全国政协委员、安天集团创始人肖新光：

用好大模型这把“双刃剑”

本报记者 张心怡

人工智能大模型在推进产业变革和生活赋能的同时，也带来了新的安全风险；在带来安全风险的同时，又成为驱动网络安全技术创新升级的重要手段。全国政协委员、安天集团创始人肖新光在接受《中国电子报》记者专访时表示，大模型既带来了风险因素，也带来了安全助力。无论是提升网络安全防御的自动化、智能化水平，还是在大型防御体系中更好地实现对数据和信息的判断整合、对深度伪造的识别，大模型都有其应用之道。

> 生成式AI和大模型不单是为产业构建了一个相对通用化的基础技术，也改变了产业主体的心态，为产业优化合作方式、构建更好的分工基础，带来了很好的机遇。

三种风险因素与三种安全赋能

新兴技术在应用过程中，往往具有“双刃剑”的特征。肖新光向《中国电子报》记者指出，新技术往往与风险伴生而来，两者有三种耦合关系。一是新技术会对原有的风险产生加速作用。二是新技术的基础设施会成为攻击目标。三是新技术本身也会带来新型风险。

但新技术带来风险的同时，也会成为应对风险的重要手段。肖新光为记者列举了互联网和云计算两个例子。互联网带来了安全威胁快速流动的风险，但也为安全能力的分发、安全运营的快速闭环构造了基础条件。云计算带来了针对其体系的攻击会导致整体崩溃的风险，但以云计算为基础，能够重构安全防护的支撑体系，从而构建更具弹性的防御机制。

大模型也不例外。

“大模型带来了上述三种风险，但也为应对每一种风险提供了相应的赋能。”肖新光说道。

其一，虽然大模型可以被攻击者利用，提升了攻击的自动化水平和攻击能力，但也在防御侧改善了安全运营的协同能力、提升运营的智能化和自动化水平；在赋能侧（安全企业）支撑更高质量的特征工程和知识工程体系，推进更为精准高效的安全能力生产；在监管侧改善研判决策能力。总之，大模型为在安全防护工作中构建更敏捷高效的响应闭环提供了更好的支撑。

其二，大模型基础设施一方面会成为网络攻击的目标，另一方面，其本身的建设也是IT基础设施的重构。在构建新型基础设施的过程中，可以将网络安全能力直接融入，成为具有强安全能力的新型基础设施。

其三，大模型带来了深度伪造等新型风险，从而使攻击者针对“人+机”系统的攻击点移到人一侧，但也同样可以用于相关攻击的检测。

“我们要更好地把人工智能技术和防御能力建设融合起来，加强网络安全企业自身的能力发展和赋能作用，提升监管侧的感知管理能力，提升关键信息基础设施和重要信息系统的运营自动化水平。”肖新光说，“做好这样的基础工作，既能实现大模型对于网络安全本身的助力，也会提升大模型自身的安全性。”

对于如何“舞”好新兴技术这把双刃剑，肖新光表示，一定要统筹安全与发展。

“新兴技术在发展初期，往往具备基础设施的相关属性。在构建新技术基础设施的过程中，就要融入安全的基本理念和方法框架，使它先天具有安全基因。”肖新光说，“在新技术的发展阶段，要合理分配安全所需的资源。同时，对于新技术的基础设施所面临的攻击风险，要做防御上的充分考量，统筹规划，同步推进，使新技术行稳致远。”

推进网络安全产业分工协作

作为一位网络安全领域的“老兵”，肖新光也从产业维度关注着大模型对网络安全的影响。他认为，大模型的出现，有望进一步释放网络安全需求，并推动不同市场主体之间的分工协作。

“当前网络安全产业存在竞争过度、协同不足的问题。”肖新光指出。一方面，网络安全深度、系统、刚性的需求还没有充分释放，产业规模还不够大；但另一方面，市场主体已经达到一定的体量。因而相关企业往往不断拓展自己的产品赛道幅宽，在一个相对碎片化的市场上进行全口径的竞争。在他看来，这并不符合现代产业的特点。因为现代产业具有非常鲜明的大工业生产属性，既有基于共性技术和基础设施的分工协同，相互之间又有产品和品牌的竞争。

而大模型为产业带来了强有力的共性技术底座。相应的，网络安全领域也需要共性技术平台，形成市场主体间的有效分工协同。

“生成式AI和大模型不单是为产业构建了一个相对通用化的基础技术，也改变了产业主体的心态，为产业优化合作方式、构建更好的分工基础，带来了很好的机遇。”肖新光说道。

全国政协委员、沈鼓集团股份有限公司副总工程师姜妍：

装备制造商要更多参与国际标准制定

本报记者 姬晓婷

3月5日，十四届全国人大三次会议在北京人民大会堂开幕，国务院总理李强在政府工作报告中指出，激发数字经济创新活力，持续推进“人工智能+”行动，将数字技术与制造优势、市场优势更好结合起来，支持大模型广泛应用，大力发展智能网联新能源汽车、人工智能手机和电脑、智能机器人等新一代智能终端以及智能制造装备。

人工智能等数字技术在智能制造装备领域的应用状况及前景如何？带着这个问题，《中国电子报》记者采访了来自压缩机行业的全国政协委员、沈鼓集团股份有限公司（以下简称“沈鼓集团”）副总工程师姜妍。

在姜妍看来，数字技术正给企业带来技术创新和生产管理方式创新两方面的加成。

当前，数字孪生技术可以帮助工厂及时发现生产中可能出现的问题并预警；AI也能承担部分生产辅助工作，在机组模拟运行培训中，AI也在发挥作用。但大模型的应用在该领域还比较有限，设备的安装操作设计，依然要靠强大的专家团队的支持。

对于姜妍来说，数字技术给企业管理方式的创新带来了更大的加成，企业生产全流程数字化后，企业能够很方便地实现生产过程的全流程追溯。不论是零部件、合同、设计图纸，还是生产的各个环节，都能够借助一个系统实现统一管理。

> 数字技术给企业管理方式的创新带来了更大的加成，企业生产全流程数字化后，企业能够很方便地实现生产过程的全流程追溯。

“管理方式的创新，给我们的工作带来了很大的便利。在数字化之前，我们只有纸质的图纸，工作人员只能在现场看。经过数字化改造之后，工作人员的工作地点变得更灵活。而且图纸下载时间和渠道可追溯，也降低了技术泄密的风险。”姜妍说道。

“加快经济社会发展全面绿色转型”是今年政府工作报告中提到的另一个关键词。近几年，姜妍所在的沈鼓集团一直在迎合服务绿色能源的方向进行产品线创新、升级。在国家发展风能、光伏等新能源产业的情况下，沈鼓集团也在尝试开拓储能业务。新业务的拓展给沈鼓集团带来了新的挑战。姜妍表示，在沈鼓集团的传统业务中，机组大部分都是连续运转的，但储能领域所需要的机组则是间断运行的，这样的变化需要工程师们适应，也有许多新的技术难题需要克服。

今年全国两会，姜妍带来的提案围绕中国标准的海外应用展开。“我国产业界流传着这样一句话：一流的企业写标准。”姜妍说，“我们希望中国的企业不仅要做设备供应商，还要参与国际标准的制定，如果能够参与产品材料标准、加工标准、检验标准等的制定环节，我们的企业就可以避免在适应国际标准上花费许多不必要的时间。”

两会声音

全国人大代表，小米集团创始人、董事长兼首席执行官雷军：

带领国产供应链向全球价值链高端迈进

全国人大代表，小米集团创始人、董事长兼首席执行官雷军表示，无论是传统产业的转型升级，还是培育壮大新兴产业，都离不开科技创新。“5年前，我们下决心加大科技创新力度，大规模投入底层核心技术，规划5年投入1000亿元的研发费用。5年过去了，我们大约投了1050亿元，一些前沿技术创新已经逐渐开花结果。”雷军说道。

在当前全球智能手机市场上，小米连续18个季度稳居全球前三。在坚持科技投入的同时，也带领国产供应链伙伴向全球价值链的高端迈进。同时，小米与合作伙伴共创共建的智能家居物联网平台，连接设备的数量也是全球最大。

“这一切都表明，全球用户越来越认可中国科技创新的价值。”雷军说道。

制造业是我国的立国之本、强国之基。雷军表示，小米作为中国制造业发展的建设者、受益者，将继续加大研发投入，带头突破更多的关键核心技术，加快培育发展新质生产力，将中国制造、中国品牌带向全球市场，为中国制造转型升级贡献自己的力量。

3月4日，雷军围绕新能源汽车、人工智能产业高质量发展，向大会提交了五份建议，分别是《关于加快推进自动驾驶量产的建议》《关于发展智能网联新能源汽车产业生态的建议》《关于加快推进人工智能终端产业高质量发展的建议》《关于优化新能源汽车号牌设计的建议》《关于加强“AI换脸拟声”违法侵权重灾区治理的建议》。

五份建议全部聚焦AI和新能源汽车产业“高质量发展”，出发点都是推动“科技带来美好生活”，既有提升中国企业在全球科技新格局中的竞争力的产业视角，又有民生视角。

其中，在加快发展人工智能终端产业方面，雷军建议，一是健全人工智能终端标准体系，编制以用户体验为导向的智能化分级等系列标准，研究制定人工智能终端产品认定方法，强化国际国内标准有效衔接。力争2027年年内初步建成人工智能终端标准体系，2030年率先形成全球领先的人工智能终端标准体系。积极推进优秀产品、典型案例遴选，助力企业创新发展。

二是强化人工智能终端产业协作，构建应用协同生态，由行业组织牵头，联合终端厂商、应用厂商、大模型厂商等，加快构建统一的终端设备和智能应用之间的接口规范与数据格式。力争到2030年前形成2至3类相对统一、国际领先的智能终端操作系统平台，促进百亿级终端应用的跨界无缝互通，建成开放共赢的人工智能终端创新大生态。

三是中央和地方部门加大对人工智能终端领域研发与应用专项的支持。力争到2030年，建成具有全球一流竞争力的智能终端产业生态。

在加快推进自动驾驶量产方面，雷军建议，一是推进自动驾驶汽车大范围测试验证，加快推进自动驾驶汽车全国性测试验证，力争2025年建立跨区域、跨省份、一体化的便捷互认机制；同时加快量产商用进程，尽快明确自动驾驶汽车的量产时间预期，力争2026年可支持高速快速路自动驾驶、城市自动驾驶等功能的量产应用。

二是争取2026年前完成设立自动驾驶汽车专属保险，包括交强险、商业险、三责险等，降低自动驾驶汽车推广门槛，维护驾驶人、乘客和行人的权益。同时，持续加强自动驾驶的宣传教育，严格规范智能驾驶、自动驾驶、无人驾驶、完全自动驾驶等用词和适用场景，避免夸大宣传。

三是加快建设自动驾驶全国性法律体系，明确合法上路身份；加快建设国家层面的自动驾驶统一标准体系，为自动驾驶汽车量产提供清晰的技术准则。

雷军表示，小米将坚定不移走科技创新的道路，走高端化发展的道路，将先进的人工智能技术应用到各个终端产品中去，让广大消费者能够体验科技带来的美好生活。

全国人大代表、中兴通讯高级副总裁苗伟：

越来越多的企业开始注重技术创新

本报记者 齐旭

当前，我国科技企业出海已经从初期的探索和试水，逐步进入深度参与全球竞争的阶段。“在此过程中，我国企业在全球市场的份额和技术影响力都在不断提升，但同时，也面临着更加复杂和激烈的国际竞争环境。”今年全国两会期间，全国人大代表、中兴通讯高级副总裁苗伟在接受《中国电子报》记者采访时表示，应制定科学的国际化战略，避免中资企业在出海过程中出现同质化竞争、靠价格战来获取市场份额，提升我国科技产业整体形象和国际竞争力，建议政府和企业共同努力，强化出海企业的资质审核和宏观调控，不断提升企业产品和服务的附加值。

> 现在，越来越多的企业开始注重技术创新、品牌建设和本地化运营，逐步在全球产业链中占据更重要的位置。

数据显示，我国高技术产品出海不断提速，2024年我国机电产品出口增长8.7%，占出口总额的比重为59.4%。其中，电动汽车、3D打印机和工业机器人的出口分别同比增长13.1%、32.8%和45.2%。

“过去，我国企业更多是依靠成本优势和规模效应参与国际竞争，而现在，越来越多的企业开始注重技术创新、品牌建设和本地化运营，逐步在全球产业链中占据更重要的位置。”苗伟坦言，中兴通讯作为全球领先的综合信息与通信技术解决方案提供商，亲身经历了这一过程。

然而，目前仍有一部分中资企业，由于国际化经验不足，在出海过程中缺乏清晰的战略规划和本地化运营能力，导致资源分散、重复建设，出现“一窝蜂”式的竞争现象。此外，由于创新驱动不足，部分企业在技术创新和产品研发上的投入不够，导致在国际市场上只能依靠价格战来获取市场份额，品牌建设能力不足，难以在国际市场上树立高端形象。

“这样不仅会削弱企业的盈利能力，还会损害我国科技产业的整体形象和国际竞争力。长期来看，这种竞争模式不利于产业的健康发展和国际市场的长远布局。”苗伟说，为了应对这一问题，政府和企业需要共同努力。在政府层面，苗伟建议强化出海企业的资质审核和宏观调控，加强企业行为监管，遏制不正当竞争，从源头上促进良性发展；在行业协会层面，建议积极牵头行业头部企业参与国际规则制定，提升中资企业的国际话语权，促进中资企业在海外市场的良性竞争，提升国际竞争力，维护“中国制造”的品牌形象；在企业层面，建议注重技术创新和品牌建设，提升产品和服务的附加值，同时，制定科学的国际化战略，避免盲目跟风和资源浪费。

“面对竞争，我们需要以更加开放和包容的心态，积极参与全球竞争，不断提升自身的核心竞争力，为我国科技产业的可持续发展贡献力量。”苗伟说道。

“人工智能+”在行动

（上接第1版）

全国政协委员、芜湖机器人产业发展集团董事长兼总经理许礼进在接受《中国电子报》专访时表示，推动人形机器人的量产应用落地，要开拓康养服务、工业制造、特种应急等场景开放试点，加速人形机器人产品的迭代优化。

如何用好人工智能？安全防线不可忽视。人工智能在赋能生产生活场景的同时，也会带来新型安全风险。在带来新型安全风险的同时，也会成为安全技术升级的助力。舞好人工智能这把双刃剑，就要统筹好安全和发展的关系。全国政协委员、安天集团创始人肖新光在接受《中国电子报》专访时表示，要更好地把人工智能技术和防御能力建设融合起来，加强网络安全企业自身的能力发展和赋能作用。

全国人大代表，TCL创始人、董事长李东生指出，随着生成式人工智能技术的发展，深度伪造技术也在快速发展。他建议从加快出台管理规章制度，明确惩罚制度、标识技术标准和发布管理、国际合作等方面，加强AI深度伪造欺诈管理。

如何跟上人工智能的迭代脚步？人才是重中之重。政府工作报告提到，加强拔尖创新人才、重点领域急需紧缺人才和高技能人才培养。教育部部长怀进鹏在首场“部长通道”上表示，DeepSeek和机器人引起国内外广泛关注，从一个方面也说明了中国科技创新和人才培养的效果。全国政协委员、天娱数科CEO贺晗向《中国电子报》记者表示，建议在高校中设置具身智能、人工智能+机器人相关专业或方向，加强多学科交叉融合，增加实践教学环节，提升学生的跨学科思维和实际动手能力。培养一批既懂AI大模型，又懂机械和自动化的复合型通才。

从底层基础设施构建到产业化落地，从新型终端载体到安全治理，从创新机制到人才培养，AI的探索与落地、发展与安全、攻关与协同，在代表委员们的建议和探讨中，有了更加清晰的图景，勾勒出智能奔涌的未来。