大模型视角下网络舆情 与犯罪风险预警研判

■ 林若铭 宋明珠 王晓磊

摘要 公共安全风险评估的科学性与精确性同社会治理的成效紧密相连，新一代人工智能作为驱动新型优质生产力发展的关键要素，已然成为犯罪风险预警分析的核心工具。深度剖析公安机关在网络舆情与犯罪活动风险预警研判领域现状，全面揭示大模型技术应用中的数据共享整合困境、技术人才短缺以及预警准确性与及时性不足等问题，针对性提出构建多源数据融合大模型架构、优化算法、建立动态预警反馈机制等策略方案，打破数据壁垒，为预警研判提供精准数据基石。综合实施应对策略，为公安机关网络空间预警研判工作注入强大动力，显著提升预警研判能力，有效打击犯罪、妥善应对舆情危机提供坚实有力的技术支撑与决策依据。

关键词 公安机关新质战斗力 背景与意义 特征与挑战 框架逻辑 实践路径

一、引言

第 54 次《中国互联网络发展状况统计报告》显示，截至 2024 年 6 月，我国网民规模已达 10.9967 亿，互联网普及率达高到 78.0%，网络的信息扩散功能催生了前所未

有的舆情传播态势。在数字化浪潮下，网络空间赫然成为国家主权的新疆域、经济发展的新引擎、社会治理的新领域。网络空间舆情与犯罪活动作为这一进程中的关键环节，其复杂性、多变性与严峻性日益凸显。随着信息技术的飞速发展，网络舆情的传播速度呈几何级数增长，影响力已渗透到社会的各

作者：林若铭，吉林警察学院副教授；宋明珠，吉林省长春市公安局大数据实战中心科长；王晓磊，吉林省白山市公安局技术侦察支队副支队长

基金项目：本文系吉林省高等教育教学改革重点研究课题“人工智能时代大语言模型赋能涉外警务课程教学生态体系构建研究”（项目编号：JLJY202555709553）；吉林省教育厅职业教育与成人教育课题“公安院校职业教育数字技术赋能与数字化转型研究”（项目编号：2024ZCY323）；吉林警察学院科研课题“数据跨境流动中的安全风险评估与治理技术研究”（项目编号：jykyzd202509）研究成果。

层面，不仅能左右公众舆论导向，在特定情形下更有可能诱发各类犯罪活动，严重威胁社会和谐稳定与人民群众的生命财产安全。

习近平总书记高度重视网络安全与信息化工作，多次强调要“树立正确的网络安全观”，做出“加快提升网络强国的各项能力”等一系列重要指示，为全国公安机关在网络空间领域的工作指明了清晰的方向，提供了坚实的理论遵循与行动纲领。2024年初，公安部积极响应国家战略部署，将本年度作为打击整治网络谣言专项行动年，号召全国公安机关开展为期一年的专项行动，坚持打防管控一体推进，加大全链条、全平台、全领域打击力度。近年来，中国公安机关在探索中逐步明确，要实现对社会治安防控形势的主动性应对，就必须充分应用现代化信息技术予以辅助，科技强警正是实现数字时代警务治理效能变革的根本要求。当前，全国公安机关充分利用大数据技术强化对犯罪行为的提前感知和精准防控，已成为全面实现风险社会主动型警务治理及推进国家治理体系和治理能力现代化建设的显著性标志。

中国公安肩负着维护地区社会稳定、保障人民安居乐业的神圣使命，在网络空间这一无形战场上，如何精准把握舆情动态，提前预警犯罪风险，是摆在全国公安队伍面前的重大课题与紧迫任务。基于大模型技术开展网络空间舆情和犯罪活动风险预警研判研究，恰是契合时代需求、落实国家政策的重要举措。通过充分利用大模型强大的数据处理能力、高度智能化的分析研判功能，能够有效整合各类碎片化信息，挖掘隐藏在海量数据背后的深层次关联与潜在风险，为公安部门实现从被动应对到主动防控的战略转变，提供强有力的技术支撑与决策依据。相关研究不仅有助于提升公安队伍在网络空间

治理领域的核心竞争力，更对国家网络安全战略在地方层面的深入贯彻与生动实践，对维护国家网络主权、保障国家、地区经济社会健康稳定发展具有不可替代的重要意义。

二、吉林省网络空间舆情与犯罪活动的关联性

国防科技大学信息通信学院助理研究员袁唯淋博士认为，网络舆情与犯罪活动相互影响、密切关联。“加强联合情报与网络开源情报大数据信息关联印证，推动跨网络平台信息融合，加速共享数据”，将有助于在网络战、心理战、舆论战、自媒体战等跨领域跨媒体舆情塑造与认知对抗中赢得先机。一方面，网络舆情通过快速曝光和舆论监督，有助于揭露犯罪、提供线索，从而加速案件侦破；但同时虚假信息的扩散可能误导执法，甚至煽动极端行为，扰乱社会秩序。另一方面，重大犯罪事件常常成为舆情热点，官方信息发布与嫌疑人回应则直接影响舆情的走向。因此，厘清两者的互动机制，对提升预警能力和有效应对犯罪至关重要。

（一）网络舆情对犯罪活动的影响

网络舆情具有强大的信息传播与舆论监督功能，能够对犯罪活动产生多维度的影响。一方面，网络舆情能够对犯罪行为起到监督与揭露的作用。在信息传播迅速的网络时代，犯罪行为一旦发生，相关信息很容易被曝光于网络平台之上，引发广大网民的关注与讨论。近年来一些社会热点犯罪案件，如校园霸凌、职场性骚扰等事件，经网络传播后迅速发酵，形成强大的舆论压力，促使执法机关加快调查与处理进程，使得犯罪者难以遁形。此外，网民们在网络舆情的扩散过程中，还可能提供大量与犯罪活动相关的线索，如

犯罪嫌疑人的行踪、犯罪手段的细节等, 这些线索为执法部门侦破案件提供了有力的支持, 极大地提高了打击犯罪的效率。然而, 网络舆情也可能对犯罪活动产生误导与煽动的负面影响。网络空间信息繁杂, 不乏虚假信息与谣言的滋生与传播。一些不实的犯罪报道或恶意编造的谣言可能会误导公众对犯罪活动的认知, 干扰司法机关的正常办案思路。在某些刑事案件中, 网络上流传的虚假嫌疑人信息或错误的犯罪动机分析, 可能会使警方在侦查初期误入歧途, 浪费宝贵的时间与资源。同时, 部分极端的网络舆情可能会煽动公众的情绪, 引发群体性行为甚至导致新的违法犯罪行为发生。当一些犯罪事件引发公众强烈的愤怒与不满时, 可能会出现网络暴力、人肉搜索等行为, 不仅侵犯他人的合法权益, 也破坏社会的法治秩序。

(二) 犯罪活动对网络舆情的影响

犯罪活动作为社会负面事件的重要组成部分, 对网络舆情的产生与发展有着显著的塑造作用。其一, 犯罪活动往往能够引发舆情热点。重大的犯罪事件, 如恐怖袭击、恶性凶杀、大型金融诈骗等, 因其具有极大的社会危害性与震撼性, 极易吸引公众的目光并迅速成为网络舆情的焦点话题。这些事件不仅在事发当地引起强烈反响, 而且通过网络传播, 能够在短时间内引发全国乃至全球范围内的广泛关注与讨论。例如, 恐怖袭击事件发生后, 网络上会充斥着关于事件现场情况、伤亡人数、恐怖组织背景等多方面信息的报道与讨论, 人们在表达对受害者同情与对恐怖主义谴责的同时, 也会对事件背后的原因、社会安保措施的漏洞等进行深入的反思与探讨。其二, 犯罪活动还深刻地影响着网络舆情的走向。在犯罪事件发生后, 官方的信息发布与通报是引导网络舆情走向的

关键因素之一。及时、准确、透明的官方信息能够有效地缓解公众的恐慌与焦虑情绪, 稳定网络舆情态势, 避免谣言与不实信息的泛滥。反之, 若官方信息发布滞后或含糊不清, 网络舆情则可能陷入混乱与猜测之中, 各种谣言与虚假信息将趁机传播, 导致舆情走向失控。此外, 犯罪嫌疑人的回应与行为也会在一定程度上影响网络舆情的发展轨迹。一些犯罪嫌疑人被抓获后可能会通过网络发表忏悔声明或为自己的行为进行辩解, 这些言行往往会引发公众新一轮的讨论与争议, 从而改变网络舆情的发展方向与热度。

三、大模型技术在相关领域的应用现状

预测性侦查是风险社会语境中, 侦查机关为妥善因应智能化犯罪态势、创新犯罪治理模式而采用的一种主动型侦查策略, 是国家凭借现代化技术推动治理体系与治理能力现代化进程的关键手段之一。公安机关通过对海量数据的深度挖掘与分析, 运用先进算法与模型, 提前洞察犯罪潜在趋势与风险, 从而实现精准预防与高效打击犯罪的有机结合, 为维护社会安全稳定筑牢坚实屏障。中国公安机关正在积极探索大模型技术在网络舆情与犯罪预警中的应用, 并已在多个地区取得显著成效。此类探索与实践展示了大模型在提升公安工作效率和社会治安管控方面的巨大潜力。

(一) 国内大模型技术应用案例分析

在国内发达地区, 公安机关积极探索大模型技术在网络空间舆情与犯罪活动预警研判方面的应用, 并取得了令人瞩目的成果, 为其他地区提供了宝贵的借鉴经验。

以上海市公安局为例, 上海市局构建的

智能化网络舆情监测与分析系统充分彰显了大模型技术的优势。该系统依托先进的自然语言处理技术与深度学习算法,具备对微博、微信、抖音等主流社交媒体以及各大新闻网站海量信息的实时监测能力。在舆情信息处理上,能够精准地进行情感分析,准确判断公众对特定事件的态度倾向,无论是积极的支持、消极的不满还是中性的客观陈述,都能清晰洞察。同时,对话题的分类细致入微,可将繁杂的舆情信息按照不同主题进行归类整理,方便后续分析与管理。热度评估功能则能迅速确定哪些舆情话题正在引发广泛关注,哪些尚处于萌芽状态,从而使公安机关能够及时聚焦重点舆情。此外,传播路径追踪更是一大亮点,可以清晰描绘出舆情信息在网络中的扩散脉络,从最初的发布源头,到逐步传播扩散的各个节点,以及最终形成广泛影响力的传播轨迹,都能完整呈现。在一次重大国际会议于上海举办期间,该系统充分发挥了其预警作用。当时,会议安保措施与交通管制等相关安排引发了部分网民的讨论,系统及时捕捉到了多条负面舆情信息。这些信息涉及对安保措施的质疑、对交通管制造成不便的抱怨等内容。系统迅速对这些舆情进行了全面分析,并及时发出预警。上海市公安局依据预警信息,迅速做出反应,对安保策略进行优化调整,加强了某些关键区域的安保力量部署,改进了安检流程以提高通行效率等。在交通疏导方面,根据舆情反映的热点路段和时段,重新规划了交通管制方案,增加了临时交通疏导标识和警力配置。同时,通过官方微博、微信公众号等权威渠道,及时、准确地发布关于会议安保和交通管制的详细信息,正面回应公众关切,解释相关措施的必要性和合理性,有效引导了舆情走向,成功避免了舆情危机的升级,

保障了国际会议的顺利进行,也维护了城市的良好形象和社会稳定。

(二) 中国公安机关的初步探索与实践

中国公安机关紧跟时代步伐,积极投身于大模型技术在网络舆情与犯罪预警研判领域的应用探索,近年来已经在实践中取得了一系列具有积极意义的成果。

在舆情监测方面,吉林公安通过与省内具有较强技术实力和丰富行业经验的知名科技企业紧密合作,成功搭建了基础的网络舆情监测平台。该平台具备强大的信息采集功能,能够对省内主要网络论坛,如吉林本地热门的社区论坛,社交媒体群组,涵盖微信、QQ等各类社交群组,以及新闻网站等多样化的网络平台进行全天候24小时不间断的舆情信息采集。采集到的信息经过初步处理与分析,能够提取出关键要素。2024年春节期间,吉林省部分地区遭受极端恶劣天气的侵袭,这一突发情况导致了小范围交通瘫痪、电力中断等问题,给民众的生活和出行带来了不便,迅速成为网络舆情关注的焦点。该舆情监测平台在第一时间捕捉到了大量与恶劣天气相关的舆情信息,包括民众在网络上发布的关于被困途中的求助信息、对交通疏导不力的抱怨、对电力抢修进度的关切等内容。随后,平台利用自身的分析功能,迅速对舆情的传播范围进行了精准定位,确定了舆情信息主要传播的地区、网络平台以及受众群体;对民众情绪倾向进行了细致分析,明确了民众主要的情绪表现是焦虑、不满还是对救援工作的期待;并准确提炼出民众的主要诉求,如尽快恢复交通、加快电力抢修进度、提供应急救援物资等信息。公安机关依据平台提供的这份详尽且准确的分析报告,迅速启动了应急预案。积极协调交通部门,调配清雪车辆、救援拖车等资源,对交

通瘫痪路段进行疏通清理，并及时发布交通路况信息，引导车辆绕行；与电力部门协同作战，组织抢修队伍加班加点恢复电力供应，并向民众通报抢修进展情况。同时，通过官方微博、微信公众号等渠道，及时发布救援工作的最新进展，包括已清理的道路路段、预计恢复电力时间等信息，有效缓解了民众的恐慌情绪，避免了舆情的进一步恶化，为抢险救援工作营造了较为稳定的舆论环境。

在犯罪活动预警方面，辽宁公安充分利用大模型技术对现有的犯罪数据库展开了深入的数据分析与挖掘工作。以盗窃犯罪为例，对近三年来辽宁省范围内的盗窃案件数据进行了全面梳理后发现，在案发时间维度上，不同季节、月份、星期以及一天中不同时段盗窃案件的发生频率存在差异性。例如某些老旧小区在冬季夜晚盗窃案件相对高发，因为冬季夜晚居民户外活动减少，且老旧小区安保设施相对薄弱；在案发地点方面，详细记录了盗窃案件发生的具体地址，如哪些社区、街道、商场周边盗窃案件频发，并结合地理环境和周边人口流动情况分析原因，例如一些位于城乡结合部的集市附近，人员流动性大且环境复杂，容易成为盗窃分子的作案目标；被盗物品类型的分析则有助于了解盗窃分子的作案动机和目标偏好，如某些地区盗窃手机、电动车等便于携带和销赃的物品较为常见；对于犯罪嫌疑人特征的分析，涵盖了年龄、性别、是否有犯罪前科、作案手段特点等多个方面，发现一些年轻无业人员更倾向于团伙作案，采用技术开锁手段盗窃高档住宅等规律。通过对这些丰富数据的整理分析，构建了盗窃犯罪风险预测模型的雏形。在模型试运行期间，取得了初步成效。成功预测了部分老旧小区在冬季夜晚的盗窃犯罪高发区域，公安机关根据预测结果提前

部署警力，加强了这些区域的巡逻防控力度，设置了临时治安卡点，增加了便衣民警的巡查频率等。据不完全统计，在试点区域内，盗窃案件的发生率在预警防控期间有了明显下降。这一成果初步验证了大模型技术在辽宁省犯罪活动预警方面的应用潜力与价值，为进一步完善和推广该技术在犯罪预防工作中的应用奠定了坚实基础。

四、体制、机制、瓶颈性问题

当前公安数据共享与整合面临体制性、机制性及技术性瓶颈。首先，公安内部各部门职责分明，但数据壁垒显著，刑侦和网安部门虽分别掌握犯罪嫌疑人身份信息及网络行为数据，但因共享机制缺失，数据难以整合，导致网络犯罪侦查时线索断裂、案件延误。其次，跨部门数据协作困难。打击网络经济犯罪需工商、税务等部门提供企业登记和财务数据，但因数据标准不统一，公安机关在获取和整合外部数据时耗费大量时间，影响办案效率。此外，数据整合技术复杂且成本高。公安内部数据结构化程度高，但外部数据多为半结构化或非结构化，且数据编码标准不一，需大量清洗和转换。数据精度参差不齐，导致在预警分析时效性和准确性上受限，严重影响打击犯罪的有效性和及时性。整体看数据壁垒和整合难题亟待解决，以便有效提升公安工作的效率性和精准度。

（一）数据共享与整合难题

数字化浪潮的席卷下，数据问题已经成为我国公安工作的核心要素之一，公安机关在数据共享与整合方面都遭遇了诸多困境。

公安内部而言，各部门职能的明确划分虽有利于专业工作的开展，但却在数据流通环节形成了壁垒。刑侦部门掌握的犯罪嫌疑

人包括身份背景、犯罪前科、社会关系等在内的详细信息，犹如一座待开发的金矿；而网安部门所掌握的海量网络行为数据，如网络访问记录、IP 追踪详情、社交平台互动信息等，则是洞察犯罪嫌疑人网络踪迹的关键钥匙。但因部门间缺乏有效的共享机制，且数据管理权限相互独立，这些宝贵的数据资源难以实现整合利用。在实际的网络犯罪侦查中，这种数据隔阂往往导致关键线索的断裂。在某起复杂的网络诈骗案件中，刑侦人员通过传统侦查手段锁定了部分嫌疑人的线下身份，但在深入探究其网络诈骗运作模式、资金流转渠道以及与其他同伙的网络关联时，却因无法及时获取网安部门的数据而陷入困境。案件侦破进度被迫延缓，犯罪分子得以有更多时间隐匿证据、转移资产，甚至继续实施犯罪，既损害了公众利益，也削弱了公安机关打击犯罪的效能。

从公安与其他政府部门的数据交互视角审视，同样面临着重重阻碍。以打击网络经济犯罪为例，此类犯罪涉及经济活动的多个层面，需要多部门协同作战，其中工商部门的企业注册登记信息以及税务部门的纳税数据尤为关键。工商登记信息涵盖企业的基本架构、经营范围、股东构成等内容，能为剖析犯罪主体的组织形式和业务脉络提供重要依据；纳税数据则可反映企业的财务状况和经营真实性，有助于揭露经济犯罪中的资金异常流动。然而，由于各部门数据标准不同，缺乏统一的数据共享规范和对接流程，数据的格式、编码以及更新频率存在显著差异。这使得公安机关在获取这些外部数据时困难重重，往往需要耗费大量时间和精力进行数据的协调、转换与清洗工作。在某网络传销案件侦查初期，公安部门向工商部门申请企业注册数据，但因数据格式不兼容，不得不

安排专人进行格式转换与数据整理，导致侦查工作延误，错失最佳取证时机，给案件后续侦破和追赃挽损带来极大挑战。

而在数据整合的具体实践中，公安系统内部及外部数据的复杂性和异构性进一步加剧了整合难度。数据来源广泛，既有公安内部结构化的案件卷宗记录、人口信息库等业务数据，其特点是具有明确的字段定义和数据类型，便于查询与统计分析；又有大量外部的半结构化和非结构化数据，半结构化数据如网络运营商提供的部分网络日志，虽有一定的结构框架，但仍需复杂解析才能提取有效信息；非结构化数据则如社交媒体上的用户言论、图片和视频等，缺乏预先定义的格式，蕴含信息的挖掘依赖于先进的自然语言处理和计算机视觉技术。在编码方式上，不同数据源可能采用不同的字符编码标准，如公安内部系统和互联网数据采用的编码就各不同，在数据整合时就极易引发乱码和信息丢失问题出现。此外，数据精度参差不齐，受采集设备误差、录入人员疏忽以及数据传输干扰等因素影响，部分数据存在错误、缺失或重复现象。以网络流量数据为例，其数据量庞大且冗余信息多，从网络运营商获取后，需进行大规模的数据清洗，去除无效的浏览记录、广告流量等，再转换为统一的结构化格式，将网络连接信息整理为包含源 IP、目标 IP、连接时长等字段的规范数据表，最后才能与公安内部数据库进行关联整合，构建完整的犯罪分析数据模型。这一过程不仅技术要求高，且需投入大量人力和时间成本，严重制约了网络犯罪预警研判工作的时效性和精准性。

（二）技术应用与人才短缺矛盾

随着科技的迅猛发展，大模型技术在公安领域的应用前景日益广阔，但我国公安机

关在这一进程中却面临技术应用与人才短缺的矛盾短板。大模型技术作为信息技术领域的前沿高地,融合深度学习、自然语言处理、计算机视觉等多学科的先进成果,在公安工作中的应用涉及数据处理全链条,从海量数据的采集汇聚,到安全存储与高效管理,再到深度分析挖掘以及直观的可视化展示,每一个环节都对专业技术人才提出了极高要求。然而,公安队伍当前的人才储备状况却远远滞后于技术发展需求。

一方面,既精通公安业务又擅长大模型技术开发应用的复合型人才稀缺程度堪忧。公安业务知识体系犹如一片广袤而深邃的海洋,涵盖法律法规、侦查学、治安管理学、犯罪心理学等众多学科领域,要求从业者不仅要熟谙各类案件办理流程,在复杂的犯罪现场和线索迷宫中精准导航,锁定犯罪嫌疑人,还要依据法律法规确保执法公正合法,维护社会公平正义。而大模型技术领域则是一座技术密集型的科技大厦,需要坚实的计算机科学、数学、统计学等学科基础,熟练掌握 TensorFlow、PyTorch 等深度学习框架,能够灵活构建、训练、优化和部署大模型,从海量数据中提炼有价值的情报信息。但国内部分省份公安机关当前的实际情况是,现有的技术人员大多长期专注于传统信息技术工作,如网络安全防护、信息系统管理等,其知识结构和技能体系与大模型技术的要求存在较大差距。例如,在构建基于大模型的网络舆情监测系统时,技术人员不仅要运用自然语言处理技术对网络文本数据进行语义理解、情感分析和话题分类,精准把握舆情走向,还要结合公安舆情工作的特殊需求,制定科学合理的预警指标和应对策略。但由于复合型人才的匮乏,导致在系统建设过程中,技术人员难以将公安业务需求有效转化

为技术实现方案,使得系统功能和性能大打折扣,无法为公安舆情监测工作提供有力支撑,严重影响了工作效率和质量。

另一方面,人才引进与培养机制的不完善进一步加剧了人才短缺困境。以东北三省为例,受地理位置、经济发展水平以及公安工作高强度、高风险等特殊职业属性的影响,东北三省地区在引进高素质的大模型技术人才方面,与国内发达省份和地区相较而言缺乏竞争力。尽管东三省政府近年来积极出台一系列人才引进优惠政策,如提供住房补贴、科研启动资金、子女教育优待等,但相较于发达地区更为优厚的待遇、更广阔的职业发展空间和更丰富的资源平台,这些政策的吸引力略显不足,难以吸引到国内一流的大模型技术人才投身公安事业。在人才培养方面,东三省公安教育部门同样面临困境。公安院校现有的基于公安网络安全技术培训体系刚刚围绕信息安全技术开展构建,对于大模型技术这一新兴领域的培训内容相对匮乏,课程设置缺乏系统性和前瞻性,课程内容部分相较于基础知识的习得,未能紧密结合公安业务实际需求开展深入的应用案例教学和实践操作训练。同时,由于缺乏专门的大模型技术实践平台,无论是公安大学生的学历培养,还是网络安全岗位的公安技术人员培训,相关人员在学过程中难以获得足够的实战锻炼机会,无法将理论知识有效转化为实际应用能力,导致技术水平提升缓慢,难以满足日益增长的公安工作对大模型技术人才的迫切需求。在组织大模型技术培训时,往往因为缺乏真实的公安业务数据和模拟实战场景,技术人员只能使用公开的通用数据集进行练习,无法深入了解公安数据的独特性和处理难点,难以掌握在实际工作中如何根据不同犯罪类型和舆情特点构建精准有效的大

模型，从而严重影响了培训效果和人才培养质量，制约了大模型技术在公安工作中的深入应用和创新发展。

（三）预警研判的准确性与及时性不足

在网络空间舆情与犯罪活动瞬息万变的当下，中国公安部门所采用的预警研判手段在准确性与及时性方面暴露出短板，难以有效应对复杂多变的安全挑战。

从准确性层面剖析，网络舆情信息的复杂性和多样性犹如一团迷雾，使现有预警研判模型在语义理解、情感倾向判断以及事件关联分析时常常迷失方向。网络舆情不仅包含传统的文本信息，而且涵盖图片、视频等多媒体元素，且语言表达形式日益丰富，网络流行语、隐喻、反讽、幽默等修辞手法层出不穷。例如，在一些热点舆情事件中，网民频繁使用诸如“绝绝子”“凡尔赛”等网络流行语来表达观点和情感，这些流行语往往具有模糊性、多义性和情境依赖性，其含义在不同语境和受众群体中可能发生显著变化。现有的预警研判模型由于缺乏对这些新兴语言现象的深度理解和语义解析能力，难以精准把握网民的真实意图和情感倾向，容易将一些网民的调侃、戏谑或轻微不满言论误判为严重的负面舆情，进而触发不必要的预警和应对机制，造成警力资源的浪费和社会恐慌的蔓延。又如，在涉及社会争议话题的舆情事件中，部分网民可能采用反讽或幽默的表达方式来隐晦地表达对事件的看法，这种表达具有较强的迷惑性和误导性。预警模型若不能及时更新并且有效识别其中的修辞手法和真实意图，可能会错误判断舆情的性质和发展趋势，导致预警信息与实际舆情严重脱节，使公安机关在舆情应对中陷入被动局面，无法有效引导舆论走向，甚至可能进一步激化矛盾，影响社会和谐稳定。

在事件关联分析领域，网络舆情信息往往涉及多个事件、多个主体之间错综复杂的关联关系，这些关系犹如一张无形的大网，既有显性的直接联系，也有隐性的间接关联，需要借助强大的文本挖掘和语义分析能力才能洞察全貌。然而，现有预警研判模型在处理此类复杂关联关系时显得力不从心，往往只能捕捉到表面的、显而易见的关联信息，对于深层次的、间接的关联线索则难以察觉。例如，在系列网络犯罪案件的舆情传播中，不同案件可能由同一犯罪团伙策划实施，或采用相似的作案手法，或存在资金、人员等方面的隐秘关联，但由于模型的分析能力有限，无法从海量的舆情信息中准确梳理出这些隐藏的关联线索，难以构建完整的犯罪网络画像，致使公安机关在打击犯罪时无法做到全面布局、精准打击，容易出现漏网之鱼，使犯罪活动得以持续蔓延，给社会带来持续的安全威胁。

在犯罪活动预警战线，随着网络技术的飞速发展，犯罪手段日新月异，呈现出高度智能化、隐蔽化和跨区域化的特征，犹如隐藏在黑暗中的幽灵，难以捉摸。新型犯罪模式例如利用区块链技术进行洗钱犯罪、借助人工智能技术实施诈骗等不断涌现，给公安机关的预警研判工作带来了前所未有的挑战。现有的预警模型由于数据更新滞后、算法优化迟缓以及对新型犯罪特征认识不足等原因，难以在新型犯罪萌芽之初及时察觉并发出预警信号。以区块链洗钱犯罪为例，区块链技术的去中心化、匿名性和不可篡改等特性，为犯罪资金的转移提供了天然的掩护，使其交易路径变得极为复杂和隐蔽，传统的金融监管和侦查手段难以奏效。而现有的犯罪预警模型由于缺乏对区块链技术原理和交易模式的深入研究，无法及时更新数据采集

和分析算法,难以对区块链洗钱犯罪的早期迹象进行有效识别和预警。往往在犯罪活动已经造成了巨大的经济损失和广泛的社会影响后,公安机关才通过其他渠道发现线索并介入调查,但此时犯罪分子可能已经成功转移了大量非法资金,销毁了关键证据,使案件侦破和追赃挽损工作陷入困境,严重损害了公众利益和社会经济秩序。同样,在人工智能诈骗犯罪中,犯罪分子常常利用人工智能技术生成逼真的影像、语音、视频或文本信息,针对特定目标实施精准诈骗,使传统的基于特征识别和行为模式分析的传统预警模型难以发挥有效作用。现有模型由于无法及时跟上人工智能技术在诈骗领域的应用步伐,更新算法模型以适应新的犯罪特征,在面对此类新型犯罪时往往处于被动挨打境地,无法及时有效地保护人民群众的财产安全和维护社会稳定,使公众对于我国公安机关各项工作的信任度受到严峻考验。

五、基于大模型提升预警研判能力的理论与策略

提升公安部门预警研判能力的核心在于构建多源数据融合的大模型架构,优化算法以提升预警精度,并建立动态预警与反馈机制。通过整合公安内部各部门数据及外部机构信息,实现数据的标准化与预处理,大模型可基于 PCA 和贝叶斯网络等技术进行高效研判,提升犯罪预测和舆情监测的准确度。此外, CNN、RNN 和 GAN 等算法在舆情分析及异常检测中展现了独特优势,通过持续动态学习与增量训练,模型能够快速适应新型犯罪和突发舆情趋势,并通过预警反馈机制不断优化,为社会治安提供精准保障。

(一) 构建多源数据融合的大模型架构

在公安部门的工作实践中,构建多源数据融合的大模型架构对于提升预警研判能力具有极为关键的意义。

在数据来源与采集范围方面,公安内部各部门拥有丰富且独特的信息资源,刑侦部门的案件卷宗信息犹如一部部犯罪纪实档案,详细记录着各类刑事案件的案发经过、现场勘查细节、证人证言以及犯罪嫌疑人的初步审讯情况等,这些信息为深入剖析犯罪行为模式、追踪犯罪团伙脉络提供了坚实基础。治安监控数据则像是城市治安的“眼睛”,全天候不间断地记录着大街小巷的人员流动、车辆行驶轨迹以及公共场所的秩序状况,对于及时发现治安隐患、预防违法犯罪活动的发生起着不可或缺的作用。网安部门的网络监测数据则深入网络空间的“虚拟战场”,捕捉着网络用户的访问行为、网络社交互动信息以及潜在的网络攻击迹象等,为打击网络犯罪、维护网络安全提供了关键线索。经侦部门所掌握的经济犯罪线索更是犹如经济领域的“风险探测器”,能够敏锐地感知到金融诈骗、商业贿赂、洗钱等各类经济犯罪活动的蛛丝马迹,在维护市场经济秩序方面发挥着重要作用。

在外部数据合作方面,与工商部门的协作能够获取企业注册信息,这对于排查经济犯罪中的涉案企业背景、经营状况以及关联企业网络具有重要价值。例如,在调查某起网络传销案件时,企业注册信息可以揭示出该传销组织的层级架构、注册地址的真实性以及背后操控者的身份信息等。税务部门的纳税记录则能反映企业的财务健康状况和资金流向,有助于发现企业是否存在虚报账目、偷税漏税等经济犯罪行为,以及是否与其他犯罪活动存在资金关联。民政部门的人口户籍信息为公安部门提供了准确的人口基础数

据,在人口失踪案件、身份核实以及犯罪嫌疑人追踪等工作中发挥着基础性作用。教育背景数据则有助于在涉及校园安全、高学历犯罪以及针对教育机构的犯罪案件中,深入了解犯罪嫌疑人的知识结构、社会关系网络以及可能的犯罪动机。金融机构的交易流水数据更是如同金融领域的“血管造影”,清晰地展示着资金的流动路径、交易频率和金额大小,对于追踪犯罪资金的去向、揭露洗钱犯罪和金融诈骗犯罪的运作机制具有不可替代的作用。网络运营商和互联网企业提供的网络用户行为数据则能深入反映网络用户的兴趣偏好、社交圈子以及在网络空间中的活动规律,在网络犯罪预警和网络舆情监测方面提供了丰富的素材。

在数据清洗与预处理环节,公安部门面临着复杂多样的数据质量挑战,针对公安内部案件数据,由于人工录入错误、信息更新不及时等原因,可能存在错误信息。例如,犯罪嫌疑人的年龄、住址等信息可能存在笔误或因户籍变动而未及时更新。利用数据校验规则,如设定年龄范围的合理性校验、地址格式的规范性校验等,可以有效纠正这些错误信息。对于网络运营商提供的海量网络流量数据,其中包含大量的重复数据,如同一用户在短时间内对同一网站的多次重复访问记录。通过数据去重算法,能够大幅减少数据冗余,提高数据处理效率。同时,不同来源的数据在格式和量级上存在巨大差异。公安内部的结构化数据可能以关系型数据库表的形式存储,而网络舆情数据可能是半结构化的JSON格式或非结构化的文本、图片、视频等。采用标准化与归一化操作,将文本数据进行统一编码转换、数值型数据进行归一化处理,使所有数据都能在同一标准框架下进行分析与模型训练。

构建大模型数据融合框架时,PCA算法在处理公安多源数据中的高维数据时优势明显。例如,在整合治安监控视频数据、网络用户行为数据以及犯罪嫌疑人特征数据时,这些数据往往具有众多的特征维度。PCA算法能够通过线性变换将高维数据投影到低维空间,在保留数据主要特征的同时,减少数据冗余和计算复杂度。而贝叶斯网络算法则能充分利用公安数据中不同特征之间的概率关系。在网络舆情与犯罪活动的综合判断中,如判断某一网络舆情热点是否可能引发线下犯罪活动时,贝叶斯网络算法可以根据以往的经验数据,计算出网络舆情热度、言论倾向性、涉及人群特征等因素与犯罪发生概率之间的关系,从而实现对网络舆情与犯罪活动的精准综合判断与预测。通过这种多源数据融合的大模型架构,公安部门能够为预警研判构建起坚实而丰富的数据基础,有效提升对网络空间舆情与犯罪活动的预警能力。

(二) 优化大模型算法提升预警精度

在公安工作情境下,优化大模型算法对于提升预警精度是极为必要的探索方向。

在网络舆情分析方面,CNN与RNN相结合的混合神经网络模型有着广阔的应用前景。以国内某地区发生的某次大型活动安保期间的网络舆情监测为例,活动期间会产生大量包含图片和视频的网络舆情信息。CNN能够对活动现场周边人群聚集的图片进行分析,准确识别出人群的密集程度、是否存在可疑人员或危险物品等关键特征。对于视频信息,CNN可以提取出视频中的关键帧,并对帧内的人物行为动作、车辆行驶轨迹等进行特征识别。例如,在监测到一段关于活动场馆附近道路的视频舆情时,CNN能够快速判断出视频中车辆是否存在

违规行驶、是否有可疑车辆徘徊等情况。而 RNN 在处理与活动相关的文本舆情信息时则大显身手。当网络上出现大量关于活动安排、安保措施的讨论时, RNN 可以深入理解文本的语义, 捕捉上下文语义关系。比如, 在分析网民对安保措施的评价时, RNN 能够准确判断出评价是正面的肯定还是负面的批评, 以及负面评价背后的具体诉求和潜在风险, 从而精准判断舆情信息的情感倾向, 为安保工作的调整和优化提供及时准确的依据。

在犯罪活动预警方面, 基于 GAN 的异常检测算法能够为公安部门提供新思路。在打击盗窃犯罪中, 公安机关能够搜集到包括盗窃地点、时间、被盗物品类型以及犯罪嫌疑人特征等信息在内的大量盗窃案件数据。通过 GAN 算法, 生成器可以根据这些真实数据生成模拟的盗窃案件数据, 这些模拟数据在特征分布上与真实数据相似。判别器可以对生成数据和真实数据进行区分判断。在训练过程中, 生成器不断学习真实数据的特征分布, 优化生成数据的质量, 使其更接近真实犯罪数据; 判别器则不断提高自身的判别能力, 更加精准地区分真实与虚假数据。通过这种对抗训练机制, 能够有效挖掘出隐藏在海量盗窃犯罪数据中的异常模式。例如, 发现某些地区在特定时间段内出现的盗窃案件特征与以往不同, 如盗窃物品类型的突然变化、作案手法的创新等, 以及潜在的犯罪趋势, 如盗窃犯罪有向特定区域或特定人群转移的迹象, 从而提前发出预警, 提高对盗窃犯罪活动的预警精度, 能够有效预防犯罪的发生, 维护社会的治安稳定。

(三) 建立动态预警与反馈机制

在公安工作的实际运行中, 建立动态预警与反馈机制对于保障预警的可靠性与有效

性起着核心支撑作用。

大模型的动态学习能力是应对复杂多变的网络舆情与犯罪活动的关键。在增量学习算法的采用方面, 当某地区出现新的网络舆情热点时, 新的舆情数据会实时流入大模型。模型能够在不重新训练整个模型的基础上, 快速学习新数据中的特征与模式。在学习关于某起突发事件的网络舆情文本时, 模型能够迅速捕捉到新出现的关键词、话题焦点以及情感倾向的变化, 更新对该地区网络舆情发展趋势的认知。在犯罪数据方面, 当某一新型犯罪模式首次在某地区出现时, 例如新型网络诈骗手段的传入, 相关犯罪数据流入模型后, 模型能够及时调整对犯罪活动规律的理解, 快速识别出这种新型犯罪的特征, 为后续的预警工作提供及时准确的依据。

预警反馈机制在公安实战工作中也有着深刻的体现。当预警模型提示某地区可能发生网络诈骗犯罪高发情况后, 公安机关会迅速加强该地区的防控工作, 加大网络监测力度、对重点人群进行防范宣传教育、在金融机构设置预警提示。同时, 对该地区实际发生的诈骗案件进行详细记录与深入分析。若发现预警的犯罪类型与实际发生的犯罪存在偏差, 如预警为网络购物诈骗, 但实际发生的多为网络贷款诈骗, 或者预警的犯罪时间、地点与实际情况不符, 如预警的犯罪高发时间段为白天, 但实际多发生在夜间, 犯罪地点预测不准确等情况, 将这些偏差信息反馈给大模型。大模型根据反馈信息对参数进行调整与算法优化, 如调整在该地区网络诈骗类型判断的权重参数、优化犯罪时间地点预测的算法模型等。通过这样不断的反馈与修正过程, 预警模型能更好地适应全国不同省份、不同地区、不同类型的网络舆情与犯罪活动特点, 不断提高其准确性与适应性, 为

我国公安机关在维护社会稳定、打击犯罪活动方面提供更加强有力的技术支持，保障人民群众的生命财产安全和社会的和谐稳定。

六、结语

展望未来，大模型技术的持续演进将为公安工作缔造前所未有的变革契机。在数据处理维度、深度与广度的拓展以及算法智能化程度的稳步上扬，将为深度解析网络空间复杂舆情态势与犯罪模式创造极大可能。特别是针对利用人工智能诈骗、加密数字货币洗钱等新型犯罪，大模型技术能够精准捕捉初期迹象，必将有效助力公安部门将犯罪活动扼杀于萌芽。随着公安工作数字化、智能化转型进程的加快，公安部门需全方位加大相关领域的投入力度。在技术研发层面，积极探寻与量子计算、边缘计算等新兴技术的融合之道，借助量子计算强大算力加速数据处理与模型训练，依托边缘计算达成数据分布式处理与快速响应，进而提升预警研判的及时性。在人才培养方面，着力构建多层次、全方位人才培育体系，联合高校、科研机构开设定制化课程与实践项目，造就理论与实践并重的专业人才，并为在职民警提供常态化技术培训与进修机遇，能够全方位地提升公安队伍技术素养。在数据治理层面，建立精细化数据管理规范与质量监控体系，运用自动化、智能化数据清洗、整理与分类工具，确保数据的准确性、完整性与时效性，为预警研判筑牢高质量数据根基。

与此同时，强化与国内国际同行的交流合作意义重大。在国内，与发达地区公安机关开展深度合作交流，汲取其先进技术应用经验与管理模式，借鉴一线城市网络舆情大数据分析平台建设与运营的成功范例，优化全国各省份舆情监测系统。在国际上，踊跃参与国际警务合作项目与学术研讨活动，及时洞悉全球网络空间安全治理前沿动态与先进技术，学习国际刑警组织跨境网络犯罪打击协作机制的创新举措，提升中国公安在国际网络安全舞台的协作能力与影响力。通过持之以恒地与时俱进、开拓创新，中国公安必将能够坦然应对新时代网络空间安全治理的严峻挑战，为构建安全、文明、和谐的网络空间生态环境挥毫泼墨，为人民群众精心营造晴朗、安全的网络空间与社会环境。

参考文献：

- [1]张全涛. 从被动应对到主动防控：我国预测性侦查的理论证成与规制选择[J]. 中国人民公安大学学报(社会科学版). 2022. 3
- [2]吴明曦. 智能化战争[M]. 国防工业出版社. 2020
- [3]艾明、欧凯文. 预测性侦查的权力扩张与程序规制[J]. 中国人民公安大学学报(社会科学版). 2024. 4
- [4]宋静怡. 成都市数字政府建设中的问题与对策研究[D]. 四川大学. 2022. 4
- [5]吴丹. 人工智能背景下电信网络诈骗犯罪样态及数字化治理[J]. 公安研究. 2024. 10
- [6]傅建平. 数字政府建设中应用生成式人工智能的风险及其克服[J]. 武汉大学学报(哲学社会科学版). 2024. 6
- [7]李翠竹. 社会热点事件(2021~2023)舆情图像的视觉框架及视觉修辞研究[D]. 云南师范大学. 2024. 6
- [8]陈涛、黄丽达、陈杨、袁宏永、范维澄. 公共安全领域工程科技未来20年发展战略研究[J]. 中国工程科学. 2024. 5

责任编辑 尚钰涛