

智能革命场域下我国意识形态安全治理： 态势、挑战及纾解^{*}

王琴棋 马建光

[摘要] 在智能革命场域下，信息传播范式经历了从“线性”向“分布式”的结构性嬗变，意识形态安全治理重心随之呈现出“至播放权—至流量权—至数据权”的三重演进轨迹。随着数字空间逐渐成为意识形态斗争的主战场，数据算法、网络基础设施与社交媒体的技术聚合效应对我国数字空间的意识形态领导权、管理权、话语权构成了系统性挑战。面对技术异化与资本逻辑深度耦合的治理困境，亟须在技术赋能与安全治理的辩证统一中构建新型治理格局，推动治理范式由“被动防御”向“主动塑权”的战略转型，形成“技术—制度协同”“社会—文化共治”“全球—区域联动”三位一体的治理路径，从而筑牢数智时代社会主义意识形态安全防护体系。

[关键词] 智能革命 数智时代 数字空间 算法规训 意识形态安全治理

当前，世界百年未有之大变局加速演进，新一轮科技革命和产业变革正以前所未有的方式展开。在智能革命场域下，一方面，智能化已成为驱动引领经济社会高质量发展的关键引擎；另一方面，智能化也成为大国竞争博弈的重点领域。从世界社会主义发展史看，智能革命可能将社会主义与资本主义的较量引向新的阶段。回顾马克思主义发展史、国际共产主义运动史，从马克思主义诞生之日起，马克思主义与非马克思主义、社会主义与资本主义、无产阶级与资产阶级之间的斗争就没有停止过。习近平总书记强调：“以互联网为核心的新一轮科技和产业革命蓄势待发，人工智能、虚拟现实等新技术日新月异，虚拟经济与实体经济的结合，将给人们的生产方式和生活方式带来革命性变化。”^① 大发展大变革必然引发思想上的大困惑乃至大混乱，我们迫切需要把握智能革命的时代特征，预判风险挑战，将智能优势转化为执政优势，为全面建设社会主义现代化国家提供强大可靠的安全保障。

一、智能革命场域下意识形态安全治理关键因素的出场逻辑

随着智能革命的浪潮席卷全球，数智技术正以其无与伦比的影响力重塑现代社会。“无论我

^{*} 本文系国家社会科学基金青年项目“算力赋能新质生产力的理论逻辑和实践路径研究”（24CKS042）的阶段性成果。

^① 《习近平关于网络强国论述摘编》，北京：中央文献出版社，2021年，第160页。

们视其为工具、伴侣还是对手，它都会改变我们作为理性生物的经验，并永久性地改变我们与现实的关系。”^①在这场革命中，一方面，数字经济的崛起和数字空间的扩张正在重构人类社会的运行逻辑；另一方面，数字文明使意识形态领域成为没有硝烟的战场，数字资本主义将本无意识形态的数学方法和信息技术卷入政治旋涡^②，数字空间的意识形态斗争比物理空间的冲突更具隐蔽性和颠覆性。

（一）意识形态安全治理的基本内涵

进入新时代，随着意识形态领域斗争日趋复杂尖锐，我国将意识形态安全提升到国家安全战略层面，并将其作为重点领域安全问题纳入到总体国家安全观中。“防范化解各类风险是平安中国建设的一项重要任务。要把捍卫国家政治安全摆在首位，坚定维护国家政权安全、制度安全、意识形态安全。”^③意识形态安全不仅是维护国家政权合法性和权威性的关键，也是增强国家文化软实力和影响力的基石，更是提升整个社会凝聚力和向心力的根本所在。意识形态安全治理是建设平安中国的重要任务，也是实现发展和安全相统一的系统性工程。从治理目标看，一方面，要坚决抵制和防范敌对势力意识形态侵蚀；另一方面，要不断实现主流意识形态的巩固和创新。从治理对象看，既有广大人民群众、各种社会力量，也包括企图搞颠覆破坏活动的敌对势力。从治理内容看，既有多元社会思潮相互交织冲击的内源性风险，也有敌对势力对我国意识形态渗透的外源性风险。在智能革命场域下，为适应形势任务的发展变化，意识形态安全治理只能加强，不能削弱。

（二）意识形态渗透：外部势力制造国家混乱的关键变量

从布雷顿森林体系崩溃到新自由主义全球化浪潮，西方资本集团的战略重心完成了由“产业资本在国化”的硬实力战争向“金融资本全球化”的软实力竞争的历史性位移，“工业资本制造了南北世界，现在，金融资本则通吃南北世界”^④。金融资本的获利模式超脱于产业资本的生产环节，主要聚焦于价格差套利策略，列宁就曾用“食利国”和“剪息票”来揭露帝国主义和资产阶级攫取利益的本质^⑤，社会越混乱，经济波动越大，金融资本越能利用价格的剧烈变化进行做多或做空来实现资本快速增殖。随着以美国为首的一些西方国家经济金融化趋势的强化，美国在对外战略上更加热衷于在非西方国家制造“可控混乱”^⑥。伴随这种巧实力和软实力的低成本运作和高收益回流^⑦，“意识形态病毒”从幕后走向台前，成为西方资本集团实现其战略意图的关键杠杆和核心工具。

① [美] 亨利·基辛格、埃里克·施密特、丹尼尔·胡滕洛赫尔：《人工智能时代与人类未来》，胡利平、风君译，北京：中信出版社，2023 年，第 17 页。

② 参见周绍东、邹赛：《国外马克思主义学者关于数字资本主义的研究》，《世界社会主义研究》2023 年第 8 期。

③ 《坚定不移贯彻总体国家安全观 把平安中国建设推向更高水平》，《人民日报》2025 年 3 月 2 日。

④ 《张文木战略文集》第 10 卷，济南：山东人民出版社，2020 年，第 201 页。

⑤ 参见《列宁专题文集·论资本主义》，北京：人民出版社，2009 年，第 186—187 页。

⑥ 田文林：《美国为何热衷策动“颜色革命”》，《人民论坛》2023 年第 9 期。

⑦ 参见温铁军、何志雄、严晓辉：《全球化与软实力竞争》，北京：东方出版社，2024 年，第 51 页。

美国学者斯蒂芬·曼恩（Stephen R. Mann）提出“可控混乱”理念，将国际秩序看成由国家行为体组成的动力系统，国家战略目标就是在这一动力系统中塑造有利态势。为达到这一目标，他主张通过制造可控的混乱局面来塑造有利于美国的国际秩序。无论是国家、政府，还是政治、经济和宗教，都离不开个体行为者的参与，每个人都是冲突能量的载体。这一冲突能量本质上是人的思想、观念和价值观等，每个人都是可被编程的“意识形态软件”。于是，曼恩提出将意识形态渗透作为武器，让美国走向终极“生物战”，“如果我们能够在全球政治混乱之海中的秩序岛屿间灵活移动，我们是否就能以更低的成本达成更好的效果呢？”^① 葛兰西也注意到，霸权的运作不仅依靠暴力和胁迫，还依靠制造共识，塑造与统治阶级利益相一致的认知和诉求，“对其历史发展的领导权属于民间力量，属于市民社会——它也就是‘国家’，而且是事实上的国家本身”^②。安德鲁·科里布科（Andrew Korybko）更是一针见血地指出，“美国花了数年时间组织所谓的非政府组织（NGO）进行意识形态渗透并将其武器化”^③。可见，意识形态渗透成为威胁国家安全的“武器”，意识形态安全治理能力的强弱关系着国家政权安危。

（三）意识形态安全隐患：算法规训下跨国资本对第三世界大众的潜在控制

跨国资本对第三世界的控制已从传统经济领域扩展到技术标准制定权和文明话语权层面。“资本帝国主义所追求的是在任何可能的地方无需借助于政治统治而树立经济霸权”^④。在数字技术深度嵌入经济全球化的背景下，算法技术与跨国资本的“联姻”正对第三世界国家的意识形态安全构成多维度的潜在威胁。这种威胁不仅体现在经济控制层面，更体现为通过技术层面的数据控制和算法规训进行意识形态渗透。跨国资本凭借平台特权掌握全球数据流动的“制高点”，利用算力和算法的技术垄断对第三世界国家施行“数字殖民”，使其陷入“技术依附陷阱”，导致数字主权被削弱。同时，算法并不是中立的工具，而是资本权力在意识形态领域的具象化。技术强国和科技巨头企业可以将人工智能生成内容作为信息操控的工具来实现文化扩张或意识形态渗透的目的^⑤。跨国资本利用算法偏见使生成式人工智能的文本生成隐含“西方中心论”的政治倾向，大数据分析用户行为偏好，定向推送个人主义、消费主义等西方价值观内容，潜移默化地影响和瓦解第三世界国家本土文化认同。由此可见，算法技术与跨国资本的合谋正在重构全球权力格局，第三世界国家面临的技术殖民风险远超传统经济剥削，“算法黑箱”和“信息茧房”使资本主义意识形态传播更具隐蔽性和渗透力，算法技术异化为价值解构加速器，给第三世界国家意识形态安全治理带来新挑战。

（四）数字空间治理：智能革命场域下意识形态安全治理的关键节点

习近平总书记强调：“网络空间已成为人们生产生活新空间，那就应该成为我们党凝聚共识

① Steven R. Mann, “Chaos Theory and Strategic Art”, *The US Army War College Quarterly: Parameters*, Vol. 22, No. 1, 1992.

② 《葛兰西文选（1916—1935）》，北京：人民出版社，1992年，第442页。

③ Andrew Korybko, *Hybrid Wars: Geopolitical Conflicts in the Postmodern Age*, London: Arktos, 2022, p. 97.

④ [加拿大] 埃伦·M. 伍德：《资本的帝国》，王恒杰、宋兴无译，上海：上海译文出版社，2006年，第2页。

⑤ 参见曾润喜、秦维：《人工智能生成内容的认知风险：形成机理与治理》，《出版发行研究》2023年第8期。

的新空间。”^① 在智能革命场域下，人类社会正经历着时空形态与文明价值的双重变革。与前三次工业革命不同，智能革命通过数据要素的重组实现了物理世界与虚拟空间的深度融合，形成了一个新的文明形态——数字空间。数字空间是数字资本主义对过往资本主义历史的一次重演^②。这种“重演”绝非简单的历史循环，而是通过数字技术对资本逻辑进行拓扑性重构，形成了更具渗透性和隐蔽性的新型统治体系。正如尼古拉·尼葛洛庞帝（Nicholas Negroponte）对数字化技术渗透至人类生产生活所提醒的，“每一种技术或科学的馈赠都有其黑暗面，数字化生存也不例外”^③。数字空间也为资产阶级维护霸权统治、攫取剩余价值提供了条件，意识形态安全治理的关键节点也随着智能革命浪潮的到来发生根本性转变。

在工业化时代，主流意识形态掌控在传统媒介手中，信息的生成和分发在可控范围内，传播流向由中心节点向四周扩散，意识形态安全治理的关键节点是“至播放权”。智媒时代，信息的生产和传播流程被重构^④，传统“中心-边缘”结构被分布式节点网络取代，这不仅改变了传统媒介线性传播的风险特征，更重构了意识形态领域风险管控的运行机制。传统的中心化审核把关机制正在让位给算法操控的分布式把关，意识形态安全治理关键节点由显性标识的“至播放权”转向隐性控制的“至流量权”。正如马克思所预见的，“一种非人的力量统治一切”^⑤。数据要素化正使算法这种“非人的力量”的统治从工厂流水线延伸至人的神经末梢，新异化的诞生将意识形态安全治理推向愈加复杂的境地。舆论引导的硬性议程被基于用户数据画像构建的软性议程所取代，“平台-用户-数据”三角闭环形成超国家形态的数据垄断。同时，在“信息成瘾”机制的作用下，用户被消解为失去主体性的“数据躯体”，而“至数据权”则成为意识形态安全治理的关键。

二、智能革命场域下我国意识形态安全的治理态势

随着智能革命浪潮的深入推进，我国已迈入数据驱动、技术引领、虚实融合的新时代。这一变革不仅重塑了经济结构和社会形态，更对我国意识形态安全治理提出了新的要求。数字空间与现实空间的深度耦合使得现实空间中的暴力、分割及不平等现象进入数字空间^⑥。在全球化的数字空间中，数据算法技术、网络通联技术和社交媒体应用使信息加速自由流动、使思想激烈交锋碰撞，给我国意识形态安全治理带来更多不确定性。

（一）滥用数据智能算法：触发社会解构风险威胁意识形态领导权

以算法、算力和数据为核心的人工智能技术正悄无声息地深度嵌入生产生活各个方面，人机

① 《习近平关于网络强国论述摘编》，北京：中央文献出版社，2021年，第74页。

② 参见〔日〕森健、日户浩之：《数字资本主义》，野村综研（大连）科技有限公司译，上海：复旦大学出版社，2020年，第142页。

③ 〔美〕尼古拉·尼葛洛庞帝：《数字化生存》，胡泳、范海燕译，北京：电子工业出版社，2017年，第228页。

④ 参见葛学彬：《智媒时代主流意识形态传播转向的三重阐释》，《思想教育研究》2023年第1期。

⑤ 《马克思恩格斯文集》第1卷，北京：人民出版社，2009年，第233页。

⑥ 参见封帅：《主权原则及其竞争者：数字空间的秩序建构与演化逻辑》，《俄罗斯东欧中亚研究》2022年第4期。

协同、跨界融合与共创分享的智能时代加速到来。“任何时候，只要你买东西、访问网站或者发表评论，都有一支由电子智能体组成的雇佣军在暗处‘观察’着你”^①。各国尤其是技术强国纷纷加大了对数字基础设施的建设投入和布局，力图抢占先机，塑造新一轮战略优势。

在智能革命场域下，数字化与智能化在处理复杂系统的“混沌变量”时形成了辩证统一的技术体系：一方面，数字化通过数据化将不确定性转化为可计算的概率空间。数字空间的诞生彻底打破了认知域、信息域和社会域之间的界域，“过去不可计量、存储、分析和共享的很多东西都被数据化了”^②，自然界的运行、社会的发展、个体的行为，都可以被看作可计算的概率空间。另一方面，智能化通过算法将概率空间升级为自组织的控制论系统。基于大数据蕴含的丰富信息，人工智能不仅可以进行深度分析和挖掘，还可以根据隐藏在数据背后的规律和价值自主作出决策、规划和操控。“意识形态以垄断精神生产营造全社会的统治思想的规律”^③，数字化与智能化的双重作用不仅能构建隐蔽且高效的思想统治体系，也能使其陷入“技术赋能的社会解构”。正如中东地区“阿拉伯之春”的前车之鉴，算法技术的滥用已从工具性辅助演变为系统性颠覆手段。通过多模态传感矩阵构建用户神经兴奋图谱，结合智能手机全天候采集的定位、社交、消费等行为数据，人工智能可自动化完成社会行为模型的训练与意识形态预判干预。当这类算法模型经过对抗性训练和优化迭代后，其输出的秩序参数可能突破社会韧性阈值。这种技术能力如果被恶意部署用于颠覆行动，必将成为国内冲突的“孵化器”乃至“颜色革命”的温床。

（二）使用断网通联技术：隐匿扩散负面信息冲击意识形态管理权

数智时代，各种不良社会思潮的传播更加便捷。智能革命与数字空间的深度耦合下，意识形态安全治理面临前所未有的复杂性，这种复杂性不仅源于技术架构的颠覆性变革，更在于社会思潮传播机制发生了跃迁，即时通信工具构建的“永远在线”状态，使社交关系呈现“虚实纠缠”的新形态。

在智能革命场域下，数字空间的实时性、开放性和无国界性，使信息传播变得更加便捷、迅速、广泛，同时也增加了信息传播的不确定性，这为一些渗透颠覆和捣乱破坏活动提供了隐蔽传播的可能。尤其是断网通信技术，它能够建立隐蔽且难以切割的信息“传播链”。从技术架构角度而言，断网通信技术依托于“去中心化”的分布式节点模式，信息不再依赖于统一的大型服务器枢纽进行中转，而是在多个相对独立的小型终端间跳跃式传递，这直接造就了其隐蔽特性。断网通信使得通信过程相对分散和难以监管，与传统的集中式网络通信相比，监管部门难以对断网通信中的信息内容、通信行为等进行有效的实时监控和管理，可能会给违法违规行为提供可乘之机，如利用断网通信进行非法集会、传播有害信息等。近年来，谷歌和推特公司发布了一款名为“Speak2Tweet”

① [美] 杰瑞·卡普兰：《人工智能时代——人机共生下财富、工作与思维大未来》，李盼译，杭州：浙江人民出版社，2016年，第7页。

② [英] 维克托·迈尔-舍恩伯格、肯尼思·库克耶：《大数据时代》，杨盛燕、周涛译，杭州：浙江人民出版社，2013年，第23页。

③ 侯惠勤：《论意识形态风险及其防控》，《阅江学刊》2022年第5期。

的专用服务,使语音留言能够被自动转换成推文,在断网情况下也可以上传至推特^①。监管缺失与技术隐蔽性相结合给有害信息传播者提供了便利,使诸如极端思想、虚假谣言等内容能够在断网通信构建的隐蔽链条中肆意蔓延,侵蚀社会公序良俗,冲击主流价值观。断网通信技术形成的“影子网络”使信息弥散于无数流动的节点,这不仅对社会治理构成挑战,也严重威胁意识形态管理权,中国亟须在技术发展与社会治理间探寻平衡法则,筑牢数字空间的防御壁垒。

(三) 利用社交媒体平台:批量生产极端思潮解构意识形态话语权

在智能革命场域下,社交媒体作为数字空间的重要平台载体,正在超越电视和纸质媒体成为人们获取信息的主要渠道,其使用量正在呈指数级增长。截至 2025 年 2 月,全球有 55.6 亿互联网用户,占全球人口的 67.9%。其中,社交媒体用户有 52.4 亿人,占全球人口的 63.9%^②。社交媒体的广泛应用正在不断重构人类世界,一方面,它创造了新的价值基础和文化规范,另一方面,它也可能成为解构和摧毁国家认同的“加速器”。

数字空间最大的威胁,并非数字空间系统被攻击,而是人群和思想被控制。在社交媒体深度渗透的当下,思想控制已突破传统宣传的显性模式,演化为基于数据科学的隐性操控体系——通过算法技术将人的主体性降维为可预测、可引导的数据集合体。这种控制范式的根本转型,折射出技术工具理性对人类自由意志的深层侵蚀,其威胁远超物理层面的网络攻击。社交媒体日渐成为示威活动的“指挥平台”,并可能异化为政治动员的“隐形战场”。一方面,利用用户画像技术定制个性化煽动内容,通过算法推荐系统进行靶向传播。这些内容常以“民主”“维权”等话语进行道德包装,实则嵌入诱导对抗的意识形态,使受众在情感共鸣中无意识接受极端思想立场。另一方面,依托社交媒体支付通道与用户基数,构建去中心化募资网络。操纵者通过加密支付渠道筹集资金,其流向完全脱离金融监管体系,这种“暗箱资金”既可用于购买平台广告扩大传播,也可能资助非法活动制造社会裂痕。此外,敌对势力可能通过技术手段制造认知扭曲,建构剧场化抗争场面。比如运用广角镜头与无人机航拍虚增示威规模,部署机器人账号批量传播伪造影像,借助算法复制形成“数据瀑布”,制造“全民参与”的集体幻觉。由此可见,在现代信息传播生态中,社交媒体平台展现的技术特征客观上为敌对势力的分裂活动提供了新型场域,当公民在社交媒体中被数据化处理为可计算的节点时,国家认同的理性基础将受到结构性冲击,这种技术机制与社会心理的互动,正在催生出基于社交媒体传播特性的极端观念生产机制,对主流意识形态安全构成系统性威胁。

三、智能革命场域下我国意识形态安全治理面临的困境

习近平总书记强调:“我们一定要认识到,古往今来,很多技术都是‘双刃剑’,一方面可

^① 参见《“黑客帝国”调查报告——美国中央情报局(CIA)(之一)》, <https://www.cverc.org.cn/head/zhaiyao/CIACH.pdf>。

^② “Digital 2025: Global Overview Report”, <https://datareportal.com/reports/digital-2025-global-overview-report>。

以造福社会、造福人民，另一方面也可以被一些人用来损害社会公共利益和民众利益。”^① 在智能革命场域下，数字生产方式塑造了一个由数字社会空间和数字技术空间构成的虚实交融、联通互动的数字空间。数字技术、算法霸权与资本逻辑的深度耦合，催生了数据垄断、数字剥削与景观幻象，导致社会主体性弱化、文化认同碎片化及意识形态风险加剧。

（一）数据安全治理困境：精准画像技术异化导致定向渗透风险

数据已经渗透到社会生活的方方面面，深刻改变着生产方式、生活方式和社会治理方式^②。智能终端、社交网络和云计算技术的普及，使人类数字生命体征在虚拟空间形成持续性数据沉淀。这种技术赋能在重构社会运行方式的同时，亦衍生出新型治理难题。强大的数据截取和分析能力意味着意识形态渗透的主动性^③，信息操控技术可以通过干预机制对主流意识形态进行解构，数据安全已超越个体隐私保护层面，上升至国家意识形态安全战略高度。

在智能革命场域下，数据价值的释放机制呈现显著变化，从初级的数据采集存储转向深度挖掘与智能应用。算法通过建构用户认知框架分析模型，对搜索、交互、消费等数字行为进行多维度解析，形成涵盖心理特征、价值取向、行为模式的精准画像系统。这种基于用户行为数据的画像建模不仅应用于商业范畴，也可能转换为意识形态渗透的技术载体。这种基于“需求颗粒度”分类的定向传播机制，在满足受众“认知闭合需求”的同时，也实现了对特定群体价值观的定向塑造。因此，基于数据画像的精准渗透机制会引发双重社会风险：在微观层面，个体认知结构的同质化会抑制思维创新与观念更新，导致主体性消解；在宏观层面，群体间信息壁垒的强化催生价值共识断裂，造成公共领域话语冲突，威胁意识形态领导权。由此可见，在推进数据要素市场化配置过程中，这种数据价值的深度挖掘若缺乏有效规制，可能会引发社会撕裂风险，对主流意识形态安全构成系统性威胁。

（二）网络安全治理困境：网络“翻墙”技术迭代造成跨域渗透漏洞

尽管网络化社会组织形式在历史上也曾存在，但新信息技术范式却为其渗透扩张遍及整个社会结构提供了物质基础^④。智能革命场域下，数字空间正在形成超越物理域的关系拓扑结构，数字技术不仅重构了社会组织的空间形态，更随着数字基础设施迭代发展，使组织渗透更便捷和彻底。这种技术范式变革不仅重构了信息传播的物理空间，更在深层逻辑上挑战了民族国家基于领土主权建立的信息治理体系。

网络“翻墙”技术作为信息控制权博弈的技术载体，其本质在于突破国家网络主权边界的物理隔离，构成了数字地缘政治竞争的新型战略工具。以美国为首的西方国家将“网络自由”纳入其数字殖民战略体系，通过系统性开发加密网络通信技术、断网通联技术及暗网技术等网络

① 习近平：《论党的宣传思想工作》，北京：中央文献出版社，2020年，第202页。

② 参见段学慧、张娜：《数据要素及其形成新质生产力的机理研究》，《经济纵横》2024年第7期。

③ 参见王超：《大数据时代我国意识形态安全探析》，《学术论坛》2015年第1期。

④ 参见〔美〕曼纽尔·卡斯特：《网络社会的崛起》，夏铸九、王志弘译，北京：社会科学文献出版社，2001年，第569页。

技术工具，构建起覆盖全球的数字渗透体系，形成了维护其霸权的新型权力架构。尽管美国非常强调数字信息领域对民主政权的挑战，但事实上美国才是那个最擅长利用其垄断的全球互联网平台和数字信息技术对其他国家政权发起舆论战、认知战的国家^①。从意识形态渗透层面看，网络“翻墙”技术构建了平行于国家主流叙事的信息空间，通过镜像网站、加密社交平台及去中心化存储技术，社会共识的生成场域由公共舆论空间向碎片化加密社群转移，使敌对势力得以绕过内容监管体系，向受众推送经过精心包装的政治叙事。面对这种技术驱动的意识形态渗透，缺乏辨识力的网民极易坠入敌对势力设置的“政治陷阱”，这将导致社会共识基础瓦解，对国家意识形态安全造成威胁。从技术演进路径来看，各类新型网络“翻墙”工具围绕“打破边界限制”不断迭代升级，加密性和隐秘性越来越强，为敌对势力对我实施意识形态渗透打开了缺口。由此可见，网络安全治理已进入“技术政治化”与“政治技术化”相互建构的新阶段。然而，网络“翻墙”技术的“双刃剑”特性使其在现有国际法律框架和技术标准下难以有效区分和规制。同时，渗透技术与防御体系呈现非对称性发展态势，治理响应周期与技术迭代速度严重不匹配，使传统的“堵漏式”治理范式遭遇严峻挑战。

（三）社交媒体治理困境：虚假信息多模态裂变引发价值失序危机

习近平总书记指出：“网络是一把双刃剑，一张图、一段视频经由全媒体几个小时就能形成爆发式传播，对舆论场造成很大影响。”^② 网络社交媒体的去中心化信息交互架构，在消解传统媒介中心化范式的同时，亦成为境外意识形态渗透与价值观念非对称博弈的技术载体。截至 2024 年 12 月，我国社交网络用户规模达 11.01 亿人，占网民整体的 99.3%，社交网络成为网民获取资讯的最主要渠道^③。AI 社交的兴起一方面推动了社交网络行业内容生态丰富发展，另一方面也为敌对势力生成多模态虚假信息提供了工具，存在主流媒体舆论主导权被解构的风险，可能对我国意识形态安全造成系统性威胁。

“数字化世界是一个崭新的疆土，可以释放出难以形容的生产能量，但它也可能成为恐怖主义者和江湖巨骗的工具，或是弥天大谎和恶意中伤的大本营。”^④ 数字空间作为新兴社会场域，其技术赋能在释放生产性潜能的同时，也埋下了系统性价值失序的隐患。其一，舆情智能操纵系统依托生成式 AI 与社交机器人网络，构建数字拟态舆论场。敌对势力通过社会热点事件的语义捕捉，定向投放算法生成的虚假观点集群，通过评论区操控和情绪化叙事重构舆论生态，形成“数据民主”假象。这种“裂变式”传播机制不仅扭曲公众对真实民意的认知，更通过“伪共识”倒逼机制干预政策制定，如果任由这种传播机制蔓延，可能会动摇意识形态治理权根基。其二，“深度伪造”技术助推虚假信息进入神经操控阶段。通过 AI 换脸、语音克隆、场景生成

① 参见温铁军、何志雄、严晓辉：《全球化与软实力竞争》，北京：东方出版社，2024 年，第 51—52 页。

② 习近平：《论党的宣传思想工作》，北京：中央文献出版社，2020 年，第 356 页。

③ 参见《第 55 次中国互联网络发展状况统计报告》，<https://cnnic.cn/NMediaFile/2025/0428/MAIN17458061595875K4FP1NEUO.pdf>。

④ [美] 埃瑟·戴森：《2.0 版数字化时代的生活设计》，胡泳、范海燕译，海口：海南出版社，1998 年，第 17 页。

等技术生成多模态虚假信息，彻底解构了“眼见为实”的认知范式。当政治人物的政策宣言、历史事件的影像档案均可被算法重构时，“煤气灯效应”便从人际操控上升到社会层面的集体认知篡改。这种技术辅助下的系统性欺骗不仅会造成政府信任危机，更在精神层面重塑群体记忆图谱，甚至可能削弱意识形态话语权的整体稳定性。其三，算法推荐机制演化为“数字利维坦”的动力装置，通过大数据画像锁定目标人群，以长周期、高密度的虚假信息渗透实施意识形态解构，最终在群体极化中实现价值坐标的集体偏移。当传统的信息系统被打破之后，处于其中的人们的“旧的角色结构可能被信息流的新模式所破坏”^①。可见，多模态虚假信息的“裂变式”传播机制正在成为新型意识形态博弈工具，这在一定程度上使传统的线性传播治理范式效能衰减，更容易导致社会价值系统性失序，将人类推向“后真相文明”的临界点。

四、智能革命场域下我国意识形态安全治理路径

习近平总书记指出：“在互联网这个战场上，我们能否顶得住、打得赢，直接关系我国意识形态安全和政权安全。”^② 在智能革命场域下，数字空间安全不仅关乎技术的发展方向，更关乎我国意识形态安全和政权安全。在现代科学技术的本质中蕴含着一种支配、统治人和自然界的盲目的力量^③，“非人的力量”在智能革命场域下更加难以控制。因此，如何应对数字空间竞争，坚守数字空间意识形态阵地成为当前亟须解决的问题。随着中国整体实力包括硬实力和软实力的提升，以及西方资本主义固有矛盾的日益加剧，我们已经具备了扭转意识形态安全治理格局被动局面的条件。相较于传统意识形态安全治理，数字空间意识形态安全治理需超越传统线性传播的“堵漏式”防御思维，转向多维立体“负熵型”综合治理模式，即通过智能技术压缩虚假信息的生存空间，以弹性制度优势统筹发展和安全，借助多元共治氛围激活社会内生动力，凭借文化自信培育理性认知生态，依托全球协作应对资本主义渗透威胁。在数字时代构建起既能抵御意识形态渗透、又能促进知识共享的“认知共同体”，为人类文明在数智化浪潮中的可持续发展筑牢根基。

（一）技术－制度协同创新：构建智能韧性的治理体系

习近平总书记强调：“数字经济事关国家发展大局。我们要结合我国发展需要和可能，做好我国数字经济发展顶层设计和体制机制建设。”^④ 智能革命场域下，面对数字空间发展的新形势、新挑战，必须强化统筹发展和安全的顶层设计和总体规划，实现技术－制度协同创新。一方面，要通过技术赋能提升制度的预见性与执行力；另一方面，要以制度约束确保技术的可控性与向善

① [美] 约书亚·梅罗维茨：《消失的地域：电子媒介对社会行为的影响》，肖志军译，北京：清华大学出版社，2002年，第165页。

② 《习近平关于网络强国论述摘编》，北京：中央文献出版社，2021年，第51页。

③ 参见俞吾金：《意识形态论（修订版）》，北京：人民出版社，2009年，第386页。

④ 《习近平著作选读》第2卷，北京：人民出版社，2023年，第539页。

性，构建智能韧性的治理体系。

首先，党的领导是构建韧性治理体系的关键锚定。“中国共产党是中国特色社会主义事业的领导核心，所以必须加强和改善党的领导，充分发挥党总揽全局、协调各方的领导核心作用。”^①在建设数字中国进程中，党的领导发挥着关键作用，是确保意识形态安全的基石。在数字空间意识形态安全治理中，党的领导不仅体现在政策制定和战略规划上，更体现在技术赋能与制度协同的动态平衡中。在新时代意识形态安全治理中，必须坚持价值理性与工具理性的统一^②。党作为最高政治领导力量，要超越局部利益，通过制度设计平衡效率与公平，构建具有中国特色的智能韧性治理体系，使技术创新与制度设计有机结合，确保数字空间安全治理的有效性和可持续性。

其次，以核心技术自主化突破数字霸权枷锁。在经济全球化背景下，数字技术已成为国际竞争的新焦点，核心技术自主化是构建智能韧性治理体系的基础。在智能革命场域下，以人工智能、大数据、量子计算为代表的新技术革命正在重塑全球格局。为了夯实意识形态安全治理的技术基础，要继续发挥社会主义制度在资源整合、战略规划与价值引领等方面的优越性，延续新型举国体制在科技博弈、教育转型、人才培育方面的竞争优势；要不断加大基础研究投入，推动产学研深度融合，打造自主可控的智能技术生态体系，进而有效摆脱数字殖民威胁，彻底打破数字霸权枷锁。

最后，加强数据安全制度建设是智能韧性治理体系的重要保障。数据作为新生产要素，在流动、分享、加工和处理的过程中数字经济实现复用增效和聚合增值。在万物皆可数据化的智能革命时代，数字空间急剧增加的海量数据既是重要资源，也直接影响意识形态安全治理效能。习近平总书记指出：“要切实保障国家数据安全。要加强关键信息基础设施安全保护，强化国家关键数据资源保护能力，增强数据安全预警和溯源能力。”^③对数字空间意识形态安全治理，离不开完善有效的数据资源管理机制。要加强政策、监督、法律的统筹协调，加快法规制度建设^④。一方面，要专项立法先行。建立“敏捷立法”机制，以技术迭代速度匹配制度更新。从源头上把控数据权属和质量，明确数字空间的行为规范和责任边界。另一方面，要动态分级监管。按照影响力划分数据监管等级，采取“底线监管+动态评估”模式，围绕数据全生命周期构建兼顾安全与创新的数据安全监管机制，确保数据使用在法治轨道上运行，避免因数据乱象引发意识形态安全风险。

（二）社会—文化协同共治：激活内生性防御生态

智能革命场域下，技术变革的内在机理正在由“工具辅助”向“自主系统”跃迁。数字资本主义通过算法推荐、数据殖民与资本权力，将意识形态渗透隐匿于日常生活场景中，形成

① 《习近平谈治国理政》第1卷，北京：外文出版社，2018年，第13页。

② 参见洪晓楠、王坤平：《新时代意识形态安全治理：总体样态、原则遵循和实践方略》，《探索》2020年第6期。

③ 《习近平关于网络强国论述摘编》，北京：中央文献出版社，2021年，第97页。

④ 参见《总体国家安全观学习纲要》，北京：学习出版社、人民出版社，2022年，第118页。

“自主无意识支配”。相较于对单一行动者点式数字空间行为的规制，治理关注点逐渐转移到数字空间场域内多元行动者合作、谈判、协调、对话的“关系结构化互动”上来^①。与工业时代的“机械安全”相比，数智时代的意识形态安全防御应从控制论思维转向生态论思维——激活内生性防御生态，通过多元主体参与、培育文化自觉、重构数字空间价值秩序来构建抵御数字异化的深层防线。

第一，变革治理范式，由单向管控向多元主体协同治理转变。单一治理主体难以应对数智时代意识形态风险的弥散性特征，自上而下单向决策难以适应技术迭代的自主性趋势，因此，需要依托社会多元主体构建内生性协同防御格局。一方面，要推进数字空间形成跨领域协同治理模式，调动各方面积极性，发挥各主体作用，广泛汇聚各方智慧和力量。在设计规则时需要多部门共同协调，从整体上提升国家数字能力，为国家加强在数字领域的自主性形成合力^②。在责任落实上，增强数字空间安全治理的内生动力。习近平总书记强调，“国家安全一切为了人民，一切依靠人民，充分发挥广大人民群众积极性、主动性、创造性”^③。要激活人民作为国家安全后盾的内生活力，汇聚全社会维护国家安全的强大合力。要赋予企业、社会组织、公众等多元主体更多参与权，形成公众参与制度化、平台责任明晰化、第三方智库赋能化的治理生态。另一方面，党要发挥总揽全局、协调各方的引领作用，兼顾政府监管、企业创新、社会监督等多方诉求，防止利益博弈导致治理内耗。搭建信息共享平台，以便及时了解全貌，围绕政策措施科学深入研讨，遇紧急情况迅速集合力量处理。

第二，厚植文化自信，不断夯实抵御意识形态侵蚀的软屏障。内生性防御生态需要通过全民在社会文化层面的集体觉醒，不断巩固文化主体地位。“如果‘以洋为尊’、‘以洋为美’、‘唯洋是从’，跟在别人后面亦步亦趋、东施效颦，热衷于‘去思想化’、‘去价值化’、‘去历史化’、‘去中国化’、‘去主流化’那一套，绝对是没有前途的！”^④“数字自由”“数字民主”等资本主义虚假叙事再华丽再精致也难掩其文明根基的腐朽。在数智时代，文化自信作为“最基本、最深沉、最持久的力量”，不仅是民族精神的内核，更是我们抵御数字资本主义认知侵蚀的战略武器。我们要激活文化内生动力，利用数字化转型机遇弥合“信息逆差”与认知鸿沟，提升全民数字文明素养。构建自主知识体系，提高全民对资本主义文化的批判性辨识能力，夯实中国式现代化的文化根基，实现数智时代意识形态安全治理的深层超越。

（三）全球—区域协同联动：共建数字命运共同体

智能革命场域下，意识形态安全治理的核心矛盾体现为资本主义数字霸权与人类解放需求之间的冲突。在数字资本主义主导的全球体系中，技术霸权与数据殖民加剧了全球南方与北方国家

① 参见李彪、高琳轩：《复杂现代性视角下中国数字空间治理的新特征》，《新闻大学》2023年第11期。

② 参见高奇琦：《国家数字能力：数字革命中的国家治理能力建设》，《中国社会科学》2023年第1期。

③ 《习近平谈治国理政》第4卷，北京：外文出版社，2022年，第390页。

④ 《习近平文化思想学习纲要》，北京：学习出版社、人民出版社，2024年，第46—47页。

之间的数字鸿沟，威胁全球数字空间的公平性与安全性。为破解数字资本主义“中心化霸权”的困局，我们迫切需要运用全球－区域协同联动的分布式治理策略，通过价值超越、规则重构与实践创新，构建数字命运共同体，实现社会主义文明对资本主义剥削逻辑的扬弃与超越。

第一，深化技术向善伦理，重构数字空间价值秩序。马克思恩格斯认为，自然科学的发展应服务于人类解放，“通过工业日益在实践上进入人的生活，改造人的生活，并为人的解放作准备，尽管它不得不直接地使非人化充分发展”^①。在数字资本主义主导的全球格局下，“资本正义”遮蔽了人的劳动价值，劳动者被异化为“数字躯体”，技术异化与资本逻辑的合谋已严重威胁人类社会的公平与正义。当下亟须重构数字空间价值秩序，凝聚技术向善的伦理共识，树立数据资源的公有属性和技术服务于人民的价值导向，使智能革命发展成果更好惠及人民。同时，要推动智能媒体与主流意识形态深度融合，将人工智能技术应用于文化传播，使技术成为增强社会主义价值观凝聚力的载体。

第二，坚持共商共建共享的全球治理观，参与全球数字治理进程。当前全球数字空间规则由少数发达国家主导，他们以“规则制定者”自居，长期通过“长臂管辖”侵犯他国数据主权，而发展中国家在数据主权、算法透明性等问题上则缺乏话语权。为打破“技术达尔文主义”的丛林法则，防止规则制定沦为霸权工具，我们要加快构建中国话语和中国叙事体系，全面提升国际传播效能^②，深入参与联合国框架下的数字空间交流合作，推动共商共建共享的多边协商，反对单边制裁、极限施压，打破西方“互联网自由联盟”的伪善叙事，推动全球数字空间治理由西方主导的“俱乐部模式”转向联合国主导下各方参与的包容性框架，为发展中国家争取更多规则话语权。

第三，深化区域合作，构建分布式数字空间安全治理网络。在数字资本主义主导的全球体系中，技术霸权与数据垄断加剧了安全风险，中心化治理模式难以应对复杂的网络攻击与意识形态渗透。我们应推动发展中国家区域合作，构建分布式数字空间安全治理网络。通过基础设施共建、技术能力提升、数据安全协同、人才交流合作及政策多边协商等区域协作实现资源共享、风险共担、能力互补。这不仅是抵御数字殖民、维护主权安全的战略选择，更为全球南方提供了第三条道路——既非依附于西方数字殖民体系，亦非孤立于经济全球化浪潮，而是通过平等协作实现“技术普惠”与“文明共生”，使数字空间真正成为连接人类命运的共同纽带，而非加剧分化的无形之墙。

（王琴棋系国防科技大学马克思主义学院 2024 级博士研究生、助理工程师；马建光系国防科技大学国际问题研究中心主任、教授、博士研究生导师）

〔责任编辑：张 婷〕

① 《马克思恩格斯文集》第 1 卷，北京：人民出版社，2009 年，第 193 页。

② 参见《中共中央关于进一步全面深化改革、推进中国式现代化的决定》，北京：人民出版社，2024 年，第 34 页。