社会科学与教育 2026年第10期
ISSN: 3079-4420

电诈引流黑话的话语变异与源头治理研究

王博暄，李冠群，满俊维，赵哲*
北京警察学院，北京，中国
*通讯作者

【摘要】电信网络诈骗已形成引流、诈骗、洗钱前后衔接的产业化链条，引流是电信网络诈骗产业链的入口环节，黑话隐语是诈骗分子规避平台风控、围猎被害人的核心语言工具。本文以2445条涉案引流语料为对象，按“行业背景—问题发现—问题解决”思路，从宏观语类结构与微观词汇特征展开分析。研究发现引流话语以行动号召为接近必现语步，含明确导流指令者逾九成，三语步完整者占45.8%，且语步前置、省略形成结构变异；黑话可归纳为同音替换、拼音混写等八类变异，前五类合计占86.5%。本文从技术识别、宣防转向与协同治理三个维度提出源头治理路径。

【关键词】电信网络诈骗；引流黑话；话语变异；语类结构；源头治理
【基金项目】北京警察学院2026年度大学生创新训练项目（编号：2026市创大学生项目14）

1.行业背景与已有研究

1.1 行业背景：电诈引流的产业化与语言伪装

电信网络诈骗已成为当前发案率最高、对群众安全感影响最直接的侵财类犯罪。在持续高压打击之下，此类犯罪不断向线上迁移并呈现明显的产业化分工，社交聊天、短视频直播、电商购物等平台成为接触被害人的主要场域。从作案流程看，电诈大体可分为引流、诈骗、洗钱三个前后衔接的环节：引流承担圈选对象、建立联系的功能，诈骗负责实施侵害，洗钱完成资金转移。引流虽不直接骗取财物，却直接决定后续诈骗能否展开，是整条犯罪链条的入口。

为了在公开平台发布信息又不被察觉，诈骗分子大量使用黑话隐语、谐音替代、符号插入等经过改造的语言形式。与传统犯罪中零散、即兴的隐语不同，电诈引流黑话呈现出高度组织化特征：它由团伙内部分工生产，借助培训手册和社群快速复制推广，并随着平台风控规则的变化持续更新。这种语言伪装使以固定关键词为核心的筛查机制频频失灵，也给公安机关的线索发现和预警劝阻增加了难度。引流话语究竟如何变异、变异又造成了怎样的治理困境，构成反诈关口前移必须回答的现实问题。

1.2 已有研究现状及其不足

围绕电信网络诈骗的话语，学界已积累一定成果，大体可分为三条脉络。其一是诈骗话语的语用学分析。学者们从语用预设、语用身份建构、言语策略等角度切入，指出诈骗者通过突显有利身份、动态调整语言资源来获取信任，黑话与话术是身份建构的重要载体。其二是身份建构的机制解释。相关研究运用顺应论、社会符号学等理论[1-2]，说明虚假身份并非静态设定，而是诈骗者针对受话人的心理需求、在具体语境中协商建构的结果，非接触式犯罪的主要媒介正是语言。其三是反诈宣传与媒介话语研究，包括对主流媒体反诈报道的批评话语分析[3]，以及对沉浸式、互动式宣防模式的探讨[4]。

总体来看，现有研究仍存在两处明显不足：一是语料多取自诈骗短信、通话等已经进入诈骗环节的文本，专门针对引流环节、面向黑灰产招募与导流话语的语类分析较少[5]；二是语言学层面的规律提炼与源头治理的实务需求之间缺乏衔接，研究结论难以直接服务于监测与宣防实践。本文以语类分析为基本视角，同时关注宏观语步结构与微观词汇变异，先把“问题”识别清楚，再据此提出可操作的治理思路。

2.引流话语的变异规律与治理困境

本研究的语料为两千余条真实涉案电诈引流文本，来源于已侦破案件中提取的引流信息，内容涉及黑灰产招募、账号交易、代收跑分、刷单兼职、博彩推广等类型。语料已经过语步自动标注并辅以人工校核：语步

一交代业务范围，语步二陈述所谓优势与风险，语步三发出行动号召。在此基础上对黑话逐字标注，记录原形、变异形式、语义指向与语境，共得到 387 个有效黑话词条。下文依次从宏观语类结构、微观词汇变异和动态迭代三个层面，揭示引流话语造成的治理问题。

2.1 宏观结构问题

语类（genre）是特定交际目的反复出现而形成的话语类型，语步（move）则是构成语类、各自承担特定交际功能的结构单位。统计显示，三个语步的出现频率差异明显：行动号召语步覆盖面最广，在 2313 条语料中出现，占 94.6%；业务范围语步出现 1659 条，占 67.9%；优势与风险语步出现 1520 条，占 62.2%。这表明引流话语的交际目的高度集中—无论文本长短、业务类型如何，最终几乎都要落到“引导对方采取行动”上，行动号召是该语类唯一接近必现的结构成分。

三个语步构成一套围绕“建立可信—激发欲望—促成联系”展开的说服结构。业务范围语步以“业务名称”“项目介绍”等模板化开头，使信息看似正规商业告示；优势与风险语步中，逾三成出现“安全、稳定、靠谱、官方、老牌”等自我背书，大多承诺“担保、保障、包赔”，又以“零风险、低门槛、包教包会”降低门槛；利益诱导尤为普遍，其含有具体数字的收益承诺，还包含如“日赚、返利、佣金、秒结”等诱导词汇。

问题恰恰出在这套框架的“灵活变异”上。在语步组合上，三语步完整者 1119 条，占 45.8%；业务范围加行动号召的 492 条，占 20.1%；仅有行动号召的 389 条，占 15.9%；优势风险加行动号召的 313 条，占 12.8%。在语步顺序上，严格按“业务—风险—号召”规范排列的仅约两成，其余大量出现语步前置、穿插和回环；尽管如此，行动号召位于文本收尾的比例仍有很多，且绝大部分的语料含 Telegram 式“@账号”，形成稳定的“尾部导流”。语步的省略与前置使引流文本能够适应不同平台的篇幅与语境，伪装成公告、闲聊或评论，固定模板难以覆盖，这正是宏观结构层面的识别难题。

2.2 微观词汇问题

黑话是诈骗团伙为规避风控与监管而创造、改造的特殊语言符号，具有封闭性、动态性和规避性。从社会学角度看，它不只是交际工具，更是诈骗亚文化的载体：团伙成员凭借一套外人难以理解的符号系统建立内部认同、划定群体边界，并以此与治理者反复博弈。对这些词条按语义指向归类，黑话主要集中在平台名称与联系方式、金钱与交易、诈骗行为指称三个领域——恰是平台风控和监管的重点，也是诈骗分子最需要遮蔽的信息。

我们对 387 个黑话词条展开系统分析之后能够发现，电诈引流黑话主要存在八类变异方式。其中同音替换所占比例最高，比如将“微信”写作“薇信”或者“v 信”，把“钱”写作“米”或者“Q”。拼音混写占比为 19.4%，例如“加我”写作“jia wo”或者“+w”。英文替换占比是 15.2%，像“微信”写作“wechat”或者“wx”。字符拆分占比 12.8%，如同把“骗”拆分为“马扁”。同义替换占比 10.5%，像是用“米”“分”“豆子”来替代“钱”。语义转移占比 6.7%，比如“跑分”原本指的是电脑性能测试，后来转指利用银行卡走账。符号插入占比 4.3%。Emoji 替换占比 2.5%。排名位于前五的变异类型，累计在黑话变异总量中所占比例为 86.5%，这表明引流黑话的变异方式比较集中，主要是围绕发音、拼写、语义这三个维度来进行的。（见图 1）

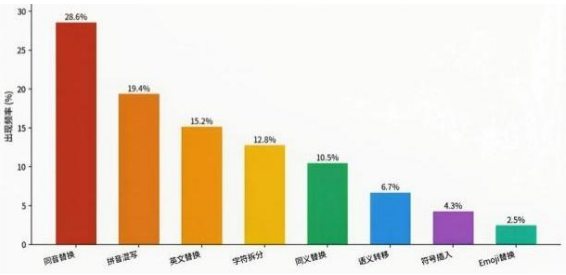


图 1.电诈引流话语主要变异类型分布

不同变异方式的规避机制各有侧重：同音替换与拼音混写利用汉字语音特点，读音不变而字形改换，人能读懂、机器匹配却失效；英文替换与字符拆分通过改变符号系统，避开以中文字符为基础的关键词匹配；同义替换与语义转移借用其他语义领域的词汇隐藏意图，其中语义转移隐蔽性最强，“跑分”“上车”在正常语境中并无异常，只有结合上下文才能识别。词汇层面的这种多维变异，使依赖字面匹配的关键词防线被系统性绕过。

2.3 黑话动态迭代使风控持续失效

然而黑话并非处于静止状态，它会随着

平台风控规则的改变而不断进行动态更新。黑话的迭代呈现出三大趋势：其形式变得越来越复杂，从单纯的同音替换朝着多重重叠变异的方向发展，语域也趋向开放化。黑话大量借助网络流行语、游戏术语等开放语域资源，比如用“上车”来代替加入诈骗群，这些词汇在正常的语境里并没有什么异常之处，其更新具有动态化的特点，热门黑话的平均生命周期只有 2 到 3 个月。通过跨时段对比研究可以发现，2024 年上半年高频使用的“薇信”“米”等黑话，到了 2025 年已经被“v 信”“豆子”等新形式所取代，替换率超过了 70%。这种快速迭代背后，存在着诈骗团伙内部的知识共享、分工协作情况。黑话的创造与传播一般由团伙里的“话术师”来负责，他们借助内部培训手册、社群交流等途径，能够迅速推广新的变异形式，进而形成了一套高效的黑话生产与传播机制。从知识社会学角度来看，黑话的迭代过程本质上属于一种集体性的知识生产、社会实践，这体现出诈骗亚文化在技术压力之下的适应性演化。

黑话的快速迭代给传统风控带来严峻挑战。本研究统计表明，仅仅使用单一同音替换就能避开约 65%的关键词筛查，要是采用多重重叠变异，规避率能够达到 90%以上。实测显示，把经过同音替换的引流话术输入主流平台风控系统，识别准确率从原文的 89%一下降到 32%。AI 技术被诈骗分子反向利用的趋势越来越明显，大语言模型可以批量生成高度拟真的引流话术，并且能依据平台反馈自动调整表达方式。从社会学方面来看，黑话与风控之间的动态博弈，本质上是技术变迁背景下社会控制与反控制之间张力的体现。

3.电诈引流的源头治理路径

针对前述三个层面的问题，源头治理应从技术、社会、制度三个维度协同发力，把已经识别的话语规律转化为治理能力。

3.1 技术路径

针对黑话迭代导致的筛查失效，关键在于建立基于语类结构与变异模式的智能监测模型[6]。在词汇层面，将已提炼的黑话词条与八类变异规则融入模型：针对同音替换建立音形映射、拼音混写做拼音还原、字符拆分做重组、语义转移引入上下文分析，改变单纯依赖字面匹配的做法。在语篇层面，重点识别“利益承诺＋尾部联系方式＋行动指令”的语步共现关系——即便关键词被替换，其结构模式仍可被捕捉，从而破解宏观结构的伪装难题。

在此基础上，建立黑话全生命周期管理与新词自动发现机制：通过对平台海量文本的异常模式聚类主动发现新词，缩短从出现到识别的时间差；构建跨平台语料共享渠道，一处发现、全网同步；对某类变异频率短时间骤升自动预警。技术应用还须守住法治底线，配套人工复核与申诉机制，防止误判正常表达，并严格保护用户隐私。

3.2 社会路径

公安机关可以参考拉斯韦尔“5W”传播模式，从五个方面重新建立反诈宣传模式。在传播主体上，推动从单一的公安机关转变为“公安+媒体+社会”多种主体，发挥主流媒体议程设置功能，培养网红民警、反诈达人等传播节点，形成多元协同的传播矩阵。在传播内容上，从泛化警示转变为精准解构，增加诈骗黑话识别、心理操控机制分析等内容。在传播渠道上，充分利用短视频、社交媒体等新兴平台，借鉴哈尔滨“中央厨房”模式实现内容一次生产、多渠道分发，提高官方渠道触达率。在传播对象上，建立易感群体风险画像，进行分层分类精准传播[7]。在传播效果上，建立系统的效果评估指标模式与反馈机制。

公安机关可以从认知、态度、行为这三个维度来进行测量并建立反诈宣传效果评估指标。在认知方面，要测量诈骗类型、黑话特征、防范方法的知晓率情况。在态度方面，测量风险感知、防范意识强度。在行为方面，测量信息分享、主动咨询、可疑信息举报等行为。通过问卷调查、平台数据监测、案件发案率变化等多种渠道来收集效果数据，并且定期对宣传策略进行调整。同时培育全民反诈社会支持网络，从社会资本理论的角度来看，邻里信息分享与互助网络是反诈宣传的重要补充内容。应该通过培训社区反诈骨干、建立邻里互助机制，以此来建立正式宣传与非正式传播相结合的全民反诈网络。

3.3 制度路径

电诈引流治理涉及多个主体，像公安机关、网信部门、通信运营商、金融机构、互联网平台、社会公众等，要建立协同治理的制度框架。有关部门应规范从线索发现、风

险研判到账号处置的全链条操作流程：线索发现环节明确平台巡查、群众举报、技术预警三类线索的录入标准；风险研判环节依据“语言指纹”特征体系制定标准化研判清单；账号处置环节严格落实实名制审核，建立跨平台账号关联处置机制。推动公安机关与互联网平台建立引流线索快速处置绿色通道，将平均处置时长从 48 小时压缩至 6 小时以内。强化基层民警对引流话术的识别能力，帮助民警掌握“看结构、辨身份、查黑话”的三步研判法，并定期更新。

各部门间要建立黑话治理的跨部门协同机制。公安、网信、通信运营商、互联网平台要建立常态化的语料共享和联合研判机制，每周汇总各平台发现的新型黑话变异，形成《电诈引流黑话动态周报》同步给各治理主体。建立黑话治理效果评估指标，涵盖发现时效、识别准确率、处置时长、复发率等方面，定期进行评估并向全社会公开。对于治理成效比较突出的平台给予政策激励，针对治理不力的平台依法予以处罚。

从社会学角度来看，电诈引流源头治理的关键在于建立“技术监测—社会动员—制度保障”三位一体的治理模式（如图 2 所示）。在技术方面，可以为社会动员、制度执行提供数据支持、智能工具。社会方面能够为技术迭代、制度优化提供群众基础、反馈渠道。制度方面可为技术应用、社会动员提供规则框架、资源保障。这三者通过“预警前置—精准阻断—宣传下沉—全民联动”的运行机制形成闭环：先是通过技术预警发现引流线索，接着由管理机制实施精准阻断，然后进行社会宣防以提高公众免疫力，并且公众反馈会反哺技术模型与管理流程优化。这样的格局既发挥了技术的效率优势，又体现了管理的规范作用，还激活了社会的内生动力与传播效能。

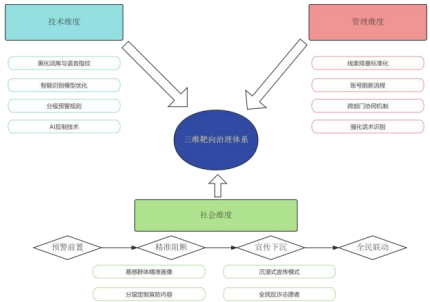


图 2. “技术–管理–社会”三维靶向治理体系框架

4.结论

本文沿“行业背景与研究现状—问题发现—问题解决”的逻辑，对电诈引流话语进行了系统考察。研究表明：在行业层面，电诈已形成分工明确的产业链，引流作为入口环节高度依赖语言伪装；在问题层面，引流话语宏观上以行动号召为接近必现语步、框架稳定却组合灵活，微观上可归为同音替换、拼音混写等八类变异、前五类合计逾八成六，并以快速迭代持续规避风控，单一同音替换即使约六成五的关键词筛查失效；在对策层面，须通过技术识别、宣防话语转向和协同制度建设三维并举实现源头治理。

需要说明的是，本研究语料主要来自已侦破案件，对尚未被发现的隐蔽引流覆盖有限，分析也以文本为主，图片、语音、视频等多模态话语及 AI 生成黑话的识别仍有待拓展，治理路径的实际成效亦需在实践中进一步检验，这也是后续研究应当推进的方向。

参考文献

[1] 包燕玲.《法治日报》电信网络诈骗媒介话语分析[J].声屏世界，2025，（5）：29-31.
[2] 石拓，曾昭龙，韩娜.融合大语言模型和语义聚类的电信网络诈骗引流话术文本分析[J].情报杂志，2025，44（10）：105-112.
[3] 刘卓娴，石拓，胡啸峰.电信网络诈骗警情要素抽取与模式挖掘研究[J].情报杂志，2025，44（6）：168-176+192.
[4] 公安部办公厅课题组.电信网络诈骗犯罪规律特点及对策建议——从受害群体视角的调研分析[J].公安研究，2025，（11）：43-52.
[5] 叶宁，赵云.“冒充公检法”诈骗中犯罪嫌疑人的身份建构：社会符号学视角[J].浙江工商大学学报，2022，（2）：17-27.
[6] 钱永红.网络电信诈骗话语中虚假身份建构的顺应性阐释[J].浙江外国语学院学报，2019，（5）：68-76+93.
[7] 刘力伟.“沉浸式”反诈话语模式构建研究[D].中国人民公安大学，2023.