新媒体助力网络安全和信息化建设的策略研究

苗 森
新疆维吾尔自治区战略和应急物资保障服务中心（乌鲁木齐中央级救灾物资储备库） 新疆 乌鲁木齐 830000

摘 要：本文深入探讨了新媒体在赋能网络安全和信息化建设中的双重角色：一方面，作为高效的宣传与教育平台，新媒体能够将抽象、专业的网络安全知识转化为通俗易懂、喜闻乐见的内容，实现全民数字素养与安全意识的精准滴灌；另一方面，作为重要的舆情监测与引导阵地，新媒体为及时发现网络风险、澄清谣言、维护清朗网络空间提供了强大的感知与响应能力。在此基础上，论文系统性地构建了一套涵盖内容生产、渠道协同、互动反馈、机制保障四个维度的策略体系，并前瞻性地提出了应对新媒体自身安全风险、实现“善用”与“善管”并重的发展路径。研究表明，科学、有效地运用新媒体，是打通网络安全“最后一公里”、激发全民共建共治共享网络空间内生动力的战略选择。

关键词：新媒体；网络安全；信息化建设；数字素养；舆情引导

引言

当前，社交媒体、短视频、直播等新媒体已深度重构信息生产、传播与消费模式，成为社会信息生态的主导力量和公共话语的核心场域。在此背景下，国家网络安全与信息化建设面临新机遇与挑战：一方面，信息化加速拓展了网络空间安全边界，从关键基础设施到个人终端均需防护，亟需构建全民安全意识防线；另一方面，虚假信息、网络谣言和恶意攻击借新媒体裂变式传播，易引发社会恐慌与信任危机。因此，如何将新媒体从潜在风险“放大器”转化为普及安全知识、培育健康网络文化、提升网络治理能力的“助推器”，成为关键课题。本文立足国家战略高度，超越表象观察，系统研究新媒体赋能网络安全与信息化建设的有效路径与策略。

1 新媒体赋能网络安全与信息化建设的独特价值

1.1 打破专业壁垒，实现安全知识的大众化普及

传统的网络安全宣教往往局限于技术圈层，其内容充斥着防火墙、加密算法、漏洞利用等专业术语，对于普通公众而言晦涩难懂，难以产生共鸣。新媒体则以其强大的内容转化能力，能够将这些高深的专业知识进行“翻译”和“包装”。通过制作生动有趣的科普短视频、设计寓教于乐的互动H5小游戏、创作引人入胜的漫画或情景剧，可以将复杂的钓鱼邮件识别技巧、密码设置原则、隐私保护方法等核心安全知识，以故事化、场景化、可视化的方式呈现出来。这种“润物细无声”的传播方式，极大地降低了公众的理解门槛，使网络安全从一个遥不可及的技术话题，转变为与每个人日常生活息息相关的必备常识，从而有效提升了全民的数字素养和风险防范能力。

1.2 构建全域覆盖的立体化传播矩阵

新媒体的传播渠道呈现出多元化、碎片化、移动化的特征。从微博、微信的社交关系链，到抖音、快手的算法推荐流，再到B站、小红书的兴趣社群，不同平台聚集了不同年龄、职业、兴趣的用户群体。这种去中心化的传播格局，为网络安全宣教提供了前所未有的覆盖广度和渗透精度。官方机构可以不再依赖单一的、单向的广播模式，而是根据不同平台的用户画像和内容生态，定制差异化、精准化的传播策略[1]。例如，在面向青少年的平台上，可侧重游戏安全、网络欺凌防范等内容；在面向中老年用户的社群中，则可重点普及电信诈骗识别、健康信息甄别等知识。通过构建这样一个全域联动、精准触达的立体化传播矩阵，能够确保安全信息有效抵达社会的各个角落，不留死角。

1.3 强化双向互动，激发公众的参与式治理

新媒体最革命性的特征在于其强大的交互性。它打破了传统媒体时代“传者-受者”的单向关系，赋予了每个用户发声、评论、分享和创作的权利。这一特性为网络安全治理带来了范式转变。官方机构可以通过新媒体平台发起话题讨论、在线问答、有奖征集等活动，鼓励公众主动分享自己的防骗经验、举报可疑线索、提出安全建议。这种双向甚至多向的互动，不仅能够收集到大量来自一线的真实反馈，为政策制定和风险预警提供宝贵的一手资料，更重要的是，它能将公众从被动的信息接收者，转变为积极的网络空间共建者。当每个人都意识到自己在网络空间安全中扮演着不可或缺的角色时，一种自下而上的、基于社区自治的网络安全文化便得以

形成，这正是构建网络空间命运共同体的社会基础。

1.4 提升舆情感知与引导的敏捷性

网络空间是现实社会的镜像，也是各种矛盾和风险的“晴雨表”。新媒体平台因其海量的用户生成内容（UGC），天然构成了一个巨大的社会情绪传感器。通过对社交媒体上的话题热度、情感倾向、关键词聚类等进行实时监测与分析，可以敏锐地捕捉到潜在的网络安全事件苗头，如新型病毒爆发的早期迹象、针对特定群体的网络谣言扩散、或是大规模数据泄露事件的民间传闻。这种基于大数据的舆情感知能力，为相关部门提供了宝贵的预警时间窗口。同时，一旦发生安全事件或谣言传播，官方机构可以迅速通过新媒体平台发布权威信息，以透明、坦诚的态度进行辟谣和解释，利用新媒体的快速传播力抢占舆论制高点，有效压缩虚假信息的生存空间，稳定社会情绪，维护网络空间的秩序与稳定。

2 新媒体助力下的核心策略体系构建

2.1 内容策略：打造高质量、分众化、全周期的安全知识产品矩阵

2.1.1 专业化内核与通俗化外壳的深度融合

内容创作必须坚守专业底线。应建立由网络安全专家、心理学家、教育学家和资深新媒体编辑组成的“内容智囊团”。专家负责确保知识的准确性与时效性；心理学家和教育学家则指导如何根据认知规律设计学习路径；新媒体编辑则负责将其转化为符合平台调性的语言和形式。例如，在解释“零信任安全架构”这一前沿理念时，可以将其比喻为进入一个高度戒备的军事基地，无论你是谁，每次进入新区域都需要重新验证身份，从而让抽象概念变得具体可感。

2.1.2 精细化的用户画像与场景化内容定制

摒弃“一刀切”的宣教模式，转向基于大数据的精准推送。通过分析不同平台用户的年龄、地域、职业、兴趣等标签，构建多维度的用户画像[2]。针对学生群体，可开发以校园贷、游戏账号安全、网络交友陷阱为主题的系列短剧；针对企业高管，则可制作关于商业间谍、供应链攻击、数据合规风险的深度解读视频；针对老年群体，重点聚焦于假冒公检法、保健品诈骗、养老金账户安全等高频风险点，并采用大字幕、慢语速、重复强调等适老化设计。

2.1.3 构建覆盖“认知-技能-习惯”全周期的内容生态

安全意识的培养是一个循序渐进的过程。内容规划应覆盖从初步认知到行为养成的完整链条。初期以激发兴趣、建立基本概念为主（如“什么是个人信息？”）；中期侧重于教授具体防护技能（如“五步教你识别钓鱼网站”）；后期则致力于引导形成安全习惯和批判性思维（如“为何要定期更新软件？”、“如何理性看待网络热点事件？”）。通过系列化、阶梯式的内容输出，引导用户实现从“知道”到“做到”再到“习惯”的转变。

2.2 渠道策略：构建全域联动、优势互补、线上线下融合的立体化传播网络

2.2.1“中央厨房”式的内容分发与矩阵化运营

建立统一的“网络安全新媒体内容中央厨房”，负责核心内容的策划与生产。在此基础上，根据不同平台的特性进行二次加工和分发。在微博上，侧重发布权威快讯、辟谣信息和话题互动；在微信公众号，则深耕长图文、政策解读和深度案例分析；在抖音、快手等短视频平台，主打轻量化、趣味化的科普短视频；在B站，则可尝试更硬核的、带有技术演示性质的中长视频。各平台账号相互导流，形成一个内部协同、外部联动的强大传播矩阵。

2.2.2 激活“关键意见领袖（KOL）”与“关键意见消费者（KOC）”的杠杆效应

除了官方发声，还应积极与各领域的网络达人合作。邀请科技、财经、教育、生活等垂类的KOL，以其专业背景和个人魅力为安全知识背书，能极大提升内容的可信度和接受度。同时，鼓励普通用户（KOC）分享自己的真实经历和防骗心得，这种“身边人讲身边事”的UGC内容，往往具有更强的感染力和说服力，能够有效打破圈层壁垒。

2.2.3 深化O2O（Online to Offline）融合，打通虚拟与现实

线上宣传的最终目的是引导线下安全行为。可以在线上发起“家庭网络安全体检”挑战，鼓励用户按照指南检查自家路由器设置、智能设备权限等，并在线下社区服务中心设立咨询点，提供免费的技术支持[3]。在“国家网络安全宣传周”等重要节点，线上直播主会场活动，同时在全国各地同步开展线下展览、讲座和体验活动，形成全国一盘棋的浓厚氛围。

2.3 互动策略：建立常态化、制度化、数据驱动的双向沟通与共治机制

2.3.1 打造便捷、高效的公众参与入口

在所有官方新媒体平台的主页显著位置，设置标准化的“安全咨询”与“线索举报”功能模块。后台应配备专业的客服团队或AI智能助手，对常见问题进行即时解答，并对有价值的举报线索进行快速流转和处置。让用户感受到“说了有用”，是激发其持续参与意愿的前提。

2.3.2 创新互动形式，激发用户创造潜能

超越简单的点赞评论，设计更具参与感的互动玩法。例如，举办“网络安全创意大赛”，征集防范电信诈骗的宣传标语、海报或短视频；开发“网络安全闯关”小游戏，用户在游戏中学习知识、赢取奖励；开设“安全议事厅”直播栏目，邀请专家、官员与网民就热点安全议题进行实时对话。这些活动不仅能产出大量优质UGC内容，更能将用户深度绑定到安全共同体之中。

2.3.3 构建数据闭环，实现策略的动态优化

充分利用新媒体平台提供的强大数据分析能力。不仅要关注阅读量、转发量等表层指标，更要深入分析用户的完播率、互动深度、跳出点、情感倾向等深层数据。通过A/B测试对比不同内容版本的效果，利用聚类分析发现不同用户群体的兴趣偏好[4]。这些数据洞察应被系统性地反馈到内容策划、渠道选择和互动设计的决策流程中，形成“实践-反馈-优化”的敏捷迭代闭环。

2.4 保障策略：完善跨部门协同、复合型人才培育与全流程风险管理机制

2.4.1 建立跨层级、跨部门的协同指挥体系

网络安全宣教是一项系统工程，涉及网信、公安、教育、工信、金融等多个部门。应由中央网信办牵头，建立常态化的联席会议机制，统筹规划年度主题、核心信息和重大活动，避免政出多门、资源浪费。同时，推动省、市、县各级建立对应的协调机构，确保国家战略在基层得到有效执行。

2.4.2 大力培育“T型”复合人才队伍

当前最紧缺的是既精通网络安全专业知识，又深谙新媒体传播规律的“T型”人才。一方面，要加强对现有网信干部队伍的新媒体技能培训；另一方面，要与高校、研究机构合作，开设交叉学科课程，定向培养后备力量。此外，可设立专项基金，支持优秀的网络安全自媒体创作者，将其纳入官方宣传体系，形成专兼结合的人才格局。

2.4.3 健全全流程的内容安全与舆情应急机制

新媒体是一把双刃剑，其自身也面临被滥用的风险。必须建立覆盖内容策划、生产、审核、发布、监测、评估全生命周期的安全管理规范。特别是要制定详尽的《新媒体舆情应急预案》，明确在遭遇重大网络安全事件、谣言大规模传播等突发情况时，各平台账号的响应流程、信息发布口径、协同联动方式和效果评估标准，确保能够在关键时刻迅速、有力、准确地引导舆论，稳定社会预期。

3 应对挑战：确保新媒体自身的安全与健康发展

在利用新媒体赋能网络安全的同时，必须重视其自身作为网络攻击与信息操纵载体的风险，坚持“善用”与“善管”并重。一是强化平台安全防护，对官方账号实施强密码、多因素认证及定期审计，严防盗用；二是优化算法机制，在提升传播效率的同时引入内容多样性，打破“信息茧房”，促进公众全面认知；三是建立快速联动响应机制，实现涉网安谣言的及时发现、核实、辟谣与处置，并加强媒介素养教育，提升公众信息甄别能力；四是平衡开放与监管，在保障言论自由和公众参与的前提下，依法治理网络暴力、隐私侵犯及违法不良信息，坚守法律与道德底线，维护清朗网络空间。

4 结语

新媒体凭借其强大传播力、连接力与动员力，为弥合网络安全与信息化建设中的“知行鸿沟”带来历史性机遇，既是安全知识的“扩音器”，也是凝聚共识、激发参与、提升治理效能的“连接器”与“催化剂”。本文提出的以内容、渠道、互动、保障为核心的策略体系，旨在为政府、企事业单位及社会组织提供系统性行动指南。面向未来，随着元宇宙、AIGC等新技术推动新媒体持续演进，我们须以开放心态拥抱变革，以审慎态度防范风险，坚持“以人民为中心”的发展思想，将新媒体打造为守护国家网络安全、驱动信息化高质量发展的强大引擎，助力构建天朗气清、生态良好的网络空间，共创安全、便捷、美好的数字未来。

参考文献

[1]明海英.新媒体语言研究助力网络生态建设[N].中国社会科学报,2023-11-22(002).

[2]段永亮,陈兆月,郭红.新媒体环境下网络舆情治理机制与公众参与研究[J].合作经济与科技,2026,(07):120-122.

[3]职铭琦,张可.新媒体时代网络文化安全的现实挑战[N].山西科技报,2026-02-09(B05).

[4]殷俊,袁菲.基于大数据的融媒体网络安全监测与预警机制研究[J].西部广播电视,2025,46(08):175-178.