ISSN：3080-2660
EISSN：3080-2679

内蒙古网络安全治理现状、困境及优化路径研究

刘彩虹[1*] 王伟伟[2]

1. 内蒙古自治区社会科学院，内蒙古 呼和浩特 010010

2. 内蒙古电力（集团）有限责任公司培训中心，内蒙古 呼和浩特 010020

摘 要：随着数字经济发展与网络空间治理需求持续提升，内蒙古已搭建起涵盖日常防护、风险处置、责任追究的网络安全制度体系，政务、能源等重点领域防护能力与宣传普及工作稳步推进。当前基层网络安全硬件与人员配置存在短板，跨部门权责划分与信息共享机制存在疏漏，群众用网安全意识存在不足。需从基层基础设施补短板、跨部门协同机制优化、全民安全素养培育层面同步发力，提升区域网络安全治理整体效能。

关键词：内蒙古；网络安全治理；协同治理

DOI：10.64649/yh.jydk.issn3080-2660.202609048

0 引言

网络安全是总体国家安全观在区域治理场景中的重要落地内容，是保障区域数字经济稳步发展、维护社会大局稳定的核心支撑性工作。内蒙古作为北部边疆的重要民族省份，数字技术向政务服务、能源生产、民生保障等领域的渗透程度持续加深，网络空间治理场景的复杂度与治理难度也随之提升。当前针对内蒙古网络安全治理的本土化适配研究仍存在一定缺口，结合内蒙古治理实际梳理现存困境、提出针对性优化路径，一方面可补齐区域网络安全治理的现存短板，为各项数字业务的稳定运行提供安全保障，另一方面也可为其他同类型地区的网络安全治理工作提供可借鉴的实践参考，助力国家网络空间治理体系的完善。

1 内蒙古网络安全治理的现实基础与发展现状

结合自治区数字经济发展与网络空间治理的实际需求，内蒙古网络安全治理工作已搭建起较为扎实的落地框架。相关治理主体把国家层面的网络安全顶层设计作为落地依据，逐步搭建起涵盖日常防护、风险处置、责任追究的地方网络安全制度体系，各项工作的开展都契合国家整体网络安全治理的方向要求。相关领域的网络安全保障工作逐步推进，政务服务平台的安全防护配置持续完善，能源、交通等关键行业的日常网络安全巡检工作常态化开展，通信行业的基础网络防护能力也得到稳步提升[1]。网络安全宣传工作面向城乡不同群体，常态化的网络风险监测机制已经落地，网络安全事件的应急处置流程逐步理顺，关键信息基础设施的分级保护工作也按既定节奏有序推进，可以为后续网络安全治理工作的深化开展提供较为稳固的现实支撑[2]。

2 内蒙古网络安全治理面临的核心困境

2.1 基层网络安全防护能力不足

基层网络安全防护能力的短板会直接影响全区网络安全治理效能的下沉覆盖。基层单位把网络设备的更新优先级放在业务运行保障之后，更新周期较长，系统防护的配置多停留在基础病毒查杀层面，数据安全的全流程管理工作没有得到完全落地。借助对基层岗位设置的实际梳理，从事网络安全相关的专职岗位占比极低，在岗人员多数没有接受过系统的专业技能培训，外部技术支撑力量的下沉覆盖也存在明显盲区。从日常运维的实际场景来看，风险监测的手段较为单一，很难第一时间发现隐蔽性较强的网络风险，应急处置的流程没有结合基层运维的实际条件进行细化，常态化的应急演练工作也没有在全部基层单位有序推开，潜在的网络安全风险很难得到提前排查与快速化解[3]。

2.2 跨部门协同治理机制不畅

跨部门协同的运行效率能直接影响全区网络安全治理的整体成效。相关治理部门在权责划分的过程中，还存在职责衔接不够清晰的问题，多个主体参与同类网络安全治理工作时，权责边界以及任务分工存在交叉或者空白，部分重叠领域的工作容易出现重复推进或者责任推诿的情况，边缘性的治理任务也难找到明确的负责主体。从信息流转的实际运行状态来看，部门间的信息共享渠道不够顺畅，网络安全风险信息、事件线索以及监测数据在不同部门之间的流转不够充分，不同主体掌握的相关信息难以及时同步，也无法为治理工作的开展提供完整的信息支撑。对应到具体事件的处置环节，跨部门联合处置机制不够完善，会商研判、联动执法以及协同应急等环节的工作流程没有进行细化统一，不同部门的处置节奏难以适配，

ISSN：3080-2660
EISSN：3080-2679

遇到跨领域的网络安全事件时很难快速形成有效的治理合力[4]。

2.3 公众网络安全意识薄弱

群众网络安全意识的薄弱会直接拉低全区网络安全治理的整体社会支撑水平。很多群众习惯把不同平台账号设置为相同的简单密码，在使用各类线上服务时随意开放通讯录、定位等隐私权限，也没有主动开展个人敏感数据加密存储的意识。进一步观察发现，很多群众无法准确辨别异常的中奖信息、冒充公职人员的诈骗话术，碰到来源不明的网络链接、仿冒的政务服务类网站也没有核验资质的习惯，看到未经证实的社会热点信息时容易随意转发扩散。结合网络安全治理的社会参与需求来看，多数群众碰到网络安全隐患时没有主动向相关监管部门举报的习惯，也很少主动向身边亲友传播官方发布的网络风险提示内容，碰到网络上的不文明言行时也大多采取旁观态度，不会主动参与网络空间秩序的维护工作[5]。

3 内蒙古网络安全治理的优化路径

3.1 完善基层网络安全基础设施支撑体系

相关治理主体把基层网络安全基础设施的补短板工作作为治理效能下沉的核心抓手，把基层网络安全防护设备的更新纳入年度运维经费的固定列支范畴，逐步完成防火墙、入侵检测、终端防护、日志审计等基础防护设施的迭代配置，将设备更新的优先级和业务运行保障的需求做统筹适配，缩短老旧设备的更新周期，完善基础防护层面的硬件短板，让基层网络防护的基础配置不再停留在简单病毒查杀的层面。针对基层数据安全管理缺乏统一载体的问题，推进覆盖基层的统一数据安全管理平台搭建工作，开展数据分类分级、访问控制、备份恢复、风险监测等全流程的管理功能落地工作，对基层日常产生的各类民生类、政务类数据开展规范化的全生命周期管理，明确不同岗位人员的数据调取权限，定期完成重要数据的异地备份，实现常态化的数据安全风险自动识别预警，补足数据安全全流程管理的落地缺口。

借助上级网络安全技术部门的资源下沉契机，开展适配基层运维场景的应急响应工具配齐工作，搭建固定的基层网络安全技术服务队伍，定期开展贴合基层实际运维需求的应急演练，优化风险排查、事件处置的全流程操作标准，对在岗的基层运维人员开展常态化的实操技能培训，补足外部技术支撑的覆盖盲区，提升基层对隐蔽性网络风险的识别和快速处置能力，让潜在的网络安全风险能够得到提前排查与快速化解。在技术标准统一方面，相关治理主体应推动基层网络安全设施的技术架构标准化工作，制定统一的接口规范与协议标准，确保不同厂商设备之间的兼容性与互操作性。建立基于零信任架构的基层网络访问控制体系，实施多因素身份认证与动态权限管理，将传统的边界防护模式向内生安全模式转变。同时，部署基于人工智能的威胁检测系统，利用机器学习算法对基层网络流量进行实时分析与异常识别，提升对未知威胁的检测准确率。完善基层网络安全态势感知平台建设，实现跨区域、跨层级的安全数据共享与威胁情报联动，构建覆盖网络层、应用层、数据层的立体化技术防护屏障，为基层治理提供持续、稳定的技术支撑保障。

3.2 健全跨部门网络空间协同治理机制

结合内蒙古网络安全治理覆盖多领域、多主体的实际运行情境，跨部门协同机制的健全能有效破除不同治理主体间的协作壁垒，为全区网络安全治理成效提升提供机制层面的支撑。相关治理主体对网信、公安、通信管理、工信、教育、市场监管等部门的网络安全治理职责进行梳理细化，明确不同部门在日常防护、风险排查、执法监管等环节的权责边界，理顺不同部门任务衔接的具体流程，减少权责交叉或者空白的情况，避免同类工作重复推进或者责任推诿的问题出现。围绕治理过程中信息流转不畅的现存问题，相关治理主体搭建统一的全区网络安全信息共享载体，对网络安全风险信息、事件线索、监测预警数据、执法监管信息的共享标准进行统一规范，打通不同部门间的信息流转通道，让不同主体掌握的相关治理信息能够及时同步，为各项治理工作的开展提供完整的信息支撑。

针对跨领域网络安全事件的处置需求，相关治理主体对跨部门会商研判、联合执法、应急联动、重大网络安全事件协同处置的流程进行细化统一，明确不同环节中各部门的参与方式与工作要求，适配不同部门的处置节奏，碰到跨领域的网络安全事件时能够快速整合不同部门的治理资源，形成有效的治理合力。相关治理主体把跨部门协同成效的考核纳入各部门网络安全工作的年度评价范畴，根据不同部门的职责定位设置适配的考核指标，引导各部门主动配合跨部门治理工作的开展，逐步破除原有部门间的协作障碍，让跨部门网络安全治理的运行效率得到稳步提升，契合内蒙古网络空间治理的实际需求，为全区网络安全治理整体效能的提升提供稳定的机制保障。在技术支撑层面，需搭建跨部门统一的网络安全协同指挥平台，打通网信、公安、工信、边境管理等部

ISSN：3080-2660
EISSN：3080-2679

门的数据接口，制定统一的数据共享标准与威胁情报交换协议，实现跨部门风险信息的毫秒级同步。针对内蒙古边疆跨境数据流动、牧区分散治理的特点，嵌入双语应急指令推送、跨境流量异常监测等定制化功能，利用分布式账本技术实现联合执法全流程存证，确保跨部门处置各环节可追溯、可核验，为协同治理提供精准的技术赋能。

3.3 深化全民网络安全素养培育工程

结合内蒙古城乡群众居住分散、网络使用场景覆盖生产生活全领域的现实情境，相关治理主体把全民网络安全素养培育作为筑牢全区网络安全治理社会支撑的核心举措。面向城乡居民、机关干部、企业员工、学生群体开展差异化网络安全宣传，对普通群众侧重科普日常用网的风险规避方法，对机关干部侧重普及政务数据安全防护的相关规范，对企业员工侧重宣传岗位对应的网络安全防护责任，对学生群体侧重培育基础网络安全常识与正向网络行为观念。结合网络安全治理实操环节的能力缺口，相关治理主体针对基层工作人员、关键信息基础设施从业人员、中小企业负责人等开展专业化培训，对基层工作人员设置政务用网安全、基层数据保密相关的培训内容，对关键信息基础设施从业人员设置日常风险巡检、突发隐患处置相关的技能培训内容，对中小企业负责人设置网络安全合规运营、用户数据风险防控相关的系统性培训内容。

技术层面需构建面向公众的低门槛参与支撑体系：一是优化统一举报平台功能，嵌入蒙汉双语智能填报模块，支持多格式线索上传，通过 AI 算法自动对线索进行风险等级初判，对有效举报开通匿名反馈通道，保障举报人信息安全；二是开发网络安全志愿服务专属工具，集成线索上报、风险识别、培训学习等功能，支持离线缓存适配牧区弱网环境，为志愿者提供实时技术指导；三是搭建面向公众的风险提示精准推送系统，基于用户特征定向推送适配的网络安全预警内容，配套开发轻量化风险自查小程序，引导公众自主完成设备漏洞检测、钓鱼链接识别等操作，降低技术参与门槛，真正实现技术赋能下的全民共治。

4 结语

网络安全治理是一项需要多主体协同参与的系统性工程，内蒙古的网络安全治理工作需结合当地的地域特征与治理实际开展适配性调整。后续推进过程中，需持续关注基层治理场景的实际需求，补足硬件设施与技术支撑层面的缺口，理顺跨部门协同的全流程运行机制，破除部门间的协作壁垒，同时拓展群众参与网络空间治理的渠道，实现治理效能与社会支撑水平的同步提升。相关优化路径的实施，既可以为内蒙古数字经济的平稳发展筑牢安全屏障，也能够为国家网络安全治理体系的区域落地提供本土化的实践样本。

参考文献：

[1] 曹伟峰 . 高职院校网络信息安全对策研究 [J]. 网络安全技术与应用 ,2026,(4):79-82.
[2] 林清圣 . 城市电信网络安全运行保障问题研究——以 L 市为例 [D]. 山东大学 ,2025.
[3] 郭炳均 . 大数据背景下网络安全发展对策研究 [J]. 中国宽带 ,2025,21(11):91-93.
[4] 梁露露 , 丁雨晗 , 晏晓峰 . 国内外网络安全保险发展现状、挑战及对策研究 [J]. 工业信息安全 ,2025,(3):12-18.
[5] 刘玥 .L 市个人信息安全治理的问题与对策研究 [D]. 中国矿业大学 ,2025.

作者简介：刘彩虹（1997.11—），女，汉族，山西朔州人，硕士研究生，研究实习员，研究方向：法学。

项目信息：内蒙古自治区社会科学院 2026 年度课题，“内蒙古网络安全治理现状、困境及优化路径研究 ”（编号：NDKT2026089）。