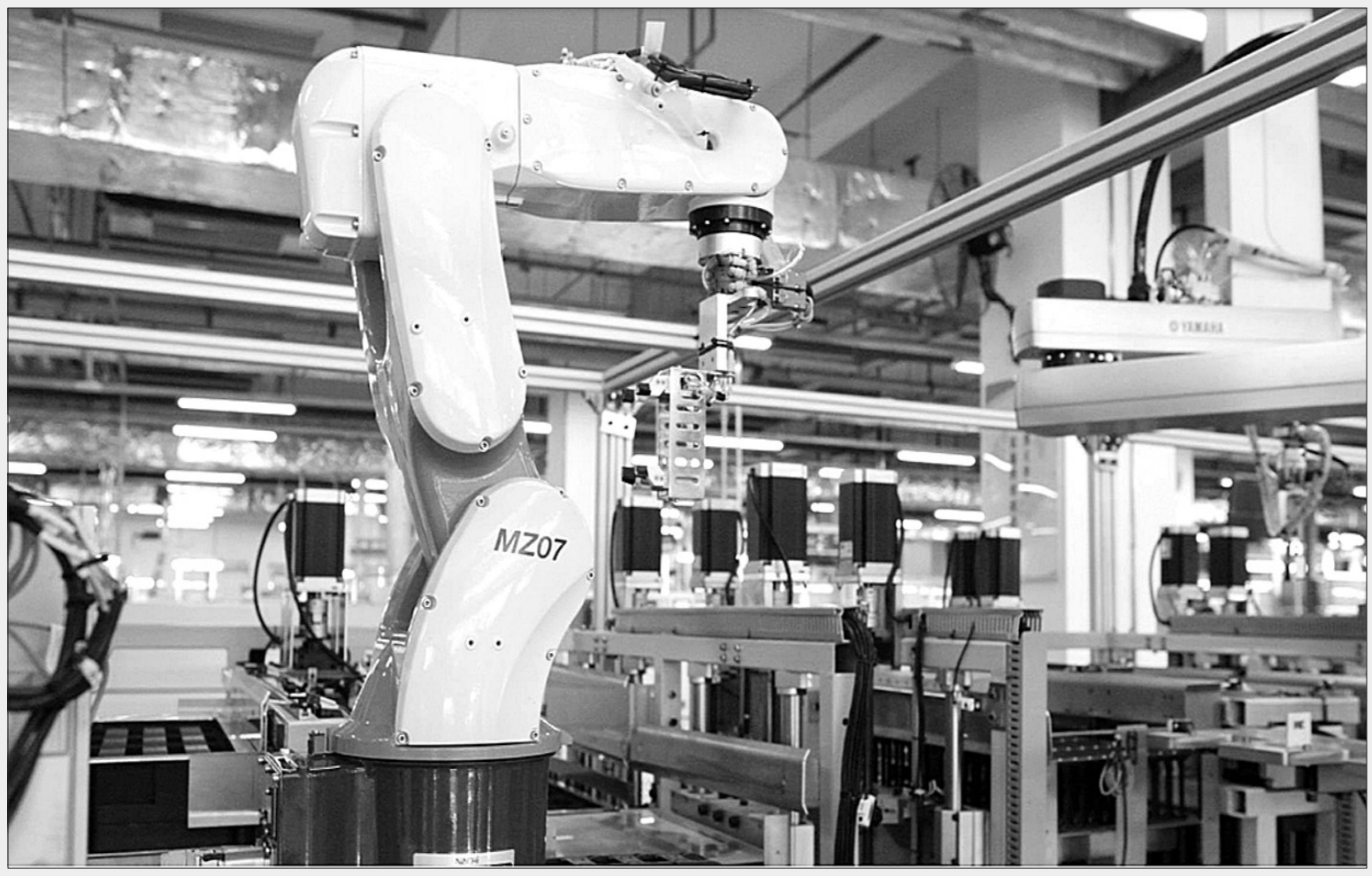


# 警惕GPT技术引发工业安全风险

本报记者 宋婧

生成式人工智能技术惊人的发展速度加剧了人们对网络安全的担忧。近来，ChatGPT引发的风波不断。意大利因数据安全问题成为首个宣布禁用ChatGPT的国家。紧接着，德国表示可能会追随意大利的脚步。加拿大也在对OpenAI展开调查。苹果、三星、SK海力士等越来越多的企业也开始禁用ChatGPT。7月6日，在2023工业安全大会上，多位专家表示，要警惕GPT技术在工业领域带来的安全风险。

## 工控安全面临前所未有的挑战

随着工业基础设施逐渐走向数字化、网络化、智能化，工控安全面临着前所未有的挑战。

工业控制网络是事关国计民生的关键信息基础设施。随着工业基础设施逐渐走向数字化、网络化、智能化，工控安全面临着前所未有的挑战。中国工程院院士邬江兴表示，以ChatGPT为代表的AI算法模型存在不可解释性、不可判识性和不可推论性，这让AI应用系统内生安全共性问题浮出水面。现阶段，人类科技能力尚不能彻查复杂系统漏洞后门问题，AI应用系统算法模型安全与网络安全问题相互交织且难以分而治之。因此，AI应用系统以及相关数字基础设施极易成为网络攻击的高价值目标，造成社会性灾难。

随着技术的发展，网络攻击手段也在不断地演变和更新。机械工业仪器仪表综合技术经济研究所所长欧阳劲松表示，人工智能技术的深度应用会让危险源、威胁变得更加难以辨识，网络物理攻击路径越发难以预测，功能安全措施与信息安全措施也会越来越难协调。

北京天地和兴科技有限公司副总裁伍泽广也指出，随着新技术的迅猛发展，安全范围越来越广，安全边界逐步“上浮”和“下沉”。以GPT为代表的生成式人工智能技术将大幅降低黑客攻击工控专有协议的技术门槛。OT（运营）环节的漏洞将会持续增加，工业企业数据资产面临的安全风险也会越来越大。

## 用好AI技术 提升网络安全水平

网安大模型的应用，就有助于安全从业者更好地理解和预测网络安全威胁。

“GPT类大模型技术在各行业的应用生态快速形成，这对工业安全而言是一把‘双刃剑’。”和利时信息安全研究院有限公司战略规划总监李季表示，GPT技术将带来包括隐私保护、资源消耗等问题，也会进一步加剧对抗性攻击、自动化攻击、恶意利用等安全隐患。但同时这项新兴技术也将为网络安全产业带来更多产业机遇。比如，网安大模型的应用，就有助于安全从业者更好地理解和预测网络安全威胁，开发出更加高效的安全工具和方案，提升网络安全的智能化水平。

实际上，任何一项新技术的出现都将带来安全风险，工业安全建设还是应该从基础设施出发。烽台科技（北京）有限公司副总经理、灯塔实验室技术负责人王启蒙指出，工业场景基础设施数字化能力整体偏弱，数字化改造有待改善。CT（通信）与OT（运营）需求对接不足，导致工业应用端到端可靠性难以保障，芯片、模组、终端产品的工业特性有待增强。

工业数据价值越高，安全风险往往越大。北京交通大学信息安全系主任、教授王伟指出，工业数据普遍存在访问控制权属关系不清晰，易产生非法盗用、非法篡改等问题，借助Web3.0，工业互联网时代的工业数据可以变成可确权、可支配、可流通的内容，并最终形成可靠、安全、合规的工业数据安全保障平台。

王启蒙建议，复杂环境下，应针对工业网络控制设备、业务服务器、工业主机、网络设备、安全设备产生的标识数、状态数据、事件数据、运维数据、实时数据等，根据内置的工业分级分类知识库对采集的数据进行分级分类，并根据数据等级进行对应安全策略处理。

值得一提的是，网络分析公司Similarweb统计的最新数据显示，2023年前5个月，ChatGPT全球访问量环比增幅分别为131.6%、62.5%、55.8%、12.6%、2.8%，增长幅度明显下降；6月份ChatGPT的访问量环比下滑9.7%，为其推出以来首次。作为这轮生成式人工智能风暴的中心点，ChatGPT的访问量持续下滑引发了人们对于人工智能泡沫的担忧。

据不完全统计，国内10亿级参数规模以上的AI大模型已超80个。多位专家指出，国内通用人工智能产业已出现过热端倪，一旦技术无法有效落地、市场期待无法实现，“泡沫”就有可能破裂。

# 欧盟Top5工业机器人国家装机量占比达70%

**本报讯** 记者**宋婧**报道：伴随全球工业自动化、智能化浪潮加速，工业机器人正进入加速成长期。近日，国际机器人联合会（IFR）发布的最新报告显示，欧洲的工业机器人呈上升趋势：欧盟（EU）27个成员国在2022年安装了近7.2万台工业机器人，同比增长6%。国际机器人联合会（IFR）主席Marina Bill表示：“欧盟内采用机器人最多的五个国家是德国、意大利、法国、西班牙和波兰，在2022年，它们约占欧盟境内安装的所有工业机器人的70%。”

作为欧洲最大的机器人市场，德国2022年安装了约2.6万台机器人（同比增长3%），占欧盟总安装量的37%。意大利是仅次于德国的欧洲第二大机器人市场，2022年安装了近1.2万台（同比增长10%），创历史新高，占欧盟总安装量的16%。法国机器人市场在欧洲排名第三，2022年总装机量为7400台，同比增长15%。西班牙的年安装量增长了12%，达到3800台。波兰的机器人安装已经持续了9年的强劲增长，2022年安装量达到了3100台，这是继2021年3500台的新峰值之后第二好成绩。

从行业应用来看，汽车制造领域是欧盟工业机器人最大的应用行业，占比达到了38.7%。例如，德国2022年新部署的机器人中有27%安装在汽车行业。法国汽车行业的工业机器人装机量达到1600台，代表了21%的市场份额。西班牙汽车行业安装了900台工业机器人，同比增长5%。

业内专家分析称，汽车制造业一直是工业机器人最主要的应用市场，也是最早应用自动化和部署机器人的行业。在欧洲能源供应紧张、汽油价格大幅上涨的背景下，欧洲新能源汽车需求有望逐步扩大，从而带动工业机器人需求增长。

从技术趋势来看，欧洲工业机器人逐渐从早期的流水线作业为主导向灵活、个性化定制方向发展，新型通信与人工智能技术正在为工业机器人的未来发展带来新的可能。

意大利机器人与自动化协会主席丽兹雅·莫菲诺（Rezia Molfino）表示：“当机器人和人需要共同合作时，他们必须先理解对方。设计者面临的挑战是，如将人类以及人的决策方式和解决问题方式建模，从而提高人机协作的效率。与人类协作的机器人需要通过训练完成特定任务，解释这些任务要达到的目的，尤其是任务存在争议或难以理解时，以确保长期负责任地利用机器自主性。这些都是当前市场需要的技术，欧盟将在这些领域加大投资力度。”

# 我国首个开源桌面操作系统“开放麒麟1.0”正式发布

**本报讯** 记者**赵晨**报道：近日，我国首个开源桌面操作系统“开放麒麟1.0”正式发布，标志着我国拥有了操作系统组件自主选型、操作系统独立构建的能力，填补了我国在这一领域的空白。

“开放麒麟1.0（openKylin 1.0）”是通过开放操作系统源代码的方式、由众多开发者共同参与研发的国产开源操作系统。据悉，该系统由国家工业信息安全发展研究中心等单位指导推动研发，其发布将有助于推动面向全场景的国产操作系统迭代更新，为政务、金融、通信、能源、交通等关系国计民生的重要行业提供基础安全保障。

据了解，“开放麒麟1.0”默认搭载6.1+5.15双内核，完成20+操作系统核心组件自主选型升级，并新增许多新特性，修复超千个bug，进一步提升系统整体稳定性和兼容性。

# 中国电子PKS生态与华为鲲鹏生态合并

**本报讯** 记者**赵晨**报道：7月12日，中国电子信息产业集团有限公司与华为技术有限公司决定合并鲲鹏生态和PKS生态，共同打造同时支持鲲鹏和飞腾处理器的“鹏腾”生态。

据悉，当前基于鲲鹏处理器、飞腾处理器的服务器和PC机已规模应用于政府、运营商、金融、电力等与国计民生相关的行业的核心业务场景，形成鲲鹏和PKS两大主流生态。面向未来，合并后的“鹏腾”生态将充分发挥中国电子和华为的各自优势，双方将秉承“优势互补、协同合作、产业共建、繁荣生态”的原则，在产业标准、伙伴计划、技术协同、开源贡献、市场营销、人才培养等多方面展开深度合作。

记者了解到，构建统一的“鹏腾”生态，将简化生态伙伴的软硬件适配和认证，便于开发更多形态的产品，覆盖云、数据中心、边缘、PC终端等全场景，基于“鹏腾”生态的产品与解决方案也将更加丰富，有机会在更多的行业中应用落地，更好地赋能千行百业的数字化。

计算产业是数字和智能时代的战略性基础产业，是构建现代产业体系、实现高质量发展的重要支撑。据介绍，中国电子与华为将联合产业链各环节开展深度合作，开创通用算力新格局，为数字化转型构筑坚实根基，推动数字经济高质量发展。

# 京东言犀大模型亮相 应用将分三步走

**本报讯** 记者**邱江勇**报道：7月13日，京东在北京推出京东言犀大模型。与通用大模型相比，这一源于产业、服务产业的大模型，融合70%通用数据与30%数智供应链原生数据，致力于深入零售、物流、金融、健康、政务等知识密集型、任务型产业场景，解决真实产业问题。对于大模型的应用实践，京东提出了明确的“三步走”规划。

为夯实产业应用，京东推出了一套大模型的完整工具，包括支撑大模型研发的基础设施——言犀AI开发计算平台、向量数据库、混合多云操作系统云舰、高性能存储平台云海、软硬一体虚拟化引擎京刚等核心产品。

依托京东言犀大模型，以及京东在产业和供应链侧的优势，京东还发布了两大服务平台，包括全新升级的优加DaaS和言犀智能服务平台，以及面向零售、金融、城市、健康、物流五大领域的行业解决方案。

京东集团CEO许冉表示，大模型真正实现自己的价值，一定是在产业应用中。在她看来，大模型的价值=算法×算力×数据×产业厚度的平方，前三个指标固然重要，但技术在产业场景落地应用，创造实际价值才是关键。

产业场景是京东非常擅长的领域。京东作为一家新型实体企业，拥有包括零售、物流、科技、健康、工业、产发等丰富的产业布局。这为京东积累下每年数百亿条优质交互数据，训练言犀大模型的数据库，就由70%通用数据和30%供应链原生数据组成。

对于大模型的应用实践，京东也有明确的“三步走”规划。目前，京东云已经基于内部实践构建了通用大模型；到今年年底这段时间，京东将经由高复杂场景大规模锤炼，迭代出扎实的产业服务；预计在2024年年初，会将大模型能力向外部严肃商业场景开放。目前，京东已经走到第二步，并在内部取得了丰富的实践成果。

据悉，京东从很早就开始布局大模型。2021年，京东就推出十亿级模型K-PLUG，2022年推出百亿级模型Vega，本次大会则展示了千亿级模型。

在大会现场，京东演示了将通用大模型转化为健康产业大模型的操作。通常，客户完成这套流程，从数据准备、模型训练到模型部署，需要十余名科学家花费一周的时间。但利用言犀AI开发计算平台，只需要1~2名算法人员，在数分钟内就能完成。通过平台模型加速工具的优化，还能节省90%的推理成本。

# 欧盟委员会发布Web 4.0和虚拟世界战略倡议

**本报讯** 日前，欧盟委员会发布了《Web 4.0和虚拟世界的倡议：在下一次技术转型中领先》的一系列文件。

欧盟委员会表示，互联网正在以极快的速度发展，在当前正在取得进展的Web 3.0（主要特点是开放、去中心化和赋予用户权利）之外，Web 4.0将允许数字世界和真实对象、环境之间的整合，并增强人与机器之间的交互。因此，Web 4.0将是带来无缝互联、智能和沉浸式世界的主要技术转型。

欧盟委员会预期，到2030年，全球虚拟世界的市场规模将从2022年的270亿欧元增长至超过8000亿欧元。毫无疑问，虚拟世界将影响人们的生产、生活方式，既会带来机会，也需要解决潜在的风险。

欧盟委员会强调，Web 4.0和虚拟世界倡议主要包含四个支柱。前三个与2030数字化欧盟项目的支柱目标一致：人才技能、商业环境和公共服务。第四个支柱，包含了算力、云等基础设施建设的目标，以及Web 4.0和虚拟世界的开放性和全球治理。

在官方文件中，欧盟委员会副主席、主管反垄断的竞争专员维斯塔格也表示：“我们希望确保Web 4.0成为所有人的一个开放、安全、可信、公平和包容的数字环境。需要将人置于中心，根据欧盟数字权利和原则来塑造这些规则，以解决关于隐私或者错误信息的风险。”（区 文）