网络信息传播安全与管理研究

陈　喆
天津市教育委员会教育综合服务中心　天津　300060

摘　要：在数字化时代网络信息传播日益重要的当下，本文聚焦网络信息传播安全与管理，从基础理论出发，剖析技术、内容、社会层的安全威胁，阐述技术防护、内容审核、用户行为管理等核心机制，提出强化平台责任、跨平台协作、公众参与等协同治理策略。旨在通过多维度研究，构建网络信息传播安全管理体系，为应对复杂安全挑战提供理论支撑与实践指导，促进网络信息传播健康、有序发展。

关键词：网络信息传播安全；安全威胁；管理机制；协同治理

引言：在数字化时代，网络信息传播迅猛发展，深刻改变社会生活。然而，伴随而来的安全问题日益凸显，虚假信息泛滥、数据泄露、网络攻击等威胁着个人权益、社会稳定与国际关系。传播学、信息安全、管理学等多学科视角为研究网络信息传播安全提供理论基础。深入剖析安全威胁与管理机制，探索协同治理策略，对保障网络信息传播安全、营造良好网络生态具有重要的现实意义。

1 网络信息传播安全的基础理论

1.1 传播学视角下的安全逻辑

从传播学视角审视，网络信息传播安全根植于信息流动的内在规律。信息传播的双向性特征打破了传统单向传播模式，用户既是信息接收者也是传播者，这种角色叠加使风险扩散路径呈现网状结构[1]。一条虚假信息可能经由多次转发形成传播链，每个节点都可能成为风险放大器。传播主体多元化是网络信息传播的显著特征，也是安全挑战加剧的重要因素。个人、机构、自媒体以及算法程序等共同参与信息生产与分发，它们在安全意识、技术能力和利益诉求上存在巨大差异。这种差异使得安全漏洞难以统一防控，不同主体可能因各自问题引发不同类型的安全风险。例如，普通用户可能因缺乏安全意识而随意转发未核实信息，专业机构则可能因技术疏忽导致数据泄露，形成多层次风险叠加效应。

1.2 信息安全理论的应用

信息安全理论为网络传播安全提供了核心框架。保密性、完整性与可用性构成安全三角：保密性要求防止敏感信息泄露，完整性确保信息未被篡改，可用性保障服务持续稳定运行。这一框架在动态网络环境中面临持续挑战，攻击手段不断进化，从简单数据窃取升级为系统性破坏。动态安全模型的出现是对这些挑战的有力回应。它通过持续监测、实时响应与自适应调整，构建“检测-防御-恢复”的闭环体系，能够及时发现并应对不断变化的安全威胁。例如，零信任架构摒弃传统边界防护思维，默认不信任任何内部或外部请求，通过多因素认证与持续验证降低横向攻击风险，这种模型与网络传播的开放性特征形成有效互补。

1.3 管理学视角的治理范式

管理学理论为网络传播安全治理提供方法论支撑。风险管理理论强调对潜在威胁的识别、评估与控制，通过建立风险矩阵与优先级排序，实现资源精准投放。危机应对理论则聚焦突发事件处置，要求制定应急预案、开展模拟演练，提升系统韧性。协同治理机制是管理学在网络传播安全治理中的重要应用。它突破单一主体局限，构建政府、平台、用户与第三方机构共同参与的治理网络。政府通过制定规则与监督执行维护秩序，平台利用技术优势实施内容审核与风险拦截，用户提升安全意识与媒介素养，第三方机构提供专业评估与技术支持，各方优势互补，形成“技术-管理-社会”三位一体的治理生态。这种多主体参与模式既避免权力过度集中，又通过责任共担提升整体安全效能。

2 网络信息传播的安全威胁分析

2.1 技术层威胁

技术层威胁犹如隐匿于数字世界的幽灵，时刻窥伺着信息安全防线[2]。数据泄露与隐私侵犯问题尤为突出，部分企业因安全防护机制薄弱，导致用户注册信息、消费记录等敏感数据被非法获取，这些数据在黑市流转后，可能被用于精准诈骗或身份盗用。隐私侵犯则体现在过度收集行为上，某些应用在用户未充分知情时，持续追踪设备定位、通讯录等隐私信息，甚至通过跨平台数据拼接形成完整用户画像，严重侵犯个人空间。网络攻击手段的多样性和复杂性是技术层威胁的显著特点。黑客利用系统漏洞发起拒绝服务攻击，导致服务瘫痪，或通过

植入木马程序控制用户设备，窃取内部数据。系统脆弱性也是不容忽视的问题，部分老旧系统因缺乏维护，成为攻击者突破防线的突破口，一旦被攻破，可能引发连锁反应，波及整个网络生态，对网络信息传播安全造成严重破坏。

2.2 内容层威胁

内容层威胁如同信息洪流中的暗礁，稍有不慎便可能触礁搁浅。在信息爆炸的时代，虚假信息与误导性内容借助社交媒体快速扩散，其传播速度远超事实核查能力，往往在澄清前已造成广泛影响。这类内容往往迎合部分受众的心理需求，以吸引眼球为目的，或夸大事实，或捏造谣言，甚至伪造权威信源，干扰公众认知，破坏社会信任基础。一旦公众对信息真实性产生怀疑，将影响整个社会的信息交流和决策制定。恶意软件与代码植入是内容层威胁的另一种表现形式，具有极强的隐蔽性和危害性。攻击者将恶意程序伪装成正常文件，通过邮件附件、下载链接等方式传播，用户一旦点击，设备便可能被远程控制，成为攻击其他系统的跳板。部分恶意软件还会加密用户文件，索要赎金，造成直接经济损失，严重影响网络信息传播的正常秩序和用户的合法权益。而且随着技术的不断进步，恶意软件的变种越来越多，防范难度日益增大。

2.3 社会层威胁

社会层威胁源于信息传播与社会环境的复杂互动。群体极化现象在网络空间尤为显著，相同观点的群体在封闭环境中不断强化极端立场，最终可能演变为非理性行为，如网络暴力或线下冲突。网络空间的匿名性和虚拟性使得部分用户容易放下道德约束，肆意发表攻击性言论，相同观点的群体在封闭环境中不断强化极端立场，加剧了群体极化现象。舆论失控则表现为信息传播脱离原有轨道，被少数利益群体操纵，形成虚假民意，影响公共决策。跨国传播中的文化冲突是社会层威胁的新表现。不同文化背景的用户对同一信息可能产生截然相反的理解，若缺乏有效沟通机制，容易引发误解与对立，甚至升级为文化层面的冲突，阻碍全球信息共享与文化交流。社会层威胁不仅影响网络信息传播的安全性，还对社会稳定和国际关系产生深远影响。

3 网络信息传播安全管理的核心机制

3.1 技术防护机制

技术防护是网络信息传播安全的第一道屏障，其核心在于通过技术手段构建主动防御体系。加密技术与访问控制构成基础防护层，加密技术通过算法将敏感信息转化为密文，确保数据在传输与存储过程中不被窃取或篡改。例如，端到端加密技术让信息仅在发送方与接收方设备解密，即使中间节点被截获也无法获取内容[3]。访问控制则通过身份认证、权限分级等手段，限制用户对资源的访问范围，防止未授权操作。区块链技术为技术防护带来了新的思路和方法。其分布式账本与时间戳特性，让每条信息从生成到传播的轨迹都可追溯、不可篡改。在新闻传播领域，区块链可记录文章创作、编辑、发布的全过程，有效打击虚假信息与抄袭行为；在供应链管理中，区块链能追踪商品从生产到流通的每个环节，确保信息真实可信，为网络信息传播安全提供了有力的技术支持。

3.2 内容审核机制

内容审核是维护网络传播秩序的关键环节，需兼顾效率与准确性。自动化审核与人工干预的结合模式成为主流，自动化审核利用自然语言处理、图像识别等技术，快速筛查违规内容。例如，通过关键词过滤、语义分析识别涉黄涉暴信息，利用深度学习模型检测虚假新闻的文本特征。然而，算法存在局限性，对隐喻、谐音等变体内容的识别能力有限，此时需人工介入进行复核。多维度内容分类与风险评级进一步提升了内容审核的精细化水平。根据内容主题、传播范围、影响程度等维度划分等级，对高风险内容采取更严格的审核标准。例如，涉及公共安全的信息需经多重人工审核，而普通生活分享类内容可简化流程。这种分级机制既保障了审核效率，又避免了“一刀切”式管理，让合规内容得以顺畅传播，维护了网络信息传播的多样性和活力。

3.3 用户行为管理机制

用户行为管理是网络传播安全治理的长期任务，需从身份认证与信用体系构建入手。身份认证通过手机号绑定、实名认证等手段，确保用户身份真实可信，减少匿名传播带来的风险。信用体系则通过记录用户行为数据，形成动态信用评分，对违规用户采取限制功能、降低曝光等措施。例如，频繁发布虚假信息的用户会被标记为低信用，其内容推荐权重降低；积极参与辟谣、举报违规行为的用户则获得信用加分，享受更多平台权益。社交关系网络的动态监测也是用户行为管理的重要手段。通过分析用户关注、互动等行为，识别异常账号与潜在风险群体。例如，短时间内大量关注陌生账号、频繁发送私信骚扰等行为，可能预示着营销号或诈骗账号，系统可自动触发预警并采取干预措施。这种以用户为中心的管理模式，既尊重了传播自由，又通过信用约束引导用户规范行为，形成良性传播生态。

4 网络信息传播的协同治理策略

4.1 平台主体责任强化

内部治理架构优化需立足平台运营全流程，搭建分层分类的管理体系。结合信息传播特点与风险点，明确各部门岗位职责边界，打破部门间信息壁垒，实现从内容审核、风险研判到问题整改的闭环管理[4]。同时依托技术赋能，升级治理工具迭代，让治理架构与平台业务规模、用户体量动态适配，避免治理滞后于传播节奏。算法透明化与责任追溯是平台履职的核心抓手。平台需以通俗化方式向公众披露算法基本原理、运行逻辑及数据来源，避免算法黑箱引发信息偏差。建立全流程算法运行日志留存机制，对算法推荐导致的不良信息传播问题，精准定位责任环节与具体责任人，确保每一项算法决策都可回溯、可核查，筑牢算法应用的责任底线，保障用户合法权益和网络信息传播的公平公正。

4.2 跨平台协作机制

信息传播的跨平台特性要求治理从“单打独斗”转向“联防联控”。信息共享与联合处置需打破数据壁垒，建立标准化信息交换协议。例如，针对网络诈骗信息，各平台可共享涉案账号、诈骗话术等数据，通过机器学习模型实时识别跨平台诈骗链条，实现“一处发现、全网拦截”。应急响应协同网络构建则聚焦突发事件处置，通过签订合作协议、开展联合演练等方式，提升跨平台协作效率。例如，面对重大舆情事件，主流媒体平台可与商业平台建立快速沟通渠道，统一信息发布口径，避免谣言滋生；面对技术攻击事件，云服务提供商可与安全企业共享威胁情报，协同启动防护措施，缩短系统恢复时间。这种协作模式既避免了重复建设，又通过资源整合提升了整体治理效能，有效应对跨平台传播带来的安全挑战。

4.3 公众参与与教育引导

公众是信息传播的最终参与者，其安全意识与行为习惯直接影响治理效果。媒介素养提升路径需结合不同群体特征设计差异化方案，针对青少年群体，可通过学校课程、互动游戏等方式，培养其信息甄别与批判思维能力；针对老年群体，可利用社区讲座、短视频教程等形式，普及防诈骗知识与平台使用技巧。社会监督与反馈渠道设计则需畅通公众参与路径，通过设立举报奖励机制、开发便捷举报工具等方式，激发公众监督热情。例如，某短视频平台推出“一键举报”功能，用户可快速标记违规内容，系统自动分类并推送至审核团队，举报属实者获得积分奖励，可用于兑换平台权益[5]。同时建立公众意见反馈闭环，定期分析举报数据与用户建议，将高频问题纳入治理策略优化方向，形成“治理-反馈-再治理”的良性循环。这种以公众为中心的治理模式，既提升了治理的精准度，又通过共建共享增强了社会认同感。

结束语

网络信息传播安全与管理是复杂且长期的课题。面对不断变化的安全威胁，需综合运用多种机制与策略。强化技术防护，完善内容审核，规范用户行为，同时加强平台责任落实、跨平台协作以及公众参与引导。多方协同发力，构建全方位、多层次的治理体系，才能有效应对挑战，保障网络信息传播安全、稳定、有序，推动网络空间健康发展，更好地服务于社会进步与人类福祉。

参考文献

[1]陶冶.电力自动化控制系统网络信息安全管理研究[J].电工技术,2024(S2):396-398.

[2]蒋忠均,荀泽涛.物联网环境下网络信息传播安全控制技术研究[J].通讯世界,2024,31(6):64-66.

[3]锁文露,赵晓露.大数据背景下高校网络信息传播安全问题研究[J].西部广播电视,2024,45(6):94-97.

[4]张宁宇.全媒体时代吉林省高校网络信息传播与舆论引导研究[J].E动时尚,2024(6):10-12.

[5]佟璐.新媒体对网络信息传播的影响与应对策略分析[J].E动时尚,2025(8):25-27.