

AI时代，“打补丁”安全逻辑行不通了

——访奇安信集团董事长齐向东

本报记者 齐旭

今年年初以来，OpenClaw(小龙虾)AI智能体掀起了“全民养虾”热潮，其引发的安全隐患也备受关注。近日举行的2026北京网络安全大会期间，奇安信集团董事长齐向东接受《中国电子报》记者采访时表示，智能体，本质上是一种软件，它帮人干活的前提是获取人类对系统操作的使用权限。一旦这些权限被滥用或误操作，极易引发重大安全事故。同时智能体自身存在安全漏洞，容易被黑客挖出而发起针对性攻击。因此智能体大规模落地应用的同时，要解决使用过程中的安全问题。

“AI大模型的发展几乎接近了极点，它的能力在快速地跃升，而黑客利用AI挖漏洞的能力也在迅速提升。”齐向东说道，网络攻击可能从“几年一遇”变成“一年几遇”，偶发性变成频发性。

“尤其是经过AI改造的生产系统和业务系统，在制造过程中一旦被攻击，企业将面临停产、停工，损失不可估量。”齐向东说道。

当前，具身智能正在各行各业展开应用。在齐向东看来，具身智能是一个连接大模型的智能体装在一个有控制单元的物体中，最典型的具身智能是智能驾驶汽车。

齐向东指出，由于具身智能的连接点很多，往往需要连接消费者的手机、语音控制模块、自身云端和IT系统，还要连接其他具身智能体实现互动，而且完全不在一类网络中，所以具身智能的攻击暴露面也非常多。

“AI时代的网络安全问题，直接变成业务安全问题和使用功能安全问题。”齐向东表示，解决具身智能的安全问题，如果还是以往安全



公司和产业公司互相独立地去做外挂，是解决不了的。需要产学研用深度融合、协同开发，在具身智能“大脑”里事先植入一个芯片、一款软件或一个模块，以此应对更为复杂的安全问题。具身智能也将成为奇安信公司未来主要的创新方向之一。

齐向东判断，未来网络安全行业的主要市场，将从政府运营单位转向更小规模、更大范围、更有活力的制造业和服务业，这些行业的企业应该加大安全投资，把安全预算提高到和其销售额可比的范围，确保企业的生产和业务安全。

伴随AI技术快速迭代，现有网络安全体系频频陷入应对乏力的窘境，在齐向东看来，其根源在于过往

安全建设多以单点布局、静态防护为主，缺少一体化架构与协同联动机制，难以处置频发多变的网络安全威胁。

“传统的‘发现漏洞-打补丁’逻辑已经行不通了，绝大多数的漏洞是打不上补丁的。”齐向东表示，网安企业要锚定攻防对抗能力，形成“三位一体”的纵深防御体系，这也是未来网安企业的竞争力所在。

据介绍，纵深防御体系是一体化的，把原有的安全资源分成“高、中、低”三位安全能力。其中，低位安全能力，就是人们所熟知的安全产品，负责执行，是“肌肉”和“手脚”；中位安全能力，是一个自主的安全智能体，负责运营指挥和调度，

是“神经”和“躯干”；高位安全能力，是大模型底座，负责情报共享和决策，是“智慧”和“大脑”。

齐向东进一步解释道，在这个体系中，低位安全产品要实施全栈AI化改造和赋能，让安全工具“好用、管用”；中位安全能力，要深度融入智能体的生态和技术，让它对安全的报警拥有100%的处理能力；高位安全能力，要实时不断地汇聚全球威胁情报以及自产威胁情报，以实战淬炼安全能力。

“只有构筑类似我国社会治安综合治理的网格化纵深防御体系，把内生安全自主、自适应、自成长的能力特性最大化，才能跑赢AI时代的攻防竞速。”齐向东说道。

OpenAI 回归机器人赛道 英伟达等同步入局

本报讯 记者杨鹏岳报道：6月1日，OpenAI 首席执行官萨姆·奥尔特曼通过社交平台宣布成立“OpenAI Robotics”团队，启动全栈工程师招聘计划，正式进军机器人领域。这是OpenAI时隔六年，再次重返机器人赛道，此前曾因数据瓶颈于2020年解散团队。

据悉，此次战略调整基于其内部名为“世界模拟(Worldsim)”研究项目的突破，由DALL-E和Sora模型的核心开发者阿迪亚·拉梅什领导，目标是实现机器人硬件与AI模型的协同设计。奥尔特曼表示，短期内，OpenAI聚焦开发协助技术工人建设基础设施的机器人；长期愿

景则是让每个人拥有可完成日常需求的个人机器人。

更多科技巨头入局，人形机器人行业有望重塑竞争格局。就在OpenAI宣布复活机器人团队的同日，英伟达也官宣牵手宇树科技，联合推出面向全球科研机构的人形机器人系统。5月底，比亚迪执行副总裁李柯首次公开确认，公司将入局人形机器人赛道。5月，特斯拉位于得克萨斯州超级工厂的专属Optimus机器人工厂正式动工，其规划年产能最高可达1000万台人形机器人。特斯拉CEO埃隆·马斯克多次提及，Optimus机器人未来的价值或将超越特斯拉整个汽车业务。

中国电信翼矩 AITMark2026 焕新升级

本报讯 记者张琪玮报道：日前，中国电信翼矩AITMark2026在2026世界电信和信息社会日系列活动上正式焕新发布，为产业提供“测试-诊断-优化”一站式AI终端专业评测服务。

自2025年发布业内首个AI手机智能度量化评测体系以来，翼矩AITMark持续输出行业洞察，本次升级聚焦三大亮点。一是评测体系全面扩容：基于人因工效学构建覆盖AI芯片、AI手机、AI泛终端及AI智能体的基准体系；优化AI手机GUI Agent评测能力，首发AI眼镜与天翼智屏评测基准，实现多场景、多维度专业化评价。二是测试系统

迭代焕新：升级后的翼矩AI终端测试系统支持200+评测场景，强化“感知-交互-决策-评价”智能闭环能力，实现多模态融合感知和升级，首发支持AI眼镜专业化评测，提升测试效率与精准度。三是发布范围拓展：AI手机评测从旗舰机型延伸至次旗舰，首次发布翼矩AITMark次旗舰AI手机场景智能评测报告，推动端侧AI能力普惠化发展。

未来，翼矩AITMark将持续迭代升级，向全品类、全场景、多维度评测体系演进，以专业标杆牵引技术创新与体验升级，加速端侧智能普及，与产业各界共筑AI终端繁荣生态，推动智慧服务惠及更多用户。

锚定新型工业化 培育新质生产力 奋力谱写上海产业发展新篇章

(上接第1版)

一是推动传统产业结构重塑。上海产业转型早，历经多轮结构调整，2/3以上传统产业企业已转型战略性新兴产业新赛道。未来五年，我们将实施传统产业焕新行动，聚焦产品增值、企业提效、绿色转型，“一业一策”加快转型升级。深化化工“降油增化”，推动炼油向化工转、化工向材料转。做强特种精品钢材，补齐关键钢材产品及装备、专业工业软件等短板弱项，支撑国家重大工程和高端装备需求。做优科技时尚的轻工名品，面向重点人群和重点领域加强新品研发，以优质供给创造新需求。以数字化提质增效，深入实施“AI+制造”，扩大人形机器人进厂应用，提升设备智联和生产环节数智化水平。以绿色化节能降碳，全面深化绿色制造体系和循环经济建设，深入实施绿色低碳供应链升级计划。到2030年，累计建设500个先进级智能工厂、300家以上国家绿色工厂。

二是强化先导产业战略引领。针对三大先导产业技术壁垒高、趋势变化快的特点，我们将着力提升创新策源能力，把握“IC+AI”产业深度耦合赋能机遇，夯实自主可控支撑力。集成电路全链创新，加快培育设计龙头企业，推动EDA/IP串珠成链，做强关键装备和材料。生物医药大IP引领，持续开展原创新药研制，加快发展高端医疗器械。人工智能创新融合，推动智算、语料、模型、应用、AI4S体系化布局，深入开展“人工智能+”行动，在人工智能发展和治理各方面走在前列。力争到2030年，三大先导产业规模均迈上万亿元台阶，制造业产值实现年均10%的增速。

三是加快壮大新兴支柱产业。针对六大新兴支柱产业从规模优势向质量效益跃升的发展要求，我们将依托市区协同着力做强主导产业特色集群。推动发展以新型智能终端、新型通信设备、具身智能为重点的新一代电子信息，以民用航空、高技术船舶、商业火箭、先进制造装备为代表的高端装备，以自动驾驶、固态动力电池为引领的智能网联新能源汽车，以基础材料、关键战略材料、前沿材料等高端应用为牵引的先进材料，以先进能源装备突破和全域示范为抓手的新能源及绿色低碳，以科技赋能和设计创新为驱动的时尚消费品等六大产业。未来五年，力争六大新兴支柱产业实现超万亿元新增量。

四是保持未来产业敏捷布局。“十四五”时期上海在全国率先布局未来产业，在多个前沿领域已形成多技术路线布局。未来五年，我们将聚焦低空经济、6G、可控核聚变、脑机接口、天基通感算等一批特色赛道，率先开展科技创新与产业创新一体规划、一体布局、一体推进，为上海产业赢得未来主动权和发展新蓝海。

五是推动生产性服务业与先进制造业融合互促。推动生产性服务

业赋能产业升级，发展“AI+生产性服务业”，推动工业设计、供应链管理、柔性制造、质量检测、设备运维等工业服务智能化发展，聚焦产业互联网提高工业品供应链一体化管理能力。培育“工赋”链主企业和数智化供应链服务商，支持“小快轻准”解决方案和行业Agent在生产一线部署，推动服务型制造向“硬件+软件+服务”一体化发展。发展“AI+专业服务业”，聚焦法律、会计、金融、人力资源等，开发特定工具链、工具包，更好助力拓展业务、提升效率，培育一批爆发力强的领军企业和高成长企业。突破软信息服务关键环节，做强AI Coding核心支撑，助力工业软件创新攻关。持续优化国产国用生态，加快布局行业智能软件。

统筹资源要素

构建友好适配的产业生态环境

一是优化产业空间布局。深化市区协同，迭代产业地图3.0版，推动各区差异化特色化发展，打造千亿元级特色产业集群。紧抓开发区管理制度改革机遇，优化园区开发运营机制，加强专业化服务、综合性配套，提升主导产业集聚度。支持中心城区依托“智造空间”建设，释放创新策源和时尚之都优势转化为实际生产力。

二是加大新质要素供给。聚焦硬核产业创新成果转化痛点，打造新型储能、人形机器人等50个专业化中试平台，建设一批场景试验场，加速工程化突破和产业化应用。主动把握工业智能变革趋势，加快超大规模智算集群和边缘智算中心布局。打造覆盖未来产业、先导产业和产业转型升级等全生命周期的产业基金体系。创新产业人才培养模式，实施卓越工程师培养行动，深化建设创芯学院、创智学院。

三是持续做优企业服务。完善招商服务一体化工作体系，推动惠企政策“免申即享、直达快享”，依托近6000名企业服务专员，构建“3公里服务圈”，通过服务包机制高效解决各类企业诉求。持续降低工业企业电、气、热、地、网、数等使用成本，实施工业用地保量控价。

四是加强长三角产业协同。以整机牵引提升产业链配套协作水平，协同打造长三角智能网联新能源汽车、大飞机、船舶与海洋工程装备等世界级产业集群，推进跨省域重大战略项目。聚焦高端装备、人工智能、生物医药等优势领域，实施长三角重点产业链强基韧链行动。

蓝图已绘就，奋进正当时。我们将牢记习近平总书记对上海产业发展的殷殷嘱托，胸怀“两个大局”，坚持“四个放在”，坚定信心、锚定目标、埋头苦干，一张蓝图绘到底，全力推进新型工业化、加快构建现代化产业体系，为制造强国建设作出新的更大贡献！

