大连重工董事长孟伟：

坚持“盈着干、算着干” 数字化转型应为客户创造价值

大连重工2026年上半年业绩预告显示，公司预计实现净利润3.51亿元至3.85亿元，同比增长12.47%至23.36%，延续了此前逆势增长的势头。2025年，这家大连制造业龙头企业同样交出了一份远超行业平均水平的成绩单：营业收入达155.17亿元，同比增长8.66%。而据中国重型机械工业协会数据，2025年行业规模以上企业营业收入同比下降2.8%。

带着这份成绩单，中国证券报记者走进大连重工，专访了公司董事长孟伟。孟伟坦言，企业竞争归根结底是质量和服务竞争，在行业供强需弱的调整期，坚持“质量上上、价格中上”能赢得客户信任，而数字化转型必须对准为客户创造价值这一根本目标。

● 本报记者 杨梓岩

大连重工装备集团为太行钢铁集团生产的取料机 视觉中国图文

业绩缘何逆势增长

过去四年，大连重工的业绩曲线与行业整体表现形成了鲜明对比。2025年，公司归母净利润达5.83亿元，同比增长17.11%，扣非后净利润同比增长20.28%，加权平均净资产收益率达7.65%，连续7年保持上行。更值得关注的是，公司经营活动现金流净额达7.74亿元，同比增长33.58%，对净利润覆盖倍数约1.33倍，呈现“收入—利润—扣非利润—经营现金流”逐级加速的特征。

孟伟将这一表现归结为企业确立的经营原则。四年来，孟伟没有选择多元扩张，而是提出了“四核”：聚焦核心技术、聚焦核心产品、聚焦核心客户、聚焦核心竞争力。“企业资源是有限的，必须解决发展边界问题。”他说。

在具体经营中，公司坚持“盈着干、算着干”，亏损的订单一律不接。过去四年，大连重工旗下18个利润中心无一亏损。2025年，公司海外新承揽订单金额达8.24亿美元，同比增长16%，与力拓签订全球框架合作协议，斩获摩洛哥近30亿元EPC项目。孟伟认为，国际化不是可选项。不走国际化道路，企业的规模做不大。

数字化转型成为必答题

在孟伟看来，传统装备制造业的智能化改造和数字化转型已经成为必答题，窗口期只有三到五年。“三五年后存活下来的企业，必定是大量应用机器人和人工智能技术、完成转型的企业。”

基于该研判，2024年6月起，公司与世界一流企业合作，用六个月时间制定了未来五年的数字化转型顶层规划，覆盖26个业务领域。

不过，孟伟也坦承转型的最大难点在于人的观念。“数字化转型的本质是转观念、转认识、转行为，不论新老员工都必须转变。”他坦言，数字化是数字世界的事，而企业基因一直是物理世界的机器设备。“传统装备制造业必须改变基因，从物理世界穿越到数字世界。”公司为此启动了IPD集成产品研发管理变革，借鉴华为等企业经验，将研发作为投资来管理，2025年研发投入强度达6.16%，是行业平均水平的两倍，产品研制周期缩短了20%。

与大连经济发展同频共振

大连重工近年每年新招本科及以上学历员工超过200人，仅2025年引进高层次毕业生140多人。孟伟说，新入职应届生三年内很难直接创造显著价值，但公司坚持自我培养，“只有人才辈出，才能业绩倍增”。这与公司正在推进的一系列管理变革相匹配——从LTC销售流程到集成供应链，都需要人才支撑。

谈到企业扎根的大连，孟伟的语气中多了几分底气与责任。在他看来，这座城市有着其他城市不可替代的硬核优势——公司主营的港机设备、大型船舶曲轴等产品，必须依靠自有码头才能交付。

“一台港机高度四五十米，单重一两千吨，必须整机在码头组装调试后滚装发运，陆路根本无法运输。”大连的港口条件、海洋经济资源，再加上市委、市政府在政策、土地、资金上的持续支持，构成了企业发展的独特“地利”。

正因如此，在大连迈入万亿GDP城市的过程中，孟伟明确表示“大连重工与大连经济的发展同频共振”。未来五年，企业将继续把根扎在这里，建设三大智能制造产业基地，目标直指全球重型装备行业的标杆。

来伊份总裁郁瑞芬：

探索“新鲜生活”价值边界

● 本报记者 乔翔

2026年7月，上海五角场万达广场，来伊份新鲜生活全球首店开业。开业以来，门店顾客数量居高不下，销售额屡创佳绩。

来伊份在下一盘怎样的棋？又看到了怎样的确定性机会？带着这些问题，中国证券报记者日前深入门店调研并与来伊份总裁郁瑞芬进行了深度交流，试图还原这家老牌零食企业的“新鲜”野心。

战略窗口显现

“这个时代给了我们非常清晰的画卷，我们一定要去答卷。”采访中，郁瑞芬用这样一句话定义了来伊份此刻所面临的行业局面。

郁瑞芬所说的“画卷”，是一个清晰的产业发展蓝图：近年来，中国大健康产业规模持续增长，消费者对新鲜、健康、好品质的要求不断提高。

国盛证券研报认为，新鲜零食能够满足市场质价比需求，有望构筑新的成长机遇。“首先是决策标准在升级，消费者开始关注配料表干不干净；其次，健康诉求在上升，短保、少添加已成为信任入口；最后，消费行为逐渐从囤货向即时消费转变。这为新鲜零食的发展提供了底层支撑。”一位业内人士表示。

对来伊份而言，此番在新鲜零食领域的动作并非临时起意。郁瑞芬在采访中透露，6年前公司就提出了“新鲜零食战略”，此后还参与制定了“新鲜零食团体标准”。

“我们之前一直在摸索和准备，这次算是厚积薄发。”郁瑞芬说这句话时，语气平静。在郁瑞芬看来，来伊份的每一次升级不是凭空而来，而是被市场和用户需求“推”着走。

具备先发优势

“新鲜生活店的核心，是公司深厚的供应链能力、运营能力以及近年来不断提升的信息化能力。”郁瑞芬在采访中直言。这背后的潜台词是：新鲜零食的竞争，表面上是店型的竞争，实质上是供应链效率等多维度的竞争。

“新鲜零食赛道的核心经营壁垒在于两端，一是短保损耗控制，二是跨区域品控能力。相较赛道内的初创品牌，来伊份具备先发优势，即供应链、成熟加盟体系与多业态协同。”郁瑞芬说。

先看供应链的“厚度”。来伊份与全国数百家核心食品工厂拥有近20年深度合作，华东供应布局尤为密集，超10万平方米物流中心、江浙沪皖核心区域每日到店冷链配送、AI销量预测系统支撑的数智化补货，这套成熟“底盘”正针对短保业态定向升级。

“新鲜零食门店的商品周期管理已不再按‘天’计算，而是按‘小时’计算。这就需要建立并完善多批次、小单量的敏捷补货机制，这样才有可能在高动销与低损耗间找到精准平衡。”郁瑞芬认为，这种“小时级”的供应链响应能力，正是短保业态最核心的盈利“命门”，也是新玩家短期内难以跨越的门槛。

再看信息化的“精度”。“来伊份在信息化上已投入近10亿元。我们一定要让这笔投入产生价值，必须借助AI驱动整个供应链的变革。”郁瑞芬表示。

按照郁瑞芬的设想，未来，公司会把AI嵌入到更多的流程、更多的智能场景中，用AI助力门店的运营管理。从早上开铺到营业结束，包括分析日报表、备货等，让运营更加精细、专业。

来伊份新鲜生活全球首店 本报记者 乔翔 摄

一场“长期主义实验”

从经营数据看，新鲜生活店开业后的相关数据表现不俗。但来伊份的野心，不止于一家“网红店”。

“我们不急于拓店，而是要先做透一家店。”郁瑞芬表示，从原料、生产、物流到终端上架，全链路严控新鲜、健康标准，这是新鲜生活店打磨的核心命题。

郁瑞芬表示，后续将坚持稳扎稳打，先通过首店直营跑通产品结构、运营标准、供应链履约的完整闭环。待单店模型验证成熟后，计划在上海核心标杆购物中心布局20家同业态门店，先深耕上海市场、打磨标准化体系，再逐步向外拓展。

在郁瑞芬的规划中，新鲜生活店的核心价值不仅是单店盈利，更在于“模型验证”。“计划落地的20家门店，前10家一定是由总部直营打标杆、定标准，把所有的体系流程跑通。之所以要先直营，是因为新鲜生活店有接近50%的极致短保商品，对管理要求非常高。”郁瑞芬说。

这种“先慢后快”的节奏，折射出来伊份对新鲜零食业态的清醒认知：短保商品的损耗控制、冷链配送的时效保障、现制产品的标准化……每一个环节都需要在实践中反复打磨，才能形成可复制的标准体系。

从更长远的目标看，新鲜生活店的意义远不止于门店的空间。这意味着，来伊份正在重新定义“门店”的边界，除了销售终端外，更是社区配送的前置节点、私域流量的线下入口、品牌体验的感知触点。

“在我们的计划中，私域与社区团购并非独立渠道，而是每家门店的自然延伸。这其中的核心逻辑是，把单店服务半径从‘到店客流’拓展至‘周边三公里全场景用户’。”郁瑞芬表示，公司计划以门店为前置仓，通过私域运营将打磨成熟的短保爆品反哺其他社区门店，消费者在来伊份App下单即可享受快速送达。

新鲜零食短期靠流量，中长期靠产品力与供应链管控，已成行业共识。此次涉足新鲜零食领域，来伊份希望构建的是一套能够自我迭代、自我优化的系统。在这个系统里，供应链的响应以小时计，门店的服务用AI赋能，对于加盟商的诉求必有回应。

在传统零食行业不断承压的当下，来伊份这家老牌企业在面对新趋势时选择以“自我革命”的方式继续探索发展路径。这条路能走多远，时间会给出答案。但至少，来伊份已迈出关键一步。

从被动防御升级为主动防护

业界热议AI安全护栏升级路径

● 本报记者 郑苹颖

近年来，人工智能（AI）技术快速发展，相关安全问题也引发各界关注。接受中国证券报记者采访的网络安全专家和企业高层表示，传统网络安全工作应融入AI能力，从被动防御升级为主动防护。此外，企业在融入AI能力的过程中，应确立安全先行、自主可控的建设原则，掌握数据安全与业务发展的主动权。

关注安全漏洞

近日，OpenAI在官网发布安全事件调查报告，披露其内部模型在评测期间发生的一起自主突破隔离环境的安全事件。

报告显示，这项测试的核心目的是检验模型能否识别安全漏洞，并将漏洞转化为可执行的攻击手段。测试过程中，尽管模型被部署在与外网物理隔离的沙箱测试环境中，但它通过投入大量推理算力，持续寻找访问开放互联网的路径，随后在程序包注册表缓存代理中发现了零日漏洞，并逐步抵达访问互联网的节点，最终尝试从人工智能开源平台Hugging Face生产数据库中直接获取测试答案。这一活动被Hugging Face的安全团队与智能体检测并阻止。

OpenAI在该事件中得出结论——“AI正在加速漏洞的发现和利用”。

中国信息通信研究院人工智能研究所安全治理部主任石霖对记者表示，过去行业谈论AI安全，大多聚焦于模型生成虚假信息、违规内容等层面；而本次事件中，模型仅为达成测试高分的单一目标，在无任何人工额外指令干预的前提下，自主挖掘零日漏洞、串联完整攻击链路、突破物理隔离环境、入侵第三方生产系统。这意味着具备自主决策、工具调用能力的AI智能体，已经拥有对现实数字世界造成实质破坏的能力，AI安全风险从“说错话”演变为“做错事”。

与此同时，事件也暴露了当前信息基础设施存在的安全短板与脆弱性。石霖认为，当前安全防护体系高度依赖已知的攻击方式，对AI可能带来的未知攻击方法和漏洞暴露风险认知存在明显局限，导致网络安全攻防两端的能力出现失衡。

OpenAI也在报告中表示，模型安全举措必须跟上模型发展进程。高级网络能力的开发必须与更强的保障措施和防御工具同步推进。

改变工作模式

在网络安全领域，渗透测试是一种常用的防护手段：通过主动对系统进行安全检测，模拟黑客攻击思路与手段，提前发现漏洞。如今，这一安全防护手段正在被AI技术改写。

绿盟科技集团CTO、高级副总裁叶晓虎对记者表示，从行业看，近年来利用AI技术进行网络攻击的事件在增加。同时，AI工具使得网络攻击的成本降低、速度提升。由于攻击链条变得复杂，传统依靠人工来进行网络防守、渗透测试已经无法达到防护要求，需要借助AI工具。

叶晓虎说：“网络安全是一项对抗性的工作，新的技术会带来新的应对手段。”他表示，结合AI基座模型，融入网络安全行业的专业知识库，加上Harness框架（智能体约束框架），形成的网络安全智能体工具可以投入实际应用。而在实际应用上，借助AI工具，还可以积累渗透测试数据，形成可复用的经验，将渗透测试变成一项常态化、持续性的工作。

同时，AI大模型还增加了渗透测试的主动性。绿盟科技集团技术专家刘红涛表示，过去基于静态检测规则，渗透测试过程中如遇到系统防护措施，会因阻断而无法达成渗透目标；而结合大模型推理能力，在渗透测试当中也会分析防护机制的薄弱性，尝试绕过以发现更深层的安全风险隐患。

AI技术应用将降低传统网络安全工作的成本。刘红涛表示，传统模式下开展一次渗透测试通常需要数天时间，针对复杂系统的测试周期更是长达十余天，单次投入成本高达数万元。而依托AI技术，当前单系统渗透测试的Token（词元）消耗量约为3000万至8000万，测试成本大幅压缩为数百元至数千元，让高频次、常态化的主动安全防御成为可行方案，也缓解了专业工程师人才供给不足的痛点。

刘红涛认为，AI赋能渗透测试的落地应用，将彻底颠覆传统网络安全服务模式。奇安信安全专家表示，用AI应对AI，已经成为安全行业的共识，通过代码安全智能体、AI安全网关等工具，行业正通过AI技术赋能传统网络安全。

设置护栏至关重要

在这次OpenAI模型导致的安全事件中，Hugging Face在官方复盘中表示，其最初尝试使用商业模型API进行事件分析，但请求受到安全策略限制，未能完成相关分析。随后，团队转而在本地基础设施部署由中国公司智谱开发的开源模型GLM-5.2，完成了整个取证分析流程。

Hugging Face在复盘中建议，企业应提前准备能够在本地基础设施运行的模型，以便在安全事件等关键场景下开展分析工作，同时保障敏感数据留存在企业环境内。

业内人士认为，这一案例反映出，随着AI逐步进入企业核心业务流程，企业越来越关注模型在真实生产环境中的部署能力、工程可用性以及完成复杂任务的能力。

奇安信安全专家认为，企业落地AI应用，需摒弃“先上线、后补漏洞”的传统思维，而应确立安全先行、自主可控的建设原则。AI并非普通应用软件，而是具备自主决策、独立执行能力的数字化主体，相当于企业的“数字员工”。对此，企业需参照人员管理标准，为AI工具建立专属身份认证、细化权限分级、明确行为规范，清晰划定AI可执行操作与禁止操作的安全红线。

同时，企业应摒弃单一防护模式，构建“人防+技防”协同的纵深防御体系，搭建从云端到终端、从网络到数据的立体防御网。在数据安全层面，企业应坚持核心数据本地化原则，针对核心数据与敏感业务，优先采用本地化AI部署方案，实现核心数据本地留存、不外泄，掌握数据安全与业务发展的主动权。

视觉中国图片