

引用格式: 尹召凯, 张为付. 三十年来中国网络科技的社会风险与防范路径. 中国科学院院刊, 2025, 40(12): 2172-2180, doi: 10.3724/j.issn.1000-3045.20241224002.

Yin Z K, Zhang W F. Three decades of Chinese Internet technology: Social risks and prevention pathways. Bulletin of Chinese Academy of Sciences, 2025, 40(12): 2172-2180, doi: 10.3724/j.issn.1000-3045.20241224002. (in Chinese)

三十年来中国网络科技的社会风险与防范路径

尹召凯¹ 张为付^{2*}

1 南京大学 信息管理学院 南京 210023

2 南京财经大学 国际经贸学院 南京 210023

摘要 随着大数据、人工智能、移动互联技术的跃升与应用, 网络科技在推动社会发展的同时, 其衍生的负向效应逐渐显现。文章基于批判性视角, 运用逻辑思辨方法, 系统梳理中国网络科技30年来社会风险的演化与特征表现, 揭示其在数据治理、资本运作和政治传播层面引发的多重隐患。新形势下, 防范化解网络科技的社会风险, 需从价值引领、制度规制、技术赋能、多元共治等方面精准施策, 从被动应对转向主动防范, 从而筑牢国家安全屏障, 推动科技强国建设, 让网络科技发展更好地造福人民。

关键词 网络科技, 社会风险, 人工智能, 国家安全, 科技强国

DOI 10.3724/j.issn.1000-3045.20241224002

CSTR 32128.14.CASbulletin.20241224002

1994年, 中国通过一条64 K国际专线全面接入国际互联网, 开启了中国互联网时代, 激荡至今。互联网自诞生起便是一项独特的超级“大规模技术系统”(LTS), 而网络科技则是以互联网为核心, 融合大数

据、人工智能、移动互联等技术形成的数字化技术集群, 是技术与社会交织融合的生成系统^[1]。截至2024年12月, 中国网民规模达11.08亿人, 互联网普及率达78.6%^①, 网络科技已成为社会运行的操作系统。随

*通信作者

资助项目: 江苏高校哲学社会科学研究重大项目(2023SJZD082), 中国音像与数字出版协会科研项目(SZCB2024-04), 国家自然科学基金项目(21BJY052), 南京大学“研究阐释党的二十大精神”专项(2025300093)

修改稿收到日期: 2025年11月22日

① 中国互联网络信息中心(CNNIC). 第55次中国互联网络发展现状统计报告. (2025-01-20)[2025-03-12]. <https://www.100ec.cn/detail-6646318.html>.

着大数据、人工智能、移动互联技术的跃升，网络科技已呈现移动化、智能化、社交化的新特征，也出现了数字经济、平台经济等新的经济表现形态。乌尔里希·贝克（Ulrich Beck）^[2]将后现代社会或者说信息社会、高技术社会、媒体社会诠释为“风险社会”，并认为风险是技术本身失控构成的现代性威胁。审视互联网发展的反面，不难发现，作为智能社会的基础性设施，网络科技能通过数据捕捉每个社会个体的要素，其应用所引发的社会风险不容忽视。习近平总书记强调，“总体国家安全观是建设更高水平平安中国的重要遵循”，“防范化解各类风险是平安中国建设的一项重要任务”^[3]。回溯中国互联网30年来发展进程，网络科技在技术狂飙中产生何种负面效应？数智时代又潜藏着哪些社会风险，该如何化解？这些关键问题，已成为平安中国建设进程中亟须回答的时代命题。文章聚焦网络科技的社会风险，通过演进视角分析网络科技30年发展的“双刃剑”效应，从数据、资本以及政治等关键维度分析互联网等数字技术嵌入社会应用引发的负外部性，从发展的视野提出化解策略。

1 双刃剑效应：网络科技的形态演变与作用审视

1994年的中国正式实现国际互联网的全功能连接，信息时代由此启程，呈现出不同阶段的标志形态：Web 1.0阶段以门户网站、电子邮件为代表，是连接人与信息进行单向线性传播的静态网页，用户是被动接受者，只能浏览内容，无法参与互动；Web 2.0阶段以社交网络、内容平台、电子商务、即时通信等为代表，注重用户生成内容的双向互动，用户成为可创作、分享、评论以及消费的主动参与者；Web 3.0阶段以加密货币、非同质化代币（NFT）等为代表，是以区块链为核心技术的去中心化新一代互联网，用户成为数据所有者，能控制个人身份和资产；Web 4.0阶段

则以人工智能（AI）助手、元宇宙平台等为代表，注重数智化、万物互联和虚实结合，用户与虚拟世界深度交互，实现万物皆媒、智周万物，形成世界的互联互通。需要指出的是，这里划分的4个阶段不是此与彼的生长消亡，而是逐渐演化，各有侧重，彼此交织。经过30年发展，中国互联网始终围绕用户需求进行产品研发和版图扩张，已成为国家发展的关键基础设施，呈现出福祉和风险共存的“双刃剑”效应。

1.1 网络科技的社会福祉

网络科技广泛应用在居民生活的各个方面，极大便利了信息获取、交流沟通和娱乐休闲，同时智能家居、机器翻译等智能技术也逐渐融入日常生活。网络科技的发展消解了传统的垄断、集权与中心化，型构兼具流动性、融合性与去中心化特征的网络社会新秩序，展现出其发展的社会福祉效应。① **网络为个体赋权**。互联网技术促进了知识和资源的流动，消弭了社会等级的差序格局，也改变了现代社会的权力结构。数字平台赋予个体发声渠道，重塑了公共话语空间，使个体意见得以汇聚并影响舆论。② **网络激发个体潜能**。网络科技重构了用户的主体性，个体前所未有的社会传播主导权、精准信息检索能力、资源优化配置效率及社交网络链接效能被网络科技大大激发^[4]，推动用户从信息接收者转变为多维度的数字行动主体。③ **网络开放市场竞争**。互联网技术重构商业生态体系，推动市场不断透明化，避免了“信息的不对称”带来的陷阱。用户通过算法匹配获得精准供需对接，价格比较工具实现跨平台实时比价，社会化评价体系构建起新型消费信任机制。

1.2 技术演进中的负面效应

当我们跳出正向的福祉逻辑去审视智能时代的网络科技，会发现它在造福于民的同时，也日益暴露出其另一面：智能算法、超级平台等新特征所带来的负面效应。① **平台从聚合生长到无序竞争**。互联网组织经历了从单一产品向生态平台的演进。头部平台通过

不断地聚合形成覆盖多场景的数字生态系统。例如，微信、淘宝等超级平台通过整合社交电商、本地生活和金融服务等垂直领域，已演变为数字基础设施。平台经济的网络效应和边际成本递减，诱使资本驱动下的非理性竞争：2010年，“3Q大战”^②首开强制用户“二选一”先河；2017年，共享单车过度投放导致“单车坟场”暴露了流量争夺战的资源错配；2020年，社区团购领域的“菜篮子争夺战”，折射出平台资本无序扩张对民生领域的冲击。② 用户从被补贴“收编”到被垄断“收割”。传统媒体的二次售卖理论是指先将媒介内容卖给消费者，再将消费者的注意力卖给广告商。而在互联网平台，初期以优惠券、免费权限等补贴形式迅速“收编”用户，形成市场支配地位后，再实施利润的攫取。一旦形成垄断，“收割”便随之而来：通过动态定价、“大数据杀熟”等算法手段最大化利润；通过抬高佣金、流量倾斜等方式挤压中小商户的生存空间。这种新霸权的恶果，远不止让用户为最初的“补贴”买单，更在于阻碍了生产要素市场化配置和商品服务流通的体制机制，扭曲了正常的市场竞争。最终，在生产、分配、流通到消费的各环节均受制约，对建设全国统一大市场构成了深层挑战。

2 网络科技社会风险的具体表现

网络科技的演进始终在与社会结构相互塑造中前行，但是革新速度远超社会制度调适能力。数智时代，网络科技在数据、资本和政治等多方面带来新的社会风险。

2.1 数据治理挑战：网络科技对社会治理的多维冲击

在网络科技的驱动下，数据成为人类生产、生活

和治理的关键要素。在全球依靠网络科技进行数字化治理转型的同时，也要时刻面对数据引发的治理挑战。

(1) 数据过度收集与算法控制机制。尼葛洛庞帝(Nicholas Negroponte)^[5]曾预言数字化时代的个性化服务图景，并提出“我的日报”概念。这一构想如今已演化为基于用户兴趣画像的个性化推送机制，常见于新闻资讯、电子商务等各类网络平台。随着深度学习算法的迭代升级，个性化推荐已经成为网络科技的基本配置，但随之衍生的信息控制风险也愈发凸显。基于用户基础数据的推送算法，为了“取悦”用户，不仅会精准推送其偏好的信息，还会利用共同爱好连接用户关系形成圈层效应。当个体长期处于经过算法筛选的信息环境中，将导致双重认知困境：① 信息获取渠道因算法过滤而持续收窄，形成“始于兴趣偏好，困于兴趣偏好”的“信息茧房”；② 社交圈层内部因观点的高度趋同产生回音室效应，通过持续的观点共振不断强化既有认知。这种算法控制机制被Pariser^[6]称为“过滤气泡”，形象揭示了数字平台如何通过信息隔离构建认知壁垒。值得警惕的是，算法推荐具有自我强化的“滚雪球”效应，当极端观点在封闭圈层内持续共振，可能引发群体极化现象。这种技术裹挟的价值观扩散机制，使得非理性思潮突破物理空间限制，在虚拟社群中形成新传播态势。

(2) 泛在化信息采集与隐私边界消解。在数字化生存的默认契约中，用户通过隐私让渡换取技术便利已成为普遍实践。但个人信息被无限制地泄露、售卖、使用导致隐私的边界在加速消解。① 数据泄露会降低社会信任。福柯(Michel Foucault)^[7]提出的“全景监狱”形容了监视的控制力量。在互联网时代，这种力量催生了“时刻被监视”的数字焦虑，致使部分

② 腾讯与360之争是中国互联网历史上具有里程碑意义的商业竞争与法律纠纷事件，涉及两家头部企业(腾讯、360)在安全软件领域的激烈对抗，并引发对行业垄断、用户权益及互联网生态的广泛讨论。

用户采取注销账号、删掉朋友圈等数字断连行为来对监控暴力抵抗。^②数据黑产影响公民生活甚至威胁安全。教育培训、卖房卖车、保险办理等骚扰信息无孔不入，它总能精确判断用户当时所需，对其进行密集的信息骚扰，更有甚者，冒充用户亲人朋友发送诈骗消息，造成了个人财产的严重损失。^③隐私让渡与窃取引发新挑战。信息采集不仅包含用户默许的隐私让渡，也涵盖了未经“知情同意”的隐私窃取，如传感器悄无声息地收集生物特征信息，恶意程序伪装合法应用窃取通信记录等，由此引发的一系列新型数字安全问题值得关注。

(3) 舆情传播失序与信息核验困境。网络参与主体多元化、参与方式多样化、信息传播的即时化、传播渠道多样化，使得舆论治理变得更加复杂。一方面，专业化的数据包装公司通过算法机器人、虚拟账号集群等技术手段，系统性地实施议程设置与情感动员，误导舆论走向；另一方面，受众认知制约信息筛选水平。相关报告显示我国网民中初中及以下学历群体占比达40.5%，而受过高等教育的群体仅占18.8%^③。这种中低学历网民居多的结构，更易使网络信息环境被情绪化内容主导。“后真相”被《牛津词典》评选为2016年的年度词汇，揭示了客观事实对民意影响弱于个体情感诉求及价值信念。部分媒体为争夺注意力资源，刻意放大争议性内容，造成谣言肆虐，破坏了主流媒体的社会公信力。正如2020年新冠疫情暴发后，与之伴随的“信息瘟疫”同样可怕——借助社交平台算法推荐形成跨圈层传播，助长民众对于疫情的恐慌，左右对疫情真相的判断，严重削弱公共卫生应对效能。

(4) 技术滥用风险与数字伦理缺失。在网络科技迅猛发展的同时，作为重要保障的数字伦理却严重脱

节。人工智能可以写新闻、写诗歌、做虚拟主播，与机器人谈恋爱亦不再是电影故事。但与之相伴的是算法歧视、人工智能滥用、假新闻……人类已经为数据失范付出代价，也无法估量技术失控的影响。当前，单是数字版权问题就难以达成共识，更遑论全领域科技驱动下的数据颠覆，乃至全球勠力发展的数字孪生。正如温德尔·瓦拉赫（Wendell Wallach）^[8]所言，技术的潜力令人惊叹也令人畏惧，新技术无法回答如何解决这些技术所引发的道德问题和投资风险。遵循数字伦理、呼吁科技向善成为与科技创新相向而行的关键行动。

2.2 资本主导异化：网络科技与资本利益的深度捆绑

30年来，在网络科技、产品不断更新迭代的背后，除了用户需求的驱动，更有资本力量的追逐。

(1) 平台垄断与市场扩张。从O2O（线上到线下）、共享经济到直播电商，每一轮技术迭代都伴随着资本的“圈地运动”，最终形成少数超级平台垄断的格局。与传统企业不同，数字平台凭借用户规模和数据积累，天然具备垄断优势。^①巨头掌握海量用户行为数据，既能对消费者实施动态定价，进行“大数据杀熟”，又能压制竞争对手^[9]。^②超级平台对市场的支配作用，降低了小企业的创新积极性。无论小型企业产品多么卓越，在缺乏超级平台流量支持的情况下也难以吸引用户。而在寻求超级平台庇护的过程中，其原有的创新动力逐渐减弱。^③垄断能一定程度提高生产效率，但也滋生一系列社会问题，如前文所谈到的社区团购问题。2020年12月，中共中央政治局召开会议，首次提及“强化反垄断和防止资本无序扩张”，进一步发挥政策作用来平衡创新与公平竞争，为平台圈地运动降温。

(2) 算法优化与数字劳工权益侵害。互联网诞生

^③ 中国互联网络信息中心(CNNIC). 第46次中国互联网络发展现状统计报告. (2020-09-29)[2024-11-1]. https://www.cac.gov.cn/2020-09/29/c_1602939918747816.htm.

了数字劳工^[10]，资本的驱逐让更多的数字劳工异化。“外卖骑手被困在系统里”的故事揭示了数据、算法、平台像无形的陀螺精密控制着每个个体的劳动模式：程序员履行平台决定，不停优化算法规则；外卖员与算法时间赛跑，“五星好评”更是无形之中让外卖员为用户的情绪服务买单；平台用差评率、超时率等数据考核站点，将风险转嫁给骑手和站点^④。智能化的网络科技让更多的数字劳工困在算法和系统中，这一逻辑可延伸至更广泛的领域，每个互联网个体在某种程度上都已成为网络平台的数字劳工。例如，抖音平台本身不直接生产内容，而是激励用户无偿地浏览与创作，构成平台的核心资产和流量基础；“今日头条”不生产内容，却有强大的算法机制抓取新闻数据，定向分发推送；直播平台不生产内容，却能在主播展演下将“人、货、场”合一，将流量变现。算法优化的背后是精巧的资产增值，如何守护数字时代下劳动者的权益，已成为亟待解决的难题。

(3) 垂直行业与灰色产业链滋生。网络科技向垂直行业渗透时，也催生出游走在监管边缘的灰色产业。在金融行业，互联网金融强力渗透中小微企业和居民信贷，信贷消费活力空前，个人对个人网络借贷（P2P）、股权众筹、互联网保险正值风口，与此同时，裸贷、骗贷、高利贷、老赖、恶意套现、暴力催收等灰色生态持续曝光，不仅腐蚀互联网金融业态，而且逐步向农村地区渗透。传媒是一种注意力经济，也是流量经济。资本裹挟下的传媒业在流量狂欢下也催生出造数据、请水军、买热搜、控评论等暗流：企业通过热搜控评，消除负面舆情、制造虚假热度；热搜明码标价成为商品，经纪公司诱导粉丝为娱乐明星集资刷数据，助推数据造假。这些灰色生态游走在监管的边缘地带，扭曲了行业的社会信任，侵害了数字社会的公平。

2.3 政治介入风险：网络科技对政治传播的潜在影响

网络科技不仅影响了政治家的政治运作，也改变了公民思考和参与政治的方式，已经成为参与政治传播的重要角色。

(1) 利用社交机器人操控政治舆论。社交机器人指运营者借助算法技术，注册并运营大量虚拟账号，扮演人类发布生产内容，与真实用户和其他机器人产生互动。这种技术最早应用于商业营销，后来被政治团体用以完成政治诉求，操纵社会舆论^[11]。近年来，政治选举、政治干扰、社会动员乃至国际事件中利用社交机器人操纵舆论的事件频频被报道，在英国“脱欧”、美法总统选举、中美贸易战中，均发现有社交机器人操纵舆论的痕迹。研究者发现2016年美国总统大选中，社交机器人生产的推文在选举前几天占比为1/4，选举后发文比例显著减少^[12]。操纵者通过利用社交机器人，干预社交媒体上的信息传递，通过大规模转发以及发布重复内容形成意见气候，影响政治舆论生态。具体而言，其操纵策略主要分为两方面：①积极包装自身形象、制造虚假的人气，虚张声势扩大自身影响力；②制造虚假消息进行政治干扰，煽动舆论，抹黑对手。运用机器人算法进行舆论操控已形成一种“地下产业”，网络科技的智能化不免成为政治博弈的工具。

(2) 社交媒体提供动员社会抗争的平台。近年来，国内外涌现出基于社交媒体开展的新型政治运动，如“占领华尔街”“伦敦青年骚乱”等事件，从线上动员到线下行动，社交媒体成为动员、组织、参与社会抗争的新阵地。抗争者一方面通过社交媒体以文字、声音、图像、视频甚至直播的方式，全方位营造抗争舆论，及时更新事件动态及现场；另一方面，通过通信软件、社交媒体动员集会、游行，传播行动

④ 赖祐莹. 外卖骑手, 困在系统里. (2020-09-08)[2024-11-2]. <https://mp.weixin.qq.com/s/Mes1RqIOdp48CMw4pXTwXw>.

信息，动员更多人参与到线下行动。在政治抗争中不乏外国势力以隐蔽的方式制造负面舆论激发矛盾，如“茉莉花革命”“埃及暴乱”等^[13]。社交媒体极大促进了公民个人表达和政治参与度，也聚合了公众对现实、民生等问题的不满情绪，并将其转为街头政治、广场政治或舆论政治等不同形式的政治抗争，最终形成冲击原有的治理秩序的巨大力量^[14]。随着未来网络科技不断发展，公民的媒介接近权会不断提高，多元化、多渠道的政治表达不断涌现，增强了数字民主，但也暗含着“革命”的新风险，这为网络治理带来了增量，也带来无限变量。

3 防范化解网络科技社会风险的路径选择

在新形势下防范化解网络科技社会风险，需要从价值引领、制度规制、技术赋能、多元共治等方面发力，提供精准施策的工具箱，实现从被动应对转向主动防范。

3.1 价值引领：坚持“以人民为中心”的法则适配

网络科技利用大数据来预测用户行为，本质是用技术手段揣摩人心。而隐私侵犯、算法操控乃至平台霸权等则是网络科技在提升商业效率的同时，借助技术之手对人的中心地位的消解。习近平总书记提出“以人民为中心”的思想，强调要使人民获得感、幸福感和安全感更加充实、更有保障、更可持续，既是网络科技发展鲜活的价值引领法则，也是衡量科技向善的校准标尺。“以人民为中心”重视人的需要、强调人的潜能、尊重人的主体性。网络科技发展的未来，需要在强调提高生产力效率的同时不断破解适配问题：① 网络科技要响应人类需求，进行需求的适配；② 平衡经济价值和人性温度，进行价值的适配；③ 将科技向善理念落地为可操作的方案，实现发展的适配。

3.2 制度规制：构建分层递进的制度保障体系

(1) 保障数据主权。根据数据在经济社会发展中

的重要程度和危害程度实行分类分级保护制度。从公民层面，个人信息处理者需采取加密、去标识化等技术措施保障数据安全，确保敏感数据“上锁”、用户信息“脱敏”，按照“谁需要用数据，谁才看得到”的规则，搭配日志记录，并进行持续的数据安全审计。在应用层面，强化数据应用的安全性和合规性，在隐私保护计算框架下，实现数据的“可用不可见”；重点评估关键信息基础设施、核心数据、重要数据，防止大量个人信息被外国政府影响、控制、恶意利用。

(2) 压实平台责任。按照用户规模、业务种类和限制能力分为超级平台、大型平台、中小平台3级，实施差异化监管，建立全流程数据安全管理制度。例如，将日活跃用户超7亿的抖音平台纳入最高级监管，针对其青少年内容要采用多重审核机制，过滤不同形式的不良信息。

(3) 加强算法治理。① 明确算法透明义务，禁止利用算法实施价格歧视。② 强化对平台用工算法的规范与约束，防止系统将劳动者困于算法之中。保障劳动者的基本休息权与人格尊严，从源头化解因算法压榨所滋生的社会负面情绪。③ 对于生成式AI服务提供者，需备案算法模型，尤其针对提供具有舆论属性或社会动员能力的生成式AI服务，更应按规定开展安全评估和算法备案，保障训练数据合法性。

3.3 技术赋能：实现正向科技创新与反向风险预见

(1) 推动核心科技创新，进行正向引领。网络科技的发展要摆脱“流量复制”路径依赖，在创新商业模式的基础上，勇于承担科技创新的责任，聚焦“卡脖子”领域进行核心技术攻坚，建立“十年磨一剑”的长效机制。用科技创新推动互联网健康发展，延长企业价值链，扩大人类知识边界。

(2) 运用技术实现风险的模拟和预见，进行反向规制。建立关键信息基础设施安全保护制度，完善智能监管的基础设施，强化监测预警与应急处置能力；

建立数据安全风险评估机制,通过技术手段量化风险概率与影响因子;探索应急响应数字孪生,基于元宇宙技术构建虚拟社会实验场,对数据跨境流动、深度伪造等场景进行压力测试,用科技新发展来对抗未来的威胁。

3.4 社会协同:探索多主体适应性的治理模式

网络科技的健康发展需要积极探索适应性的治理模式。基于风险治理路径的“简单化”与法律治理需求“复杂化”存在矛盾^[15],要打破传统“一刀切”监管,注重制度设计的场景化和弹性化,丰富分级分类标准来进一步匹配场景化规制,发挥“底线防控型”和“守法激励型”政策工具相结合的作用效能。例如,2023年出台的《生成式人工智能服务管理暂行办法》,在确保安全和伦理的前提下,鼓励大模型创新和应用^[16],欧盟《人工智能法案》根据风险等级差异化约束算法应用。

与此同时,进一步探索多主体的协同共治方案。

① **政府主导**。制定底线规则,统筹协调关键信息基础设施的安全保护,监测、防御、处置网络安全风险和威胁,依法惩治网络违法犯罪活动。② **企业主责**。网络科技企业履行主体责任,优化生产要素市场化配置和商品服务流通的体制机制,提升智能社会产生的AI偏见、深度伪造、隐私泄露等应对能力。③ **社会补位**。发动社会力量分层次开展数字文明培育工程,针对不同群体特征进行精准施策。例如,将数字伦理纳入义务教育的必修课,针对银发群体开展“反网络欺诈”专项行动等。通过多方协同,构筑起网络科技安全发展的护城河。

4 结语

从一条64 K国际专线开启的信息革命,到如今万物互联的智能社会图景,网络科技在30年间深刻地重塑了社会结构和运行逻辑。文章揭示了网络科技发展带来福祉的同时,也伴生着结构性的社会风险:在

数据层面,过度采集、算法操控与隐私边界的消解挑战着个体尊严与社会信任;在资本层面,平台垄断、数字劳工的异化,以及灰色产业链的滋生扭曲了市场秩序与劳动价值;在政治层面,舆论操纵与社会动员的失序则对国家安全与政治稳定构成潜在威胁。面对社会风险的交织叠加,任何单一维度的应对都力有不逮。文章提出价值引领、制度规制、技术赋能与多元共治的主要路径,旨在从被动应对转向主动防范,以保障国家安全,推动科技强国建设。展望未来,唯有在发展与治理、创新与规范、效率与公平之间寻求动态平衡,才能将风险化解于未萌,真正让网络科技的发展造福于人民。

参考文献

- 1 方兴东,金皓清,钟祥铭.中国互联网30年:一种全球史的视角——基于布罗代尔“中时段”的“社会时间”视角.传媒观察,2022,(11):26-42.
Fang X D, Jin H Q, Zhong X M. Thirty year development of the Internet in China: A perspective of global history. Media Observer, 2022, (11): 26-42. (in Chinese)
- 2 乌尔里希·贝克.风险社会.何博闻,译.南京:译林出版社,2004.
Beck U. Risk Society. Translated by He B W. Nanjing: Yilin Press, 2004. (in Chinese)
- 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,2025-03-02(01).
Resolutely Implement the Holistic National Security Vision to Elevate the Construction of a Safe China to a Higher Level. People's Daily, 2025-03-02(01). (in Chinese)
- 4 喻国明,张超,李珊,等.“个人被激活”的时代:互联网逻辑下传播生态的重构——关于“互联网是一种高维媒介”观点的延伸探讨.现代传播(中国传媒大学学报),2015,37(5):1-4.
Yu G M, Zhang C, Li S, et al. The era of “individual activation”: The reconstruction of communication ecology under the logic of the Internet—An extended discussion on the viewpoint that “the Internet is a high-dimensional

- medium". *Modern Communication (Journal of Communication University of China)*, 2015, 37(5): 1-4. (in Chinese)
- 5 尼古拉·尼葛洛庞蒂. 数字化生存. 胡泳, 范海燕, 译. 海口: 海南出版社, 1997.
Negroponte N. *Being Digital*. Translated by Hu Y, Fan H Y. Haikou: Hainan Publishing House, 1997. (in Chinese)
 - 6 Pariser E. *The Filter Bubble: What the Internet is Hiding from You*. London: Penguin Press, 2011.
 - 7 米歇尔·福柯. 规训与惩罚: 监狱的诞生. 刘北成, 杨远婴, 译. 北京: 生活·读书·新知三联书店, 2003.
Foucault M. *Discipline and Punish: The Birth of the Prison*. Translated by Liu B C, Yang Y Y. Beijing: SDX Joint Publishing Company, 2003. (in Chinese)
 - 8 温德尔·瓦拉赫. 科技失控用科技思维重新看透未来. 萧黎黎, 译. 南京: 江苏凤凰文艺出版社, 2017.
Wallach W. *A Dangerous Master: How to Keep Technology from Slipping Beyond Our Control*. Translated by Xiao L L. Nanjing: Jiangsu Phoenix Literature and Art Publishing, 2017. (in Chinese)
 - 9 阿里尔·扎拉奇, 莫里斯·E. 斯图克. 算法的陷阱: 超级平台、算法垄断与场景欺骗. 余潇, 译. 北京: 中信出版社, 2018.
Ezrahi A, Stucke M E. *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy*. Translated by Yu X. Beijing: CITIC Publishing House, 2018. (in Chinese)
 - 10 姚建华. 媒介产业的数字劳工. 北京: 商务印书馆, 2017.
Yao J H. *Digital Labor in the Media Industry*. Beijing: The Commercial Press, 2017. (in Chinese)
 - 11 张洪忠, 段泽宁, 杨慧芸. 政治机器人在社交媒体空间的舆论干预分析. *新闻界*, 2019, (9): 17-25.
Zhang H Z, Duan Z N, Yang H Y. Analysis of public opinion intervention by political bots in social media space. *Journalism Circle*, 2019, (9): 17-25. (in Chinese)
 - 12 师文, 陈昌凤. 分布与互动模式: 社交机器人操纵 Twitter 上的中国议题研究. *国际新闻界*, 2020, 42(5): 61-80.
Shi W, Chen C F. Distribution and interaction patterns: How social bots manipulate the Chinese-related issues on Twitter. *Chinese Journal of Journalism & Communication*, 2020, 42(5): 61-80. (in Chinese)
 - 13 韩娜. 社交媒体对政治传播影响的研究——基于批判的视角. *新闻记者*, 2015, (8): 81-86.
Han N. A study on the impact of social media on political communication: From a critical perspective. *Journalist*, 2015, (8): 81-86. (in Chinese)
 - 14 刘文富. 网络政治. 北京: 商务印书馆, 2002.
Liu W F. *Cyber Politics*. Beijing: The Commercial Press, 2002. (in Chinese)
 - 15 张凌寒. 人工智能法律治理的路径拓展. *中国社会科学*, 2025, (1): 91-110.
Zhang L H. Expanding the legal governance path of artificial intelligence. *Social Sciences in China*, 2025, (1): 91-110. (in Chinese)
 - 16 施锦诚, 王国豫, 王迎春. ESG 视角下人工智能大模型风险识别与治理模型. *中国科学院院刊*, 2024, 39(11): 1845-1859.
Shi J C, Wang G Y, Wang Y C. Artificial intelligence foundation model risk identification and governance model from the ESG perspective. *Bulletin of Chinese Academy of Sciences*, 2024, 39(11): 1845-1859. (in Chinese)

Three decades of Chinese Internet technology: Social risks and prevention pathways

YIN Zhaokai¹ ZHANG Weifu^{2*}

(1 School of Information Management, Nanjing University, Nanjing 210023, China;

2 School of International Economics and Business, Nanjing University of Finance and Economics, Nanjing 210023, China)

Abstract With the rapid advancement and application of big data, artificial intelligence, and mobile Internet technologies, network technology has been driving social development, while its negative effects have gradually emerged. Based on a critical perspective and logical reasoning, this study systematically reviews the evolution and characteristic manifestations of social risks in China's network technology over the past 30 years, revealing multiple hidden dangers it has caused in data governance, capital operation, and political communication. Under the new situation, to prevent and defuse the social risks of network technology, precise measures should be taken from aspects such as value guidance, institutional regulation, technological empowerment, and multi-party governance, shifting from passive response to proactive prevention, so as to build a solid national security barrier, promote the construction of a technological power, and enable the development of network technology to better benefit the people.

Keywords Internet technology, social risks, artificial intelligence, national security, science and technology powerhouse

尹召凯 南京大学信息管理学院助理研究员。主要研究方向为:媒介效果、数字出版、全民阅读。
E-mail: yzk@nju.edu.cn

YIN Zhaokai Assistant Researcher at the School of Information Management, Nanjing University, with a Doctorate in management. His main research focuses on media effects, digital publishing, and national reading. E-mail: yzk@nju.edu.cn

张为付 南京财经大学国际经贸学院教授,江苏现代服务业智库首席专家。主要研究方向为:服务经济、开放经济。
E-mail: cwf-01@163.com

ZHANG Weifu Professor at the School of International Economics and Business, Nanjing University of Finance and Economics, Doctoral Supervisor, and Chief Expert of the Jiangsu Modern Service Industry Think Tank. His main research focuses on the service economy and the open economy. E-mail: cwf-01@163.com

■责任编辑: 文彦杰

*Corresponding author