

ChatGPT 变革与风险

美国人工智能公司OpenAI的大语言模型ChatGPT在推出约两个月后,1月已达到1亿月活跃用户,成为历史上增长最快的消费者应用程序。相关专家预计,ChatGPT不仅是新一代聊天机器人的突破,也将为信息产业带来巨大变革,但由此带来的学术造假、技术滥用、舆论安全等风险亦不容忽视。



德国培训乌军 操作“豹2”坦克

据新华社电 德国国防部发言人13日说,德方已开始培训乌克兰士兵操作“豹2”主战坦克,培训预计持续数周。

德新社援引德国国防部发言人的话报道,德方对乌方士兵的培训主要在德国联邦国防军位于西部城市明斯特的训练场进行。

据德国《明镜》周刊先前报道,德方将把通常耗时数年的培训缩短为6至8周的高强度培训。鉴于时间大幅缩短,培训将限于这一主战坦克的基本操作。

上月25日,迫于美国等盟国压力,德国政府宣布向乌克兰提供14辆“豹2 A6”主战坦克,并同意盟友向乌克兰提供德国制造的“豹2”坦克。同日,美国总统约瑟夫·拜登宣布将向乌克兰提供31辆“艾布拉姆斯”主战坦克。

另据德新社报道,德国还在培训乌方士兵操作“黄鼠狼”步兵战车。

俄罗斯外交部发言人玛丽亚·扎哈罗娃上月27日指出,西方方向乌克兰提供坦克不会使局势向有利于乌方的方向转变,而会将西方与俄罗斯的对抗推向新高度。俄总统新闻秘书德米特里·佩斯科夫也说,西方决定向乌克兰提供坦克等武器,使得乌克兰局势的紧张程度加剧。

专家称

俄计划2027年 开建自己空间站

新华社莫斯科2月13日电 塔斯社13日援引俄罗斯空间站总设计师弗拉基米尔·科热夫尼科夫的话报道说,俄计划于2027年发射相关舱段并开始组建自己的空间站。

科热夫尼科夫也是俄“能源”火箭航天集团副总设计师。他说,目前包括“能源”火箭航天集团在内,约有30家企业参与俄空间站的初步设计工作,此项工作按计划将于2023年完成,随后相关建设工作也将展开。预计2027年俄将开始组建空间站,并发射首个舱段——能源舱,2028年至2030年将陆续发射连接舱、出入过渡舱、基础舱和专用舱等。

科热夫尼科夫指出,未来俄空间站将采用机器人、虚拟现实和增强现实等技术,以辅助宇航员在轨作业。

俄罗斯国家航天公司总裁尤里·鲍里索夫今年1月24日在莫斯科出席一个航天领域会议时曾表示,俄计划在今年4月12日展示空间站的最终外观。他去年7月曾表示,俄将在2024年后退出国际空间站项目。

■ 相关新闻

ChatGPT火爆背后有法律风险

存在信息泄露等隐患
借热度“搭便车”牟利行为大量出现

ChatGPT的问世掀起了新一轮人工智能浪潮,但其使用过程中可能涉及的法律问题不容忽视。

存在信息泄露风险
可能侵犯知识产权

公开资料显示,ChatGPT可以总结研究论文、回答问题、生成可用的计算机代码,甚至快速通过美国医学执照考试、沃顿商学院的MBA期末考试、司法考试。一些医学论文预印本和已发表的文章甚至正式赋予了ChatGPT作者身份。

但在受访的法律人士看来,ChatGPT的强大功能也隐含着不少法律风险。

“ChatGPT对信息、数据来源无法进行事实核查,可能存在个人数据与商业秘密泄露和提供虚假信息两大隐患。”北京盈科(上海)律师事务所互联网法律事务部主任谢连杰说。

谢连杰说,ChatGPT依托海量数据库信息存在,其中包括大量的互联网用户自行输入的信息,因此当用户输入个人数据或商业秘密等信息时,ChatGPT可能将其纳入自身的语料库而产生泄露的风险。虽然ChatGPT承诺删除所有个人身份信息,但未说明删除方式,在其不能对信息与数据来源进行事实核查的情况下,这类信息仍然具有泄露风险。

“对于这类隐患,平台应充分提示用户其生成的内容可能为虚假信息,且在其生成疑似违法信息时进行拦截或提示用户存在安全风险。”谢连杰说。

泰和泰(重庆)律师事务所高级合伙人朱杰说,ChatGPT在建立语料库、生成文本时,如果使用并非公开的开源代码、使用开源代码商用未办理许可证或者未按照许可证的要求实施的,可能会导致侵权。他解释说,这类人工智能主要是通过挖掘人类日常交流以及文本,进而统计分析,因此,对于一些受著作权保护的文本、视频、代码等,如果没有经过权利主体的授权,直接获取复制到自己的数据库中,并在此基础上修改、拼凑,极可能侵害他人的著作权。

谢连杰提到,ChatGPT的文本数据挖掘技术可能导致其在他人享有著作权的作品中“借鉴”部分内容。对于这部分

内容,若不能构成我国著作权法所规定的“合理使用”的情形,则可能引发侵权纠纷。

借势贩卖租赁账号
“搭便车”山寨频出

ChatGPT走红后,由于服务端对中国大陆的IP有限制,无法注册使用,其账号一时在国内多个网购平台、社交平台上销售火热。在某电商平台上售卖成品账号的店铺,一天之内多达万人付款,价格最低1.68元。

记者在一家名为“ChatGPT账号供应商”的店铺购买了账号,商家随后私聊发来账号和密码,并特别标注输入时需要复制粘贴,还附有登录教程。登录后,记者发现这是一个多人共享账号。记者发现,某电商平台上,多数商家售卖的都是共享账号,而单人定制账号或者代注册账号的价格往往更高。

近日,多个电商平台对ChatGPT账号销售行为进行了查禁,相关关键词被屏蔽。记者先前账号订单显示商品不存在,进入到商家界面发现,所有的商品均已下架。

然而,记者在社交平台上搜索“ChatGPT账号”等关键词发现,仍有不少网友在提供代注册、有偿账号分享服务,围绕ChatGPT账号展开的买卖行为仍在野蛮生长。

朱杰认为,这种买卖行为可能构成非法经营等违法行为。ChatGPT的正版服务由境外机构提供,而未经我国相关部门批准利用VPN跨境提供经营活动是被明确禁止的,所以国内这些代问、代注册的商家以营利为目的,搭建或使用VPN进行注册账号,未办理国家相关行政许可,擅自经营买卖国外账号,可能会受到行政处罚甚至刑事处罚。

ChatGPT账号价值被炒作成商品以外,借其名称热度“搭便车”的牟利行为也大量出现。朱杰说,“山寨”软件打着正版软件的旗号进行宣传,欺骗消费者进行下载,可能构成虚假广告;同时,“山寨”软件使用的名称及标志如与正版软件相同或相似,引导他人误认为与正版存在特定联系,可能构成反不正当竞争法中规定的商业混淆行为。 据《北京晚报》

新一代操作系统平台的雏形

多语言撰写充满想象力的诗歌,编写可运行的程序,快速生成论文摘要,自动制作数据表格,纠正文章中的语法和表达错误,把一周大事写成新闻综述……ChatGPT不仅能理解很多人类问题和指令,流畅展开多轮对话,也在越来越多领域显示出解决多种通用问题的能力。

ChatGPT还轻松通过一些对人类难度较高的专业级测试:它新近通过了谷歌编码L3级(入门级)工程师测试;分别以B和C+的成绩通过了美国宾夕法尼亚大学沃顿商学院MBA的期末考试和明尼苏达大学四门课程的研究生考试;通过了美国执业医师资格考试……业界形容它的诞生是人工智能时代的“iPhone时刻”,意味着人工智能迎来革命性转折点。

北京智源人工智能研究院院长黄铁军接受记者专访时说,人工智能领域的过去十年是深度学习的十年,但产业总体上并没有出现移动互联网和

引发新一轮人工智能科技竞赛

ChatGPT的问世正在人工智能领域引发新一轮科技竞赛。北京时间2月8日凌晨,微软推出由ChatGPT支持的最新版本必应搜索引擎和Edge浏览器,宣布要“重塑搜索”。微软旗下Office、Azure云服务所有产品都将全线整合ChatGPT。

北京时间2月7日凌晨,谷歌也发布了基于谷歌LaMDA大模型的下一代对话AI系统Bard。同一天,百度官宣正在研发的大模型类项目“文心一言”,计划在3月完成内测,随后对公众开放。阿里巴巴、京东等中国企业也表示正在或计划研发类似产品。

人工智能大模型领域的全球竞争已趋白热化。黄铁军认为,ChatGPT未来有望演变成新一代操作系统平台和生态。这种变革似移动互联网从个人电脑到手机的转化,大部分计算负荷将由大模型为核心的新一代信息基础设施接管。这一新范式将影响从应用到基础设施各层面,引发整个产业格局的巨变,大模型及其软硬件支撑系统的生态之争将成为未来十年信息产业焦点。

值得注意的是,ChatGPT有时会“一本正经地胡说八道”,存在事实性错误、知识盲区和常识偏差等诸多问题,还

云计算级别的爆发,“ChatGPT的出现,具有划时代意义,大模型+ChatGPT已形成新一代操作系统平台的雏形”。

黄铁军说,ChatGPT在技术路径上采用了“大数据+大算力+强算法=大模型”路线,又在“基础大模型+指令微调”方向探索出新范式,其中基础大模型类似大脑,指令微调是交互训练,两者结合实现逼近人类的语言智能。ChatGPT应用了“基于人类反馈的强化学习”训练方式,用人类偏好作为奖励信号训练模型,促使模型越来越符合人类的认知理解模式。

“这样的AI可帮助人类进行真实创造,尤其是帮助人类提高创造效率,比如提高获取信息的效率或提出新颖想法,再由人解决其真实性问题。创造效率的提高将产生巨大效益和多方面影响,可以改变世界信息化格局。”中国科学技术大学机器人实验室主任陈小平对记者说。

面临训练数据来源合规性、数据使用的偏见性、生成虚假信息、版权争议等人工智能通用风险。多家全球知名学术期刊为此更新编辑准则,包括任何大型语言模型工具都不会被接受为研究论文署名作者等。

“学术论文的署名作者须满足至少两个条件,其一是在论文工作中做出‘实质性贡献’,其二是能承担相关的责任。目前这两个条件ChatGPT(以及其他AI系统)都不满足。”陈小平说。

ChatGPT也有应用在舆论信息战方面的潜力。加拿大麦吉尔大学研究团队曾使用ChatGPT前代模型GPT-2阅读加拿大广播公司播发的约5000篇有关新冠疫情的文章,然后要求其生成关于这场危机的“反事实新闻”。

“针对这些问题,需要我们在发展技术的同时,对于ChatGPT应用边界加以管控,建立起对人工智能生成内容的管理法规,对利用人工智能生成和传播不实不良内容进行规避。同时加强治理工具的开发,通过技术手段识别人工智能生成内容。这对于内容检测和作品确权,都是重要前提。”北京瑞莱智慧科技有限公司副总裁唐家渝说。

据新华社北京2月13日电