

# 让人工智能拾起初心

## ——对话三位人工智能领域专家

◎本报记者 倪麟

随着《全球人工智能治理倡议》的发布,人工智能治理再次引发全球关注。作为引领科技革命和产业变革的战略力量,人工智能的广泛应用正在深刻改变经济社会结构,重塑人们的生活方式。

同时,人工智能也带来改变就业结构、冲击法律与社会伦理、侵犯个人隐私等问题,对政府管理、经济安全和社会稳定乃至全球治理产生深远影响。

当前,该如何让人工智能拾起初心,平衡其安全和发展?科技日报记者近日邀请中国工程院院士沈昌祥、百度首席技术官王海峰、清华大学人工智能研究院视觉智能研究中心主任邓志东共同探讨,解读人工智能发展之路。

### 本意:人工和智能,孰轻孰重

**记者:**人工智能定义最早出现在1956年达特茅斯会议上。从各位的实践来看,人工智能是什么?

**沈昌祥:**人工智能是指通过人类设计和编程,使智能机器能够完成各种复杂任务,从而取代传统人工角色。

**王海峰:**人工智能是研究和开发模拟、延伸和扩展人类智能的理论、方法、技术及应用系统的科学。现阶段,人工智能已成为引领新一轮科技革命和产业变革的战略性技术,正驱动第四次工业革命,将人类社会带入智能时代。

**邓志东:**从实践来看,人工智能具有模拟人类解决各种复杂任务的能力。

**记者:**随着ChatGPT等产品的出现,有人认为人工的作用逐渐被智能取代,也有人认为智能只是辅助人工的工具。在各位所属领域中,对于人工智能中“人工”与“智能”的权衡有何看法?

**沈昌祥:**智能机器是由人类智慧演化而来的智能产品,能根据人类的喜好和需求,提供个性化服务。智能机器的所有动作和行为都是由人类编程和控制的,不可能完全脱离人类的掌控。

**王海峰:**人工智能发展要“以人为本”,增进人类福祉。以大语言模型为代表的人工智能技术飞速发展,文心一言、ChatGPT可与人对话、辅助创作,提升人们的工作效率与生活体验。本质上它仍是提升生产力的工具,能替代人类完成部分工作,也创造了更多工作机会。未来,人类将作为管理者,人工智能将辅助人,与人协同,提高工作效率,激发创造力。社会各界应对人工智能抱有正确认知和合理期待,推动人工智能发展,使其更好地为人类服务。

**邓志东:**“人工”与“智能”密不可分。人工智能指机器模拟实现的人类智能,两者关系应称为人工智能与人类的关系。短期内,通用人工智能是辅助工具,帮助人类完成挑战性任务。长远来看,交互式人工智能会推动人类与智能体“共融”,迈向“人一机融合发展”的新新世界。

### 定位:增长产品还是基础设施

**记者:**人工智能对相关行业发展产生了重要影响。各位更倾向于将人工智能视为增长产品还是基础设施?

**沈昌祥:**人工智能最初是独立产品,后来被集成为具有各种功能的设备。当设备相互连接、协调工作时,就形成了系统。这些系统的集合和互相作用,构建起人工智能基础设施的框架,为我们提供各种产品和服务。

**记者:**在人工智能基础设施建设领域,各位对哪个方面特别关注?

**沈昌祥:**安全问题至关重要。人工智能衍生出人工智能自身失误、智能硬件被恶意袭击以及机器人智能行为失控等重大风险。需对这些问题加强研究和防范,构建由法律、战略和制度等组成的安全可信的保障体系,确保人工智能基础设施的安全、稳定、可持续运行。

**王海峰:**我长期关注深度学习平台和大模型。深度学习平台相当于智能时代的操作系统,处于人工智能技术体系的关键核心位置。深度学习呈现标准化、自动化、模块化的特征,推动人工智能进入工业大生产阶段。随着深度学习技术的普及和预训练技术的突破,大模型已成为人工智能发展的主流方向,具有效果好、泛化性强、研发流程标准化的特点,正成为人工智能技术及应用的新基座。

**邓志东:**从文本单模态的基础大型语言模型到原生多模态大型语言模型,需要解决高水平人工智能通用大模型的API接入问题,推进“以我为主”的人工智能基础设施建设,包括人工智能芯片与云服务、开源框架生态建设等。视觉智能领域需要打好基础,从国家层面推进人工智能基础设施建设,补短板,赋能从基础与基座大模型到垂域模



图为在第六届进博会技术装备展区,观众与傲银机器人互动。新华社记者 张建松摄

型的开发与应用。

**记者:**企业在利用人工智能时可能面临双重需求。能否根据经验,谈谈在这种情况下,企业如何将人工智能的价值最大化?

**沈昌祥:**企业需要考量产业数字化、数字产业化以及社会智能化的需求,充分利用人工智能技术,提升生产效率和服务质量。同时,应高度重视人工智能领域的人才培养与引进,推动技术研发,以保持技术领先地位。还应加强与其他行业的合作,不断探索新的商业模式和应用场景,为社会提供更便捷、更高效的服務。

**王海峰:**百度既是人工智能基础设施建设者,也是人工智能技术创新引领者。以飞桨深度学习平台、文心大模型等为代表的人工智能技术,已成为智能时代的重要基础设施,赋能制造、能源、农业等领域,带动新技术、新产品、新业态等的发展。大模型产业落地,可采取“集约化生产、平台化应用”模式,即具有算法、算力和数据综合优势的企业将模型生产的复杂过程封装起来,通过低门槛、高效率的生产平台,为千行百业提供服务。文心大模型支撑大量AI原生应用的开发,重构现有产品,“从0到1”构想出全新产品,构建人工智能原生应用生态,推动经济社会高质量发展。

**邓志东:**以多模态大型语言模型为代表的通用人工智能产业的发展,尚处于产业早期。不同企业应有不同侧重,人工智能头部企业要对标具有国际一流水平的基础、基座大模型产品,缩短高性能AI芯片的国际差距。中小企业要积极开展人工智能价值与应用产品的研发,着重于应用场景多样性、落地速度与商业模式创新。

### 风险:无处不在,谁更堪忧

**记者:**当前人工智能风险普遍存在吗?请结合具体案例说明。

**沈昌祥:**人工智能风险与网络安全密切相关。网络安全是人工智能发展的底座,其风险度=脆弱度×威胁度,其中脆弱度来源于图灵计算原理缺少攻防安全理念、冯·诺依曼体系结构缺少防护部件和重大工程应用无安全治理服务三大原始性缺失。这使得网络空间极其脆弱,受网络攻击的风险性增加。2021年5月7日,美国最大的成品油管道运营商科洛尼尔管道运输公司(Colonial Pipeline)受到勒索软件攻击,被迫关闭其美国东部沿海各州智能化供油网络,美国政府宣布美国17个州和华盛顿特区进入紧急状态。

**王海峰:**从历次工业革命来看,驱动科技革命和产业变革的技术,无论是机械技术、电气技术、信息技术,还是当前的人工智能技术,在为人类带来巨大价值的同时,也会带来一定的风险。但随着科技的进步,人类有足够的力量控制风险,充分发挥新技术的价值。

**邓志东:**通用人工智能的发展速度已超出大多数人的预期。只要通用人工智能发展,其风险就必然会普遍存在。从法律、伦理、隐私到就业等,各个领域与赛道,千行百业都面临重写、重塑的挑战与风险。

**记者:**在自动驾驶、智慧医疗和人脸识别等特定领域,人工智能风险是否更为突出?

**沈昌祥:**自动驾驶、智慧医疗和人脸识别等技术,一旦出现问题将威胁到人类的生命安全和财产安全。IT系统

设计不能穷尽所有逻辑,利用逻辑缺陷挖掘漏洞进行攻击的风险一直存在,传统“封堵查杀”难以应对未知恶意攻击,找漏洞、打补丁的思路也不利于整体网络安全,需要通过由被动防御转为主动免疫的方式来降低人工智能特定领域风险。

### 治理:安全与发展能否相向而行

**记者:**随着人工智能技术的持续发展,数据隐私和安全、能耗等问题日益凸显。你们认为,针对这些问题应先发展后治理还是边发展边治理?

**沈昌祥:**要注重治理和发展平衡。应构建主动免疫可信计算新模式,打造计算部件和防护部件为核心的并行体系结构,建设可信安全管理中心支持下的主动免疫的防护框架,实现主体、客体、操作、环境可信动态访问控制,确保体系结构、资源配置、操作行为、数据存储、策略管理可信。以此达到让攻击者进不去,非授权者重要信息拿不到,窃取保密信息看不懂、系统和信息改不了,系统工作瘫不成和攻击行为赖不掉的防护效果,全方位维护人工智能安全。

**王海峰:**要坚持发展和安全并重的原则,保障安全的同时支持和鼓励创新发展。只有持续发展人工智能技术,才能在发展中发现、解决问题,把握科技竞争主动权。

**记者:**从各位的经验来看,行业或者企业应如何预防人工智能潜在的安全问题?

**沈昌祥:**要科学严谨分析研究,坚持自主创新,掌握核心竞争力,把握主动优势。要以具有可信计算功能的国产软硬件设备为基础,在完备的法律、战略和制度的支持下,尽快建立起完整的可信计算产品链,打造安全可信人工智能新生态,筑牢数字经济发展基石。

**王海峰:**正确认识人工智能潜在的安全问题。任何一项技术的发展和运用,都会带来潜在的安全问题,而人工智能作为驱动科技革命和产业变革的战略性技术,其安全问题更加受到关注。技术安全问题,可以用技术的手段来解决;产业安全问题,一方面政府应支持自主可控的人工智能技术及应用,另一方面应建立健全相关法律法规,推动产业在合适尺度、明确标准之下发展人工智能技术及应用。

**邓志东:**人工智能发展在安全问题上尚存在许多不确定性。行业或企业需要边走边看,大胆深入,小心布防,造福人类。

**记者:**人工智能治理已经上升为国际竞争合作的重要议题。在推动人工智能治理国际合作方面,各位有何见解?

**沈昌祥:**应认真贯彻落实《全球人工智能治理倡议》,从创新发展、安全保障、治理三个方面着手,全方位保障我国人工智能基础设施,并积极走出国门,与全球伙伴共建网络空间命运共同体。

**王海峰:**人工智能领域的研究本身是开放合作的,人工智能治理是其研究热点之一,各方都很关切。来自全球学术界、产业界的专家学者,都可以通过开源社区、项目合作、学术会议、专题研讨等多种方式开展交流合作,贡献智慧。

**邓志东:**人工智能的治理与国际竞合,已超越了学术与产业,需要更强而有力的国际合作,以期取得国际共识,尽快构建具有约束性、一致性、平衡性的国际规范。

### 热点追踪

## 《中央企业社会责任蓝皮书(2023)》发布

科技日报讯(记者刘园园)记者12月24日从国务院国资委获悉,《中央企业社会责任蓝皮书(2023)》在京发布。

国务院国资委社会责任局副局长汪洋对《中央企业社会责任蓝皮书(2023)》进行了解读:在坚持创新驱动、支持科技自立自强方面,中央企业把科技创新作为“头号工程”,完成了一系列具有标志性、引领性的创新成果,助力科技强国建设。2022年,中央企业研发投入首次突破1万亿元,同比增长9.8%,工业企业研发投入强度超过3%,科技创新驱动力进一步增强。

《中央企业社会责任蓝皮书(2023)》显示,在践行绿色发展,服务“双碳”目标实现方面,中央企业积极布局新能源产业,创新开发绿色低碳新产品,着力建设绿色循环产业体系,探索延伸零碳产业,努力实现从源头到终端减碳。2022年,中央企业万元产值综合能耗比“十三五”末期下降6.09%,达到“十四五”规划目标进度;万元产值二氧化碳排放比“十三五”末期下降11.5%,超过“十四五”规划目标进度。此外,《中央企业社会责任蓝皮书(2023)》从其他多个方面对中央企业2022年度社会责任履行情况进行了系统分析与总结。

“总体来看,中央企业在责任实践、责任管理、责任沟通方面积极作为、创新探索,积累了较为丰富的经验,取得了较大成绩。同时,我们也要看到,一些中央企业在将社会责任理念全面融入企业战略、重大决策、经营管理和文化建设方面,仍有较大的提升空间。”汪洋表示。

## 工信部组织开展网络安全保险服务试点

科技日报讯(记者崔爽)记者12月25日获悉,为加快推进网络安全保险新模式落地应用,工信部近日印发通知,组织开展网络安全保险服务试点工作。

据悉,结合现阶段我国网络安全保险现有险种,本次试点险种主要包括网络安全财产类保险和网络安全责任险两大类。网络安全财产类保险,主要保障因网络安全事件造成的第一方直接损失以及因此产生的技术服务费用。内容包括直接物理损失、营业中断损失、数据资产重置费用、硬件改善成本、应急处置费用,以及因网络安全事件导致的公关费用、法律费用等。

网络安全责任险类保险,主要保障因网络安全事件引起的对第三方个人或机构需要承担的赔偿责任。内容包括数据泄露责任、网络安全事件责任、媒体侵权责任、外包商相关责任、产品责任或技术服务职业责任等。

通过开展网络安全保险服务试点,可以完善网络安全风险管理,建立健全网络安全保险流程机制,促进网络安全保险规范健康发展。同时,创新一批网络安全保险产品,培育一批优质网络安全保险机构,形成一批可复制可推广的网络安全保险解决方案。

## 院士专家建言医学基础学科发展 交叉融合是孕育新发现的“摇篮”

◎本报记者 张佳星

近年来,随着全球基础医学和生命科学的迅猛发展,医学领域原创性成果频出。如何进一步强化基础研究前瞻性、战略性、系统性布局?如何通过体制机制改革和建设高水平支撑平台,促进基础研究在交叉融合中取得颠覆性进展?在日前召开的第二届中国医学基础学科发展大会上,多位院士专家围绕加强基础研究、从源头和底层解决关键技术问题等方面建言献策。

中国工程院副院长、中国工程院院士、中国医学科学院北京协和医学院院校长王辰指出,医学融合了多学科的“基因”与“骨血”。应当全面加强医学与理学、工学、社会科学、人文科学的联系与研究,形成融通局面。

颠覆性医学基础研究成果的产出与生命健康和经济社会息息相关。“在具体研究中,我们要面向前沿,抓住共性难题开展研究。”中国工程院院士曹雪涛认为,得益于基础理论的突破,知识的革新、手段的提升,医学正在以前所未有的趋势向前发展。

以走入临床阶段的治疗性基因编辑技术、合成生物学技术为例,这些为医疗行业、医药产业带来变革的技术中凝结着大量跨学科、多领域基础研究新发现。

交叉融合是医学基础研究中孕育新发现的“摇篮”。在中国工程院院士张学看来,搞基础研究要从学术角度打破传统的学科边界。遗传学专业的研究人员不能只懂遗传学。例如,研究神经系统遗传病,还要懂电生理和发育生物学。因此,应形成跨学系、跨学科的联合研究机制。

人才是第一资源。构筑跨学科人才基础是实现医学与多学科深度融合的关键。王辰表示,协和医学院采用“4+4”医学教育模式,并与其他大学合办“协和医班”,创新人才培养模式,在医学教育中体现多学科融合,在医学发展中体现医学的多学科性。

为进一步激发人才创新活力,一系列改革措施正在实施。中国科学院院士张学敏表示,国家自然科学基金委通过临床医学人才评价试点改革等举措,营造鼓励科研人员“十年磨一剑”的良好学术生态,探索我国基础研究人才自主培养之路。

基础研究的融合创新离不开高水平的支撑平台。为进一步促进医学基础研究,中国医学科学院基础医学研究所建设实验细胞、人脑组织、人口与健康科学数据三个国家科技资源共享服务平台。平台在重大疾病发病机制、国民健康调查和国人生理参数、遗传病基因鉴定与诊断等领域开展科技攻关,持续推进基础与临床交叉融合,产出多项“从0到1”的医学创新成果。

与会专家认为,当前我国医学基础研究原始创新的数量和质量仍有较大提升空间。通过加强学科融合,形成合力挑战前沿难题,将进一步提升我国医学基础研究领域的原始创新能力,催生更多科研成果,形成“提出真问题、解决真问题、真解决问题”的良好学术体系。

### 专家呼吁——

## 建立与土壤健康对应的有机质指标体系

◎本报记者 马爱平

日前,首届“土壤健康与再生农业”论坛举办。论坛上,中国工程院院土徐明岗基于大量长期试验强调,有机质是土壤肥力的核心,要重视建立有机质与土壤健康相对应的指标体系。

土壤是生命之基、食物之源。当前,全球三分之一的土地因侵蚀、盐碱、酸化等问题出现不同程度的退化,土壤保护迫在眉睫。

据《世界土壤资源状况》报告,全球约

有33%的土壤中度或高度退化。“在全球范围内,可耕地每年流失750亿吨土壤,估计造成每年约4000亿美元的农业生产损失,还极大削弱了土壤储存和循环碳、养分及水分的能力。《世界土壤资源状况》报告指出,土壤功能面临着10大威胁,包括土壤侵蚀、养分不平衡、土壤酸化、土壤污染等。”联合国粮食及农业组织驻华代表处项目官员姚春生表示,健康的土壤是可持续的农业粮食体系的基础,人类大约95%的食物营养来自土壤。

土壤健康和粮食安全问题密切相关。

“守护土壤健康对于粮食安全、农业可持续发展、生态环境保护的意义不言而喻。各方仍需加倍努力,竭尽所能地减缓冲突与地缘对抗,积极应对气候变化,加强全球协同,减少饥饿,促进粮食安全。”联合国世界粮食计划署中国办公室南南合作主管贾焰表示。

没有健康的土壤,就没有健康的农产品。中国农业大学资源与环境学院教授张俊伶认为,土壤有保持空气和水环境质量、促进动植物健康的能力,并和人类健康息息相关。

“让农户既看到短期效益,又能够见到

长期的效果。解决土壤用养矛盾,是当前我们面临的巨大挑战。需要探索出一些可持续发展的土壤用养结合模式。”张俊伶表示。

“土壤有机质是耕地质量的核心,决定着土壤的物理、化学和生物学性质,是实现粮食安全的基础。大量研究表明,作物单产与土壤有机质含量密切相关。土壤有机质含量每提升0.1%,在北方旱区可提高粮食作物生产能力0.3—0.5吨/公顷,在南方稻区可提高0.4—0.6吨/公顷;全国土壤有机质含量每提升0.1%,粮食的稳产性可提高约5%。”徐明岗说。