

曲靖农特产品展示中心在上海市宝山区揭牌——

富源味道成“流量担当”

本报特约记者王园芬 文/图

近日,云南高原特产美食街暨曲靖农特产品展示中心在上海市宝山区泗塘集贸市场正式揭牌开业。这是沪滇协作三十周年之际,曲靖优质农产品在上海落地的又一常态化阵地,标志着两地消费协作从阶段性展销迈入长效化深耕的新阶段,“富源味道”登场亮相,吸引来众多当地消费者。

滇味飘香泗塘集贸市场

走进泗塘集贸市场近万平方米的街区,傣族花伞装点摊位,各色山货整齐陈列。展示中心内,宣威火腿、罗平蜂蜜、富源大河乌猪系列产品、富源魔芋、马龙野生菌菇等30余种特色产品琳琅满目;美食街上,菌子炒饭、牛肉汤锅米线摊位前排起长队。

“这个大河乌猪火腿切片直接吃,咸香回甘,和超市里卖的味道完全不一样!”家住上海市宝山区张庙街道泗塘新村的张阿姨一边试吃一边赞叹,“以前想买正宗云南特产得托朋友带,现在下楼遛个弯就能买到,价格还实惠。”展示中心开业首日现场人气火爆,牛肉汤锅米线摊主丰应海夫妇惊喜不已:“今天一早准备了400份米线,没想到刚到饭点就不够卖,紧急加了100多份,最后全都卖完了!上海市民特别喜欢这个味道!”

据了解,展示中心总面积超1000平方米,规划建设18个云南特色美食档口 and 标准化农特产品展销区,集中展示曲靖各县(市、区)的原生态农产品与特色美食,以“山海相逢,一味同心”为主题,打造集产销对接、便民消费、文化交流于一体的社区便民示范街区。

“曲靖人家”乡友驿站落地

与一般展销中心不同,展示中心还藏着一个特殊功能空间——“曲靖人家”乡友驿站。由曲靖市商务局统筹,联动人社、民政、工商联、共青团、妇联等多部门共同搭建,集消费帮扶、劳务对接、创业咨询、乡友交流、临时帮扶于一体的综合服务平台。

走进“曲靖人家”,极具曲靖地域特色的



当地市民争相购买大河乌猪系列产品。

文化墙醒目亮眼,内部划分茶歇区、洽谈区、多功能活动区,整体环境温馨雅致、功能完备。平台建立常态化服务机制,持续为在沪曲靖籍务工人员、创业青年、妇女群体推送家乡资讯、更新就业岗位、开展创业沙龙、提供政策咨询,定期组织乡友联谊活动。同时为遭遇临时困境的在外乡友,提供免费简餐、临时休憩、救助渠道对接等应急帮扶服务,全方位护航在沪乡友工作生活。

“以前想找老乡聊天、打听工作机会都没个固定地方。现在每周六下午有免费茶歇,还能看到家乡的就业信息,心里踏实多了。”在沪务工的富源籍群众贺贤强坦言,专属服务阵地的落地,为在沪乡友搭建了稳定可靠的“大后方”,推动消费、劳务、人才协作持续深化,切实解决了在外乡友的急难愁盼问题。

产地直供产销共赢

泗塘集贸市场作为宝山区核心便民农贸

市场,辐射周边多个成熟社区,消费氛围浓厚、客流稳定集中。此次曲靖农特展示中心落地运营,一改以往短期展销、阶段性推广的模式,采用长期运营、产地直采、现货直销的常态化模式,搭建起稳定长效的沪滇产销对接桥梁。

通过产地直达社区的运营模式,曲靖优质农产品省去层层分销环节,既保障产品新鲜原生态、质优价宜,丰富了上海市民餐桌选择,也为曲靖涉农企业、种养农户开辟了稳定广阔的东部消费市场,有效破解山区农产品销售渠道单一、推广受限等难题,实现云品入沪惠民、沪上消费助农的双向共赢。

“依托沪滇协作平台,我们打通曲靖产地直供上海零售通道,减少中间流通环节。展示中心常态化运营,让宣威火腿、富源魔芋等家乡特产稳定走进上海社区。同时,我们也希望借助这个窗口,持续打响曲靖农特产品品牌,带动家乡农户稳定增收。”上海沪滇缘供应链有限公司胡雄说道。

富源县综合行政执法局探索基层治理新路径

本报讯 为纵深推进城市管理进社区,富源县综合行政执法局积极探索基层治理新路径,通过创新联动机制、延伸服务触角、精准回应群众关切等举措,基层治理服务效能明显提升。

该局积极推动治理力量、管理职能、工作机制向社区下沉,出台“城市管理进社区”实施方案,择优选派30名业务精通、作风扎实的骨干力量,组建驻社区城管工作队,实现城区2个街道6个社区“城管工作站”全覆盖,依托社区服务中心,将政策咨询、投诉受理、简易处置等12项服务延伸至群众“家门口”,实现服务与群众“零距离”对接。并全力打造了太和社区“城管示范工作站”,5个城管驿站被稳步推动落地。在实践中逐步建立完善“一委一办一平台”城市治理工作体系。与此同时,该局建立“部门、街道、社区、网格”四级联动议事协调机制,推行“三事分流”,推动问题分层分类解决:社区驻点人员解决“小事”,执法大队协调“中

事”,分管领导统筹“大事”,形成“网格吹哨、分级响应、部门报到”的工作格局。

针对“富源县城清溪河沿岸存在违规搭建的建(构)筑物侵蚀河道空间,影响行洪安全、存在安全隐患、周边群众反映强烈”的问题,该局坚持“为人民管理城市”工作理念,以清溪河沿岸“拆违”为切入口,探索“党建引领、服务托底、共建共治”的工作机制,把“城市管理进社区”工作做到群众心坎上,用法治力度、民生温度、绣花精度,探索出一条依法治理与群众工作深度融合的新路径。通过“拆一片、治一线、美一城”的系统实践,清溪河沿岸存在的112处(其中违建建筑68处、私搭便桥44座)历史遗留违建问题处置工作稳步推进。坚持群众路线,把“对立面”变成“共同体”,群众参与后,把“我的河”变成了“我们的河”,目前清溪河沿岸城市更新工程正如火如荼地展开。

朱凤



工作人员到社区了解民意。朱凤 摄

科技

AI对网络安全的“双刃剑”效应日益凸显

新华社记者吴晓凌

自主行为突破边界

美国抱抱险公司系统遭到入侵事件表明,现有前沿AI模型已具备持续实施复杂网络攻击的能力。

这起失控事件发生在一项网络安全基准测试期间。包括GPT-5.6 Sol在内的多个模型识别并利用了第三方软件的一个“零日漏洞”,获取了互联网访问权限,在推断抱抱险公司可能存有完成测试所需数据和解决方案后,入侵了该公司系统,以“窃取”答案。

OpenAI在扩大调查后还发现了该公司其他AI产品突破内部隔离的情况。另一家美国AI企业Anthropic日前也承认,在审查约14.1万次网络安全能力评估记录后发现,其模型曾在多次测试中未经授权访问了3家机构的“生产基础设施”。

分析人士认为,当AI模型获得明确的目标以及充足的算力、运行时间和操作权限后,可能不会按照人类预想的方式完成任务,而会自主寻找路径绕过限制甚至“作弊”。

美国安全技术专家布鲁斯·施奈尔指出,AI智能体可能过于字面化地完成任务目标,却不能自然领会人类没有明确写入指令的限制。有研究发现,模型会利用任务、评分规则、提示词或评测框架中的漏洞取得高分,而没有真正展示评测原本希望衡量的能力。

随着前沿模型自主能力持续提升,这种偏差带来的风险正进一步放大。OpenAI在一份安全报告中说,早期模型遇到沙箱限制或环境障碍时往往停止工作,而新模型会不断自主尝试新办法寻求突破。

近期,美国两起与人工智能(AI)模型网络攻防能力相关的事件引发外界关注。美国开放人工智能研究中心(OpenAI)的模型在测试中失控并入侵了其他公司系统;苹果公司则因收到太多AI辅助生成的漏洞报告而限制外部提交的相关报告数量。

一方面是AI智能体为了完成任务自主突破边界,另一方面是AI辅助发现的潜在漏洞超过了人工审核能力。两起事件表明,随着AI网络攻防能力不断增强,其“双刃剑”效应日益凸显,急需匹配的安全约束、人工验证和风险处置机制。



位于上海徐汇区的上海创智学院,机器人制作奶茶。新华社发

安全措施急需完善

失控事件发生后,OpenAI表示已在修补漏洞期间收紧研究基础设施配置,并加强模型训练和评测过程中的隔离、监控、访问控制及安全保护。

不少企业和研究机构认为,应建立“多重防线”以提高防护系统的稳健性。OpenAI认为,对于可以自主运行数小时、数天甚至数周的AI智能体,只审核单个动作已经不够,还需要判断其完整行动轨迹会导致什

么结果。

谷歌深层思维公司提出,应建立系统级别的AI控制机制,包括沙箱、持续监控和分级授权;使用监督系统不断检查AI智能体的推理、行动和计划,在发现危险行为时进行拦截;对于可能造成严重后果的网络攻击等高风险行动,应从事后审查转向实时防护。

英国人工智能安全研究所建议,可能造成重大后果的操作应有人工

审核,限制AI智能体访问敏感资源,并保留在发现可疑行为时终止其运行的能力。

美国国家标准与技术研究所提出,应将AI智能体作为网络中的独立实体进行权限管理,为其制定专门的授权策略,只赋予AI智能体完成特定任务所必需的最低权限。

据媒体报道,多家AI企业的代表已受邀于4日与白宫官员会面,讨论AI安全问题。

漏洞处置压力陡增

此前业界认为,AI擅长大规模数据分析、模式识别和自动检测,可助力网络安全,使防御方受益。使用AI协助识别和发现漏洞已成为行业普遍做法,但如何充分利用AI提高网络防御能力正成为新的挑战。

英国《金融时报》报道说,AI正在迅速重塑网络安全领域的攻击和防御。苹果公司近期所发布操作系统更新中的安全修复数量约为之前更新的5倍。该公司表示,其中多个漏洞由AI工具帮助识别。

但AI识别漏洞的能力也给苹果公司带来“烦恼”。该公司2025年推出了一项机制征集关于其软件漏洞的线索,对于其中最严重、最复杂的威胁最高可支付500万美元奖励。苹果公司近日表示,由于其审核系统收到大量AI“幻觉”生成的“漏洞”报告,因此限制研究人员在一定时间内可以提交的报告数量。

《金融时报》报道说,意大利一家网络安全初创企业使用AI模型,在3个星期内发现了苹果笔记本电脑操作系统50多个漏洞,但由于苹果公司设置的限额而无法提交相关报告。该公司负责人阿尔弗雷多·佩索利表示,整个行业面临的现实是,维护人员和供应商正在被新发现的大量漏洞所“淹没”。

分析人士认为,OpenAI模型失控与苹果公司面临的情况看似没有直接关联,但两者反映出一个结构性矛盾:在网络安全领域,AI发现问题和采取行动的速度,正在超过人类验证、约束和处置的速度。如果治理跟不上AI迭代,原本用于提高效率的AI工具可能产生新的安全风险。

(新华社旧金山8月4日电)