入侵劫持、物理风险不容忽视 具身智能ESG合规守住安全底线

当前，具身智能产业迎来从技术尝鲜向场景落地的关键拐点，工业机器人、服务机器人、巡检机器人等产品加速渗透生产生活场景，行业进入规模化应用前夜，而安全成为不可或缺的前置条件。

中国证券报记者梳理发现，云迹、优必选、极智嘉等一批已上市的具身智能企业披露的最新ESG信息显示，安全合规已成为ESG治理的核心议题，同时也成为资本市场衡量具身智能产业的长期成长性、商业化落地能力的关键标尺。企业、网络安全公司、科研机构正协同发力，构建全链条安全防护体系，为产业扩容筑牢根基。

● 本报记者 郑萃颖

单臂协作机器人抓取脏衣服放入洗衣机，左为单臂协作机器人，右为收衣服机器人。 本报记者 郑萃颖 摄

安全成为规模化发展前提

中关村东升国际科学园，云迹面向商用的新一代具身智能产品——单臂协作机器人，正在进行日常测试。这款机器人采用可自主定位、规划路线的轮式底盘，搭配视觉识别抓取机械臂，能够完成指定商品抓取、洗衣机开盖等全套作业。未来在酒店中，除了人们习以为常的送物机器人，这些新形态的机器人将与酒店智能系统互联互通。智能系统收到住客指令后，自主分配机器人前往客房收取待洗衣物，送至洗衣房，在单臂协作机器人辅助下完成洗烘，在指定时间送回客房；或是接到住客订购零食、饮品的需求后，单臂协作机器人从货架取货，再由送物机器人送至客房。

酒店中的机器人已经完成了与人们生活的数亿次交集。云迹发布的2025年年报显示，公司旗下的酒店机器人产品服务次数，已经从2024年的约5亿次增加到2025年的超7.6亿次，服务超4万家酒店及200余家医院。

随着具身智能机器人逐步走进大众生活，其安全问题也变得愈发重要。云迹CEO李全印认为，2026年将是具身智能行业从炫技到实用的分水岭，在封闭、低速、服务类场景，具身智能机器人的渗透率会在未来一两年内快速提升，“当几万台甚至几十万台具备感知和行动能力的机器人进入人们日常生活，安全就成为行业发展的前提条件”。

目前，具身智能从业者将行业安全问题主要归为物理安全、信息安全两大类。智身科技联合创始人、联席总裁刘宇龙感受到物理安全对于具身智能机器人发展的重要性。今年4月，在2026北京亦庄半程马拉松暨人形机器人半程马拉松赛场上，该公司自研的四足机器狗“铜锤 M1 Pro”以“关门兔”的身份完成陪跑任务。刘宇龙表示：“比赛过程中，会有运动员主动与机器狗合影，这就需要机器狗进行自主躲避，避免碰撞造成物理伤害。”今年6月，智身科技刚刚交付了1万台四足机器狗。随着机器狗在应急救援、景区巡逻等场景的落地应用，保障物理安全成为必要条件。

在业内企业的推动下，具身智能机器人正加速走进家庭，也让业界对信息安全问题展开了全新思考。5月25日，自变量机器人宣布其新一代机器人正式入驻真实家庭。自变量机器人CEO王潜此前在发布会上提到机器人领域面临的信息安全挑战。为了让机器人获得用户的信任，该公司对机器人进行视觉脱敏，即在设备端对视觉图像进行实时打码。“机器人‘看到’的是去除了用户个人特征的场景数据，而且用户不授权则机器人不开机，数据绝不共享给第三方。”王潜称，安全与信任是机器人走进家庭的必要前提。

如今，具身智能产品在生产、生活场景加速渗透：一方面，工业协作机器人、人形机器人、四足机器狗等越来越多地应用于3C生产、汽车制造、电力巡检、应急救援等场景，替代人工完成高危险性、高度重复的作业；另一方面，配送、清扫、安防等服务机器人广泛入驻酒店、医院、商超、居民社区，深度融入民生服务体系。

北京人形机器人创新中心CMO薛明认为，安全必须成为具身智能机器人商业化的前置条件，不安全的产品无法推向市场。行业普遍认为，2026年将是具身智能机器人从尝鲜到常用的拐点之年，安全不是创新的对立面，而是具身智能领域最坚固的商业底座。

安全合规考验治理水平

伴随具身智能行业成熟度提升，国内已有数家具身智能机器人公司上市，宇树科技科创板IPO申请已过会，一批具身智能明星公司，如云深处、乐聚正在冲刺IPO，行业资本化进程全面提速。资本市场对于具身智能企业的评价，不止停留在技术参数、产能规模、营收增速，安全合规也成为判断企业能否长期稳健经营的关键维度。李全印表示：“云迹作为一家在港交所上市的公司，实现安全不是一锤子买卖，而是运营连续性的一部分。安全是1，功能、效率、成本都是后面的0。”

梳理多家具身智能上市公司近期披露的ESG信息，不少与安全相关的议题被列为重要议题。

优必选在今年4月发布的2025年年报中披露了ESG报告章节，将产品质量与安全、信息安全与隐私保护识别为高度重要议题。公司明确，所有系统、产品与技术不得侵害人身安全、隐私权、财产权，同时通过保密分类、访问控制、数据加密及脱敏等方式管控信息安全。

越疆、云迹均在2025年年报中披露了ESG相关章节。越疆把质量管理、客户健康与安全、运营合规等与安全相关的ESG议题识别为重要议题。该公司表示，依托双冗余安全控制架构，搭建高危场景人机协作安全技术体系；IT部门协同业务部门，统筹监管数据安全与信息保护相关工作。云迹把产品质量与安全、数据安全与隐私保护列为最重要议题，对业务数据加密存储，AI语音通话加密传输，严控数据全生命周期安全。

极智嘉今年4月披露的2025年ESG报告，将产品质量管理、网络信息安全作为较为重要议题，并表示，公司把安全与合规作为前置约束嵌入研发全流程，通过“一键急停”“安全工衣”等技术手段，确保与机器人在同一区域办公的人类安全。

安全相关议题作为具身智能公司ESG治理能力的核心，成为资本市场衡量相关公司发展前景的重要标尺。

兴业碳金融研究院高级研究员吴艳阳表示，对比其他行业，具身智能行业最重要的ESG议题集中在S（社会）维度，包括数据安全与隐私保护、人机交互安全、AI伦理和供应链管理等方面。其中，数据安全与隐私保护的重要性正快速提升。机器人智能化程度加深使它们成为海量个人数据的采集终端，单台服务机器人日均采集数据量越来越大，而各国数据监管法规日趋严格，使数据合规成为机器人产业必修课。

此外，吴艳阳认为，人机交互安全的重要性也在显著提升。随着机器人日渐融入家庭、医疗、教育等敏感场景，它们给人体与用户心理带来的潜在风险愈发受到重视，安全事故可能对企业声誉造成毁灭性打击。AI伦理、供应链管理等ESG议题的重要性同样日益凸显，随着行业智能化水平快速提升，机器人自主决策引发权责归属、责任追溯等争议，将对具身智能时代的人机关系产生深远影响。

行业协作筑牢安全底座

中国信通院人工智能研究所安全与具身智能部主任石霖表示，具身智能机器人带来的安全风险，直接与物理世界的人身安全、财产安全绑定，一旦发生安全事件，其后果往往是不可逆的。

中国网络空间安全协会副理事长卢卫认为，具身智能将AI产品的安全风险进一步升级为系统性风险，通信层面的漏洞也将影响到物理安全。北京人形机器人创新中心CMO薛明举例称，在2025年安全极客大赛现场，两名白帽黑客现场演示了如何劫持一台机器人，并利用它通过近场通信成功“感染”另一台完全未联网、处于物理隔离状态的机器人同伴。最后这个机器人同伴走上舞台挥拳将假人击倒，整个过程不到三分钟。

薛明介绍，北京人形机器人创新中心通过推出慧思开物通用智能体平台，构建具身智能大脑和小脑的协同安全架构。在检测方面，北京人形机器人创新中心联合中国信通院、中国家用电器研究院等机构，以及小米、海信、海尔、国家电网等头部场景应用方共同成立具身智能测评实验室，推动建立统一、可落地的测评体系。薛明建议，应加速制定具身智能安全标准与规范，建立责任认定框架，将安全问题前置，让它成为与感知、决策、执行同等重要的核心基础要素。

云迹与网络安全公司奇安信合作，在6月2日发布“云迹高安全机器人”，面向央国企、政府等高安全等级业务场景，推出安全解决方案。李全印介绍，公司把“身份可信、行为可溯、数据防泄、合规可控”做成了标准化模块，植入每一台机器人。云迹参与起草了国家标准《服务机器人信息安全通用要求》等文件，把合规前置到研发环节。

绿盟科技集团副总裁曹嘉认为，要真正保障具身智能机器人安全，必须推动机器人厂商、大模型厂商、安全厂商、行业用户、监管机构五方协同，加快建立统一的安全架构，以及测评体系、合规标准体系，让安全成为具身智能机器人规模化落地的前提。

另外，具身智能机器人带来的安全挑战还体现在对事故责任的追溯上。英国约克大学助理教授戴晓天对记者表示，理论上，技术人员可通过融合传感器日志、操作指令历史、视频记录等实现事故全过程数据追溯，但会面临数据量巨大、数据完整性缺乏保障、多厂商设备间互联互通标准缺失等问题，未来应明确事故责任划分规则。来自汉堡大学多模态技术研究所的具身智能机器人安全领域专家张磊建议，应将操作记录的可追溯性作为产品合规要求与上市条件，建立明确的数据保留期和使用授权，并推动保险产品覆盖与机器人相关的责任风险。

零碳园区加速落地 “绿电+AI”助力减碳

● 本报记者 郑萃颖

近日，总投资逾164亿元的山西大同经开区零碳园区专项规划正式落地，国家级零碳园区的建设进入全面实施阶段。作为产业聚集区域，工业园区的绿色转型成为推动全社会绿色低碳转型的重要抓手，零碳园区建设有望推动这一进程加快。其中，绿电直连成为零碳园区建设的关键路径，而AI与数字化技术将为零碳园区建设助力。

零碳园区建设提速

6月2日，大同经开区网站披露了《大同经济技术开发区管理委员会关于〈大同经济技术开发区零碳园区专项规划（2026-2030年）〉的批复》，标志着山西省首个国家级零碳园区建设进入全面实施阶段。

根据规划，大同经济技术开发区零碳园区位于大同经开区通航产业园与高新产业基地内，规划面积379.74公顷，以新建“园中园”的方式推进零碳园区建设，规划期限为2026年至2030年。零碳园区建设总投资估算为164.08亿元。

规划提到，到2030年，大同经济技术开发区零碳园区全面建成，将形成以高比例可再生能源供电为核心，以高端先进电池产业集群为支撑，能源系统、产业系统、基础设施系统深度融合的近零碳运行体系。

友绿智库创始人、中国绿色建筑与节能专业委员会委员黄俊鹏表示，大同经济技术开发区零碳园区专项规划的出台，是国内零碳园区政策从顶层设计向地方实践演进的一个缩影。

2025年7月，国家发展改革委等部门联合发布《关于开展零碳园区建设的通知》，首次提出加快园区用能结构转型等8项重点任务，以及国家级零碳园区指标体系。2025年12月，《国家级零碳园区建设名单（第一批）》发布，包括北京经济技术开发区、天津经济技术开发区、山西大同经济技术开发区、上海临港新片区零碳湾等52个园区。

一位零碳园区资深从业者表示，目前我国的国家级、省级工业园区超过2500家，工业园区能耗占全国总能耗比例超过66%，工业园区碳排放量占全国碳排放总量超过四分之三，“园区实现零碳、低碳发展，将帮助全社会降碳”。

绿电直连为园区转型赋能

根据国家级零碳园区建设要求，衡量零碳园区的核心指标为单位能耗碳排放：年综合能源消费量在20万吨-100万吨标准煤的园区，单位能耗碳排放要求不大于0.2吨/吨标准煤；年综合能源消费量在100万吨标准煤以上的园区，单位能耗碳排放要求不大于0.3吨/吨标准煤。

“这一要求意味着，园区的煤炭消费总量、石油消费总量必须大幅降低，非化石能源消费占比要大幅上升，核心目的是推动园区能源结构转型。”上述从业者表示，要达到这一指标，一个高耗能产业聚集的园区至少有70%的用电要来自零碳电力，也就是俗称的绿电，其中来自绿电直连的比例不低于50%，其余部分可以通过绿电交易来实现。因此，绿电直连成为零碳园区建设的关键路径。

按照大同经济技术开发区零碳园区专项规划，该园区依托山西省能源局批复的绿电园区建设试点，规划建设522MW风光发电项目实现绿电直供，同时配置电化学储能设施及用户侧储能，用于平抑风光发电的波动性。园区还部署智慧能碳管理平台，通过“源网荷储”协同管理，打造国家级零碳园区示范标杆。

而在上海的临港新片区，零碳湾作为第一批公布的国家级零碳园区，正面临绿电供应的挑战。据报道，该园区计划在三年时间内，将使用绿电的比例从目前的20%提升至50%，同时通过配套储能设施来保障电力的稳定供给。

今年5月，国家发展改革委和国家能源局发布《关于有序推动多用户绿电直连发展有关事项的通知》，明确了多用户绿电直连的方式，为零碳园区等多主体用户场景提供了绿电直连的政策托底。所谓多用户绿电直连，是指风电、太阳能发电、生物质发电等新能源发电不直接接入公共电网，通过专用线路和变电设施向多个用户供给绿电。

AI技术破解零碳园区痛点

打造零碳园区进程中，智能化、数字化改造成为核心突破口。AI技术有效破解零碳园区建设难点，助力园区兼顾绿色低碳与智能高效发展。

南京福加智能科技有限公司技术总监刘冬表示，当前国内零碳园区建设仍面临多重现实瓶颈。首先是能源系统运行挑战，光伏、风电等间歇性新能源大规模并网，极易造成电网功率波动，而高端制造设备对供电稳定性要求尤其严苛，新能源供给的不稳定性与高端产业的高标准用能需求难以匹配。其次是能源与碳排放数据体系割裂，园区电力、碳排放数据分属不同管理部门，核算标准、统计口径不统一，难以实现全域数据统筹治理。另外，传统园区智能化管控能力不足，缺乏事前预警机制，而园区升级改造需要较大成本投入，面临资金压力。

刘冬认为，依托数字化与AI技术可有效破解上述行业痛点，推动园区内的数据互通，将园区能源调度升级到智能化新阶段。针对零碳园区建设需求，行业推出AI驱动的“源网荷储”综合解决方案，在能源供给端，整合风电、光伏、余热发电、生物质、地热等多元新能源资源，构建多元化绿色供能体系；在电网调度端，依托AI算法精准预测新能源发电波动与用户负荷变化，智能优化储能充放电策略，大幅提升绿电消纳率。同时借助AI技术，可实现碳管理的自动化、精准化，并对用能设备进行智能监测与运维，提升能源供给系统的稳定性。

从“存款为王”到“多元配置”：新周期下的财富配置思路和转变

广发证券 林思廷

随着今年宏观数据陆续披露，勾勒出当下财富管理的时代图景：央行一季度末数据显示，居民存款余额突破173万亿创历史新高；而今年4月CPI同比涨1.2%，银行一年期定存利率普遍在1%附近。手握存款求安全，或已不再是居民财富配置的最佳选择。我们正站在财富管理的历史转折点，从“存款为王”的单一时代，走向多元配置的新周期。

推动这一转型的核心，是几方面深层次因素的交织影响：一方面，近年来利率的持续下降，无风险收益的空间被大幅压缩；另一方面，国家层面持续推进“房住不炒”、规范平台经济、促进共同富裕等政策，改变了传统财富增值路径。资管新规的全面实施打破了理财产品刚性兑付，推动居民重新审视资产配置逻辑；此外，居民财富管理的目标从简单的追求“保值”向追求“增值”乃至“传承”演进。同时，中国正加速进入老龄化社会，这也催生了对于资产长期保值增值的需求。

多元配置的“金字塔”模型

面对众多资产类别，多元配置金字塔模型为普通投资者提供了清晰的思维框架，模型从下到上分为三层，可根据个人生命周期、财务状况、风险偏好、市场估值等动态调整。

第一层：稳健基石层

核心目标：波动小、收益确定性相对较高、流动性好。

配置工具：货币基金，是最基础的流动性管理工具。稳健基石层还可以考虑配置同业存单基金、低波动的银行理财等。

配置比例：不固定，如果刚工作不久，储备有限，或对于求稳的群体，这一层配置比例可以高达70%；如果已经积累了较多资产，且可以承受更高的波动，这一层比例可降至30%。关键是要覆盖个人的"资产稳健需求"。

第二层：平衡增长层

核心目标：在控制风险的前提下，追求比稳健基石层更高的收益。需要承担一定的波动，但波动要可控；追求的不是短期暴利，而是长期的复利增长。

配置工具：债券基金，特别是中短债基金和信用债基金，它们能提供相对稳定的票息收入，但存在一定的净值波动风险；红利指数基金，这是连接固收和权益的"桥梁资产"，底层是相关红利股票，在波动中既有可能享受股息收益，又有机会分享企业成长。

第三层：机会增值层

核心目标：分享经济成长的红利，追求更高的长期回报。

配置原则：高回报必然伴随高波动，配置遵循比例控制、长期持有。

配置工具：含权类资产，如股票型基金、偏股混合基金，可通过专业基金经理来参与股市；行业主题基金，如科技、消费、医药等，把握结构性机会。指数增强产品，在跟踪指数的基础上争取超额收益。还有一小部分另类资产，如黄金，起到分散风险的作用。

资产配置和财富管理理念转型

居民资产配置的核心转变，在于从传统旧思维升级为新的财富管理哲学，核心实现三大转向：从“追逐产品”转向“构建组合”，从“预测市场”转向“管理风险”，从“短期博弈”转向“长期规划”。

其中“追逐产品”的旧理念存在三大缺陷，一是存在幸存者偏差，投资者容易看到的是成功者，但无数失败产品已悄然消失；二是风格轮动和适应性，任何极致风格的产品都有其“顺风期”和“逆风期”。追逐当下热门，往往买在风格顶点，随即陷入长期低迷；三是风险集中，所有资金押注于单一资产、单一风格、单一管理人，风险极高。

因此，向“构建组合”的新理念转型尤为关键，核心行为模式是先明确“我的整体财务目标是什么？”，再以建筑师设计建筑的思路，打造结构稳健、生态平衡的投资组合，让每一笔投资、每一款产品，都成为服务于整体组合的“一块砖”。

这一理念的核心思想是不依赖任何单一资产的胜出，而依靠系统结构的稳健。承认自身无法始终选对市场最佳单品，但能通过系统设计，确保在任何市场环境下，组合中总有部分资产能发挥作用，平稳穿越周期。投资者可根据自身实际情况理性投资，市场有风险，投资需谨慎。

（登记投资顾问编号：S0260620070045）