如何适用于网络空间仍存在许多分歧,而中印在这一问题上立场相近,可发挥影响力合作推动工作组就国际法如何适用于国家使用信息和通信技术这一问题进一步达成共识,尽早促成网络空间国际法的明确化。通过共同参与工作组,中印两国可以在主流机制下深化相互了解,推动未来可能的网络空间安全合作。除此之外,对于印度提出的在联合国主持下建立全球网络安全合作门户网站、制定公平详细的网络犯罪公约等合理诉求,中国可予以支持。这些举措有助于提升全球网络空间的治理水平,为两国深化网络空间安全合作提供有力支撑。其次,中印可借助金砖国家、上海合作组织等新兴多边机制合作推动规范生成。新国际机制能够通过议程设置等方式避开原有机制陷入行动困境的桎梏,为规范倡导者说服其他行为体另辟蹊径。尽管近年来印度在战略层面与美西方的关系日益紧密,但其仍致力于扩大其在金砖国家机制以及上海合作组织内部的影响力。对于中印两国而言,通过这些机制展开合作仍具有可行性和潜力。如双方可在金砖机制下共同明确跨国网络安全防御能力标准,在上海合作组织下推广打击信息技术犯罪协议等。最后,中国还可以与印度通过多边框架扩展网络安全合作的领域。中印可以凭借议题外溢的趋势,加强在网络空间安全技术研发、人才培养、信息共享等方面的合作。这既有助于提升两国的网络空间安全防护能力,又为日后的双边合作积累必要的经验和基础。总之,相比于中印在双边框架下的矛盾和分歧,两国在多边框架下存在较广泛的合作空间。以多边助推双边,积极落实各项多边合作举措,可促进两国共同应对网络空间的安全挑战。

其二,从具体议题入手,以行动促进战略。网络空间安全合作不只是宏观的战略规划,更是由具体微观的议题构成,包括信息共享、对话沟通、规则制定等多

个方面。唯有通过这些实际行动层面的积极合作,方能防范战略误判和管控冲突升级。中印两国应充分发挥各自优势,从任何可做的事做起,不能因整体战略层面的矛盾和分歧而影响具体领域合作。首先,由于中印都饱受网络电信诈骗困扰,双方可就网络跨国犯罪这一单一议题推进合作与互信,通过加强情报交流、联合打击网络犯罪、提升受害者援助等方面的合作,减少网络犯罪行为对两国公民的影响,提高双方的获得感,进而提升互信水平。其次,中印两国的数字基础设施均面临安全风险,这关系到两国的经济发展和国家安全。例如,水下电缆是数字基础设施的重要组成部分,其安全状况对于整个数字基础设施的稳定运行至关重要,双方可就保护水下电缆等具体议题展开深入的沟通,共同探讨应对措施,建立相关技术互信,以确保作为网络空间物理支撑的数字基础设施安全稳定。最后,两国还可在军队、外交部、商务部等具体职能部门间搭建具体的联络热线,提高中印边境事务磋商协调工作机制、金砖国家领导人会晤、上海合作组织等磋商机制的互动质量,促进信息、观点和经验的交流,并在发生严重网络安全事件时直接进行沟通,以避免误解。总之,中印应从具体议题入手,以行动促进战略,逐渐积累两国在网络空间的安全合作成果。

其三,共谋数字经济,以经济带动安全。相比于其他网络空间领域,中印在数字经济上的矛盾较小,合作动力较大。中印早已通过数字产品和服务贸易相互联系,两国近年来都倡导大规模的公共和商业服务数字化,双方数字经济发展互补性高。数字经济的运行与合作有赖于安全的网络环境。为保护海量数据的完整性、促进数字要素的高效率流通,中印两国加强网络空间安全合作是应有之义。首先,双方应优先解决两国间的商业摩擦。针对小米、华为、TikTok 等中国企业在印经营受阻问题,中印需加强沟通,寻求合理的针对性解决方案。例如,中国可以提出加大在印度的投资力度以及提高在印本土化运营程度,以换取印度市场对中国企业的开放,这不仅有助于解决中国企业目前在印度市场所面临的困境,也有利于推动两国间的合作,实现共同的数字经济发展诉求。其次,中国可根据印度感兴趣的数字经济规则制定、平台安全和数据保护等具体议题化整为零,分别与之进行合作;同时还应发挥主动性,向印方强调数字产业供应链

安全等中国重视议题的重要性。最后,中国可与印度强化通信、银行、金融、物流系统等数字经济基础设施保护合作,为中印企业在网络空间的经济活动提供稳定、可预期的商业环境。总之,中印应充分认识到数字经济是两国间矛盾较小、合作动力较大的议题,以经济带动安全,可以释放合作的活力和积极性。

其四,消除信息迷雾,以威慑倒逼互信。威慑思想古今中外皆有,有效的威慑可以促使对方基于利益最大化考量不敢或不愿随意采取单边危害安全的行动,从而倒逼对方提升建构安全信任措施的意愿。威慑的有效性取决于实力、使用实力的决心和对手的感知三个要素。[①] 为使威慑有效,一方面,中印两国政府应尝试明确阐述自身的网络安全战略、理论和能力,给予对方直接感知。通过网络空间安全战略、理论和能力的透明化,网络威慑的有效性能够得到加强,有利于倒逼信任措施建构。同时,双方可以借此加深对彼此的了解,降低误判网络安全行为意图的风险。此外,透明度提升也为两国相互借鉴共同提升网络安全防护水平提供了可能。另一方面,在政府沟通之外,中印还需同时加强智库、高校、私营部门等机构的人员交流,[②]发挥私营部门和第三部门在网络安全治理中的主动性和创造性,以民间协力官方,促进信息流动,帮助消除信息迷雾,提升威慑效果。比如两国可借助智库、高校或个人组织的网络安全政策研讨会等形式,增进对于对方网络安全政策的认识;还可借助私营部门对于技术创新、政策风险等问题的敏感度,通过加强投资、优化公私伙伴关系、布局科技产业园区等措施充分准确评估对方的安全政策取向。总之,加强交流沟通,消除信息迷雾,有利于提升政策透明度、增进网络威慑效果,以威慑倒逼互信,是推进中印网络空间安全合作的重要方式。

其五,重视外部因素,以斗争求取和平。当今人类社会正面临世界之变、时代之变、历史之变,地缘政治斗争激烈化,全球态势也极大影响到国际行为体之

① 李彬,胡高辰:《美国视阈中的中国核威慑有效性》,《外交评论》2018 年第 5 期,第 21 ~ 41 页。

② “第三部门”包括公民个人、技术社群等,与政府统称为“公共部门”;“私营部门”则是与“公共部门”相对的概念,可以定义为以市场调节为主体,以组织利益最大化为目的的工商企业组织或盈利性国际组织。参见 Cai Cuihong and Yu Dahao, “The Role of Private and Third Sectors in Cybersecurity Governance: The Russian Ukrainian Cyber Conflict,” *Journal of Governance, Security and Development*, Vol. 4, No. 1, p. 3。

间的双边关系。当前,美西方在现实空间和网络空间均将中国视为主要竞争对手,并对印度进行极力拉拢。面对美西方与印度在网络空间安全领域合作对中国产生的压力,应从两方面着手加以应对。一方面,中国应给予足够的重视,要看到印度与美西方的网络空间安全利益的确在较多方面契合,互信程度较高,其合作态势也可能会持续下去,对中印网络空间安全合作将产生越来越大的阻力。另一方面,中国对此应坚决斗争,不能对美、对印妥协,要看到印度与美西方的网络安全诉求并不完全契合,美国强化与印度的合作更多是出于围堵中国的意图,但印度并不想为了美国的利益而冒被卷入冲突中的危险。因此,中国对美印网络安全动作的态度越是强硬,印度越能感知到与美西方网络结盟的风险。同时,印度也要看到,中印两国事实上都处于世界数字体系中以美国数字霸权为核心的中心—边缘结构下,遭受着中心国家对边缘国家的数字殖民剥削,同属数字“全球南方”,[①]两国在网络空间安全领域的核心利益在根本上其实是一致的,只有中国安全,印度才能安全。总之,重视外部干扰因素的影响,但不能对其妥协,以斗争求取和平,是中印网络空间安全合作顺利推进的重要保证。

四、结　　语

本文全面剖析了中印网络空间安全合作的机遇、挑战与应对。研究发现,中印在网络空间安全领域的安全诉求、发展诉求、治理诉求和战略诉求均有一定程度的契合,分别成为驱动中印推进网络空间安全合作的直接动力、间接动力、深层动力和上层动力。在四大动力的驱动下,中印网络空间安全合作已在双边和多边两个层面取得部分实际成果,存在合作的机遇。然而,中印相关合作仍相当薄弱,面临着共识有限且落实困难的挑战,这些挑战源于中印两国在现实空间的既有矛盾及全球地缘政治态势,包括中印历史纠葛夹杂现实摩擦导致信任危机蔓延、印度自身的民粹化倾向导致合作难以达成、美西方外部因素的离间导致合

① 蔡翠红、于大皓:《“帝国的新衣”:世界数字体系下的美国数字霸权》,《当代世界与社会主义》2024 年第 3 期,第 4 ~ 12 页。

作进程饱受干扰。这些挑战也受到网络空间的自身特点影响,包括技术民族主义强化网络空间斗争色彩、全球网络空间缺乏国际安全制度规范、中印网络空间安全政策均缺乏透明度。若想化解挑战,需采取措施多面并行推进,以多边助推双边,以行动促进战略,以经济带动安全,以威慑倒逼互信,以斗争求取和平。

数字时代和“大变局”时代已然同时到来,中国和印度均面临严峻的网络空间安全态势,两国亟需携手采取积极措施、加强网络安全防护,以弥合安全赤字、维护信息时代的国家安全。中国在网络空间治理方面已取得显著成就,构建了符合国情的网络安全治理体系,努力维护网络空间的和平与稳定。与此同时,印度作为南亚地区的科技大国,也在网络空间安全方面有着自身的优势和特点。两国在网络空间安全领域存在着广泛的共同利益,如能相向而行、求同存异,积极探索网络空间治理的安全合作模式,不仅可以分享网络安全治理经验、提升各自的网络安全技术水平与防护能力,还能加强互信共同应对跨国网络安全威胁,构建一个更加安全公平的网络空间环境,为人类的和平与发展作出贡献。未来,中国和印度应当努力超越分歧、深化合作,共建网络空间命运共同体,携手各国重塑一个公平、安全、开放、有序的新网络空间秩序。