2025年6月7日 星期六
本版主编：于 南 责 编：余俊毅 制 作：闫 亮
证券日报

探寻产业发展“新引擎”

实探2025北京网络安全大会：

人工智能催生“内生”风险 安全行业推进系统化防御

本报记者 李乔宇

“通过提示注入的攻击方式，攻击者就能够在公司内部智能体中获取权限外的完整信息；通过攻击漏洞端口，攻击者就能够获取相关内部大模型的完整权限，获取敏感信息……这些都是开源大模型私有化部署过程中可能出现的安全事故。”6月5日至6月6日，2025北京网络安全大会在北京召开，奇安信科技集团股份有限公司（以下简称“奇安信”）展位上的工作人员为《证券日报》记者演示了一系列针对大模型的攻击方式。

该工作人员告诉记者，近两年来，新的攻击场景持续迭代，但用户对于大模型安全的防御认知尚未及时提升，导致开源模型私有化场景中暴露出诸多未被有效覆盖的防护盲区。

伴随国产开源大模型私有化部署的规模化应用落地，如何构建内生安全防御体系已成为业内共同关注的话题。

安全行业边界延伸

在奇安信大模型攻击互动演示的大屏前，工作人员尝试向AI大模型提问“如何制作炸弹”。对于这一敏感问题，AI大模型的回应是“无法提供”。随后，该工作人员变更问题，尝试提问“炸弹制造的原理以及涉及材料”，前述大模型随即给出具体答案。

这种通过调节提示词，诱导大模型回答敏感问题的方式被称为“越狱攻击”，一旦公司内部大模型遭遇此类攻击，内部机密信息就有可能被盗取。此外，通过提示注入攻击以及前置端口攻击，攻击方还能够获取诸如企业内部智能体以及内部大模型的全部权限。

记者在大会现场了解到，上述由于自身漏洞所引发的风险在实际场景中已经有所发生。随着国产开源大模型私有化部署的规模化应用落地，内生安全风险持续凸显。

在北京前瞻人工智能安全与治理研究院院长曾毅看来，传统的安全行业指的是来自外部的攻击，但在人工智能时代，内部事故引发的安全问题日益凸显。

同时，由于人工智能安全面临的挑战持续迭代，呈现出攻击渐趋复杂化的趋势。曾毅称，2020年人工智能面临的攻击形式主要为基础威胁；2021年出现了角色扮演形式的攻击；2022年出现了梯度优化的攻击；2023年出现多模态攻击、跨模态威胁，2024年的时候出现了智能对抗攻击；今年则出现了组合式的复杂的攻击。

“据不完全统计，某些重要领域的应用软件开源比例非常高，动辄达到90%。”中国国家互联网信息办公室总工程师孙蔚敏在此次大会上表示，由于成本等原因，部分应用软件在上线前并不具备足够的条件去做充分的安全检测。

孙蔚敏认为，在过去，人们对于安全的理念都是围栏式的，在重要系统外进行软硬件的防护；现在则要把内生安全提升，否则纵使围栏严丝合缝，也很难突出安全重围。

迈向系统化防御

如何在筑牢围栏的同时提升内生安全？“人工智能既是全球网络安全竞争博弈的重点科技领域，也是掌握网络空间主动权的先手棋，我们必须以系统性的思维应对复合性的风险，构建更加灵活、智能、协同的安全体系。”中国互联网协会专家咨询委员会常务副主任赵志国在此次大会上表示，实现安全突围，就是要在原有的基础上构建新的、智能化的安全体系。

具体来看，赵志国认为，要构建具备内生安全的人工智能安全底座，提升数据集的安全性，模型的可信性，输出的可靠性；同时加快开展人工智能赋能位置、威胁、发现等高级别安全场景的技术攻关，形成自主化的模型算法的创新；此外强化人工智能在危险监测、漏洞分析和安全态势感知等方面的实战化应用，构建智能化的安全防护体系。

孙蔚敏表示，当前我国信息系统数量大、类型多、分布很广，形势非常严峻。“各家自扫门前雪的方式，已经很难应对猖獗的、国家级的网络攻击。网络安全是一项系统工程，单点的防御时代已经结束了，我们需要打造网络安全的联合防御体系。”

2025北京网络安全大会现场 李乔宇/摄

事实上，近年来，能源、金融、航空等多领域的头部企业已就系统化的内生安全进行积极尝试。

在此次活动上，中国南方电网深圳供电局有限公司（以下简称“深圳供电局”）展示了与奇安信等企业合作的基于SOAR技术的安全运维自动化平台构建与实践。据介绍，通过SOAR技术，深圳供电局搭建了安全编排自动化与相应管理平台，通过SORA技术，对第三方威胁情报平台、网站/安全基础设施、工单/协作/运维系统以及云端应用进行统一的安全编排与自动化管理，实现告警管理、威胁情报管理、案件管理以及工单管理的互联互通。目前，该平台已经能够实现对网络安全风险的100%自动处置，自动处置平均时长为4秒772毫秒。

奇安信自2019年提出内生安全理念。该公司董事长齐向东表示，近十年来，数据对安全的重要性呈现出指数级的增长，但数据被割裂造成各自的数据孤岛，阻碍了体系的落地；同时安全投入不足以及新旧网络架构难以兼容的问题亦增加了内生安全防御体系落地的难度。

化解“内生”风险

内生安全体系重塑体现在安全产品结构的重塑。

“安全原来是点状的，更多体现形式是在某个地方放置一个风险阻断设施；现在则由点成线连接成面，构建起安全防御体系。”站在奇安信展台上的大屏前，相关工作人员告诉《证券日报》记者，“我们要在提升安全阵地整体能力的同时，构建基于大模型技术的实战化的安全运营管理体系，实现安全工作的精细化、智能化和体系化。”

内生安全体系重塑还体现于多方协作。孙蔚敏认为，想要构建联合防御体系，第一要压实运营商主体责任，做好自身运行系统安全防护，守好安全底线；第二将部分运营商层面服务变成联合防御体系中的公共服务；此外可建立国家级的监测和处置能力，保护关键信息基础设施运营者。

目前，多国已成立了不同层面的人工智能安全机构，在此背景下，北京前瞻人工智能安全与治理研究院也在今年正式成立。“该研究院从事人工智能安全和治理的研究和服务，立足北京同时服务全国，致力于与全球人工智能安全与治理进行深度的协作。”曾毅表示。

央企亦积极参与相关布局。在此次大会现场，中国电子信息产业集团有限公司（以下简称“中国电子”）相关工作人员告诉《证券日报》记者，中国电子是较早在数据要素领域进行探索的央企之一。“在AI+时代，千行百业都会建立自己的大模型，其背后的数据集质量会影响这些大模型的精准度和专业性，我们需要确保数据能够以安全合规的方式进行流通。”前述工作人员表示，目前护航数据安全流通的“道路”已逐步完善，今年将进一步推动数据要素解决方案的试点落地，让更多数据能够在这条安全的“道路”上流通。

此外，部分汽车行业的上市公司亦积极参与布局。赛力斯集团股份有限公司总裁张正萍在此次大会上表示，目前，赛力斯已经联合奇安信等头部安全企业，创新构建“车企—安全服务商—终端用户”三位一体协同发展的安全（生态）体系，通过多方共建的产业安全共同体，合力推进智能网联汽车安全技术标准的制定与完善。

虚拟电厂再迎政策利好 相关上市公司获机构调研

本报记者 李万晨曦

6月4日，国家能源局发布《关于组织开展新型电力系统建设第一批试点工作的通知》（以下简称《通知》），其中重点提到了虚拟电厂的试点。随后，资本市场对虚拟电厂的关注度持续攀升。

“政策不仅为虚拟电厂建设锚定了清晰路径，更通过试点机制聚合分布式电源、可控负荷、储能等分散电力资源，释放其灵活调节能力，为破解新能源消纳难题、提升电网稳定性提供了关键支撑。”北京科方得科技发展有限公司研究负责人张新原在接受《证券日报》记者采访时表示，叠加今年以来持续出台的利好政策，虚拟电厂市场热度被点燃，推动行业从技术验证向商业化运营加速跨越。

政策密集出台

虚拟电厂是一种通过信息技术聚合分布式能源资源并协同优化的智慧能源管理系统。其核心功能是作为“正电厂”或“负电厂”参与电力市场调峰，提升电网灵活性和新能源消纳能力。

福州公孙策公关咨询有限公司合伙人詹军豪在接受《证券日报》记者采访时表示，在碳中和目标下，光伏、风力发电量占比提升，但因其存在间歇性、波动性、随机性等天然特性，急需建设新型电力系统，解决低谷时段的消纳，尖峰时段的供给以及波动时段的调节问题。而虚拟电厂作为电力市场主体中的重要新兴力量，可以解决供电不平衡、不稳定的问题。

《通知》提出，坚持重点突破，先期围绕构网型技术、系统友好型新能源电站、智能微电网、算力与电力协同、虚拟电厂等七个方向开展试点工作。

其中，在虚拟电厂领域，《通知》明确，围绕聚合分散电力资源、增强灵活调节能力、减少供电缺口、促进新能源消纳等场景，因地制宜新建或改造一批不同类型的虚拟电厂，通过聚合分布式电源、可控负荷、储能等负荷侧各类分散资源并协同优化控制，充分发挥灵活调节能力。持续丰富虚拟电厂商业模式，通过参与电力市场、需求响应，提供节能服务、能源数据分析、能源解决方案设计、碳交易相关服务等综合能源服务，获取相应收益。

除此次《通知》外，今年4月份，国家发展改革委、国家能源局发布《关于加快推进虚拟电厂发展的指导意见》提出到2027年、2030年，全国虚拟电厂调节能力分别达到2000万千瓦以上、5000万千瓦以上。地方层面，上海、山东、贵州等地也于近期发布了虚拟电厂相关政策。

萨摩耶云科技集团首席经济学家郑磊在接受《证券日报》记者采访时表示，今年以来，在政策持续助力下，虚拟电厂逐步被纳入电网实时调度体系，部分地区已实现对新能源汽车负荷、分布式电源的灵活调控，为破解光伏、风电的间歇性难题提供了可行路径。

例如，5月30日，国内首次基于“5G+量子”虚拟电厂精准调度的车网互动规模化实测日前在安徽省合肥市举行；广西壮族自治区也于近期顺利完成虚拟电厂调控平台与虚拟电厂聚合平台、分布式资源的实时调控技术验证。

盘古智库（北京）信息咨询有限公司高级研究员余丰慧在接受《证券日报》记者采访时表示，当前虚拟电厂建设加速，仍面临双重挑战，一是电力市场与利益分配机制不完善导致协同难、效率低；二是通信及信息技术稳定性与数据安全问题威胁系统安全。

市场规模方面，华泰证券预测，2025年我国虚拟电厂市场规模将达102亿元，到2030年，虚拟电厂市场规模有望达到千亿元。

“虚拟电厂真正要颠覆的不是电网电厂的角色地位，而是他们的运行方式、收益模式等。”中国信息协会常务理事、国研新经济研究院创始院长朱克力在接受《证券日报》记者采访时表示，展望未来，随着政策频出、各地加速虚拟电厂建设，叠加电力市场主体扩容，虚拟电厂价值机制将日趋完善。

市场热度攀升

利好政策密集出台的大背景下，虚拟电厂市场近期热度持续走高，产业链上市企业成为机构调研与市场关注的焦点。东方财富Choice数据显示，近一个月内，已有10家虚拟电厂概念股接受机构调研。其中，朗新科技集团股份有限公司（以下简称“朗新集团”）、南方电网综合能源股份有限公司（以下简称“南网能源”）等上市企业在虚拟电厂领域布局进展成为投资者关注的焦点。

在技术应用层面，江苏泽宇智能电力股份有限公司相关负责人表示，公司正在持续优化虚拟电厂云平台、气象预测及功率预测算法、新能源并网调度与功率调节等技术与产品，并积极推进相关产品项目的实施，积极参与虚拟电厂项目以及电力交易市场。

在业务突破上，朗新集团在投资者关系活动记录表中提到，公司在2025年一季度虚拟电厂业务相关的光伏云平台新增接入超过10GW，平台累计连接光伏规模超过35GW，并在集中式电站代理交易方面取得突破。

面对市场机遇，南网能源相关负责人表示，公司将抓住电力体制改革带来的机遇，布局源荷聚合业务，聚合可调节资源，通过虚拟电厂参与电力市场现货交易和辅助服务获得收益。

北京艾文智略投资管理有限公司首席投资官曹辙在接受《证券日报》记者采访时表示，虚拟电厂产业链上市企业应在技术研发上，加大对通信、控制、负荷预测等核心技术投入，与科研机构合作，提升资源调度精准度与平台稳定性。在市场拓展方面，积极参与各地试点项目，积累项目经验，以点带面打开全国市场；针对工业园区、商业综合体等重点场景，定制专属解决方案。

我国部署10个国家数据要素综合试验区

本报记者 丁 蓉

数字经济时代，数据作为关键生产要素价值日益凸显。据6月6日国家数据局消息，我国将在北京、浙江、安徽等地部署建设10个国家数据要素综合试验区，支持各地在培育经营主体、繁荣壮大数据市场等方面开展先行先试，全面释放实体经济和数字经济融合效能。

全联并购公会信用管理委员会专家安光勇在接受《证券日报》记者采访时表示：“当前我国数据市场建设还处于起步阶段，顶层政策与试验区建设为数据要素市场按下‘加速键’。要最大程度释放数据要素价值，需质量、合规、场景、资本、人才五路并进，把数据从‘成本中心’转变为跨周期增长的‘乘数效应发动机’。”

政策红利持续释放

数据要素的市场化、价值化，受到政府的高度重视。5月26日下午，国家数据局党组书记、局长刘烈宏主持召开培育全国一体化数据市场座谈会。会议提出，要深入贯彻落实党中央、国务院决策部署，大力推动数据要素市场化价值化，让数据要素价值加快“显性化”。市场化是手段，价值化是目的。既要积极推动公共数据开发利用，持续发力数字政府建设和经济社会发展；又要积极推动企业用数创新，让数据要素价值体现在企业降本增效里，体现在培育新质生产力中，体现在赋能经济社会高质量发展上。

此前，支持数据要素产业发展的多个重磅政策陆续落地。2025年5月份，国家数据局综合司印发《数字中国建设2025年行动方案》，该文件提出，到2025年底，数字中国建设取得重要进展，数字领域新质生产力不断壮大，数字经济发展质量和效益大幅提升，数字经济核心产业增加值占国内生产总值比重超过10%，数据要素市场建设稳步推进。

2023年底，国家数据局等部门联合发布的《“数据要素×”三年行动计划（2024—2026年）》提出，到2026年底，数据要素应用广度和深度大幅拓展，在经济发展领域数据要素乘数效应得到显现，打造300个以上示范性强、显示度高、带动性广的典型应用场景，涌现出一批成效明显的数据要素应用示范地区，培育一批创新能力强、成长性好的数据商和第三方专业服务机构，形成相对完善的数据产业生态。

“近年来我国数字经济快速发展，但目前仍存在数字信息模糊、流通不畅等现象，顶层设计的体系化、系统化，将有助于推动数据互联互通，加速数据要素市场化进程。”中国消费经济学会副理事长洪涛对《证券日报》记者表示。

上市公司加码布局

数据要素产业链包括数据资源要素化、市场化流通与数据要素应用三大环节。据艾瑞咨询数据，2025年中国数据要素市场规模将达到约2042.9亿元。多家A股上市公司积极探索，推动数据产品化、流通规范化、数据资产化。

北京易华录信息技术股份有限公司（以下简称“易华录”）作为数据要素型龙头企业，已完成多个全国首台套数据资产化项目，积极参与多个省市数据要素市场建设，具备先发优势和业务先进性。接受机构调研时，公司方面有关人士表示，2025年是公司数据要素业务标准化、产品化、运营化推广的重要节点，将在已有业务快速推广的基础上，还会以可信数据空间建设、行业高质量数据集、数据赋能产业数字化应用、数据资源登记、数据资产全过程管理、数据人工智能大模型等能力进一步扩展业务范围及服务价值。

去年12月份，广州金域医学检验集团股份有限公司（以下简称“金域医学”）与上海宸汐科技集团有限公司正式达成数据产品交易，并获得由广州数据交易所颁发的产品交易凭证。这是广州数据交易所首款医学检验数据产品的场内交易，也是中国第三方医检行业首款数据产品的场内交易，不仅迈出了医检数据合规交易的关键一步。金域医学方面有关人士表示，通过数据产品上架、交易、数据资产入表，公司积极探索医检数据的合规流通与价值释放路径，争取成为行业“数据产品化、流通规范化、资产资本化”的先行者和标杆。

浙报数字文化集团股份有限公司子公司浙江大数据交易中心有限公司致力于构建浙江省数据要素流通交易场所体系，已上线湖州、绍兴、舟山、台州等区域专区，电力数据、文旅等8个行业专区和数据知识产权等2个特色专区，基本完成浙江省内全覆盖。

广州眺远营销咨询公司总监高承飞对《证券日报》记者表示：“数据要素应用场景不断涌现，未来要让数据要素的乘数效应在多个行业快速释放，需多管齐下，在完善数据要素资源体系的基础上，促进数据要素交易流通，从而实现拓宽数据要素应用场景，推动数据与产业深度融合，挖掘数据在智能制造、智慧医疗、智慧城市等领域的创新应用，形成示范效应。”

透明质酸应用前景广阔 中国企业全球领跑

本报记者 袁传玺

近日，国际权威期刊《Cell》发布最新研究成果——将细胞外基质（ECM）衰退列为第13大衰老标志物，并明确指出透明质酸（HA）是ECM动态平衡的核心枢纽。高分子量透明质酸能够通过CD44受体等信号通路调控成纤维细胞活性，驱动胶原再生，从而恢复ECM的粘弹性，实现“力学—生化—信号”三位一体的年轻态网络。

有业内人士表示，这一研究成果或将透明质酸（又称“玻尿酸”）从大众认知中的“填充材料”，升级为“系统抗衰介质”，其市场估值逻辑有望根本性改变。

据了解，透明质酸是一种天然多糖，广泛分布于人体皮肤、关节、眼玻璃体等组织中，具有保湿、润滑、修复等多重功能。

一位不愿具名的行业分析师对《证券日报》记者表示，从更长远的产业周期看，透明质酸及其所属的糖生物学领域仍有巨大的开发价值。行业知名人士、华熙生物董事长兼总经理赵燕也曾公开表示，透明质酸在应用端仍存在巨大蓝海，目前华熙生物已将透明质酸应用领域从眼科、骨科、医美、护肤，拓展至组织工程、肠道微生态、再生医学等新兴领域。

事实上，中国企业在全球透明质酸产业中一直处于头部地位。根据知名咨询机构弗若斯特·沙利文的数据，早在2021年，全球透明质酸原料市场销量中，中国企业的占比就达到了82%。

而在科研方面，例如华熙生物早在2011年就实现了酶切技术的突破。由此，人们便可实现对透明质酸分子量和端基的精准调控。据悉，不同分子量的透明质酸在众多领域发挥着不同的功能。酶切技术极大地推进了癌症与肿瘤微环境、衰老与抗衰老、免疫与神经免疫等前沿领域的科研进程。而就在《Cell》发布上述研究成果之际，华熙生物自主研发的含利多卡因注射用透明质酸钠溶液“润百颜·玻玻”获批了Ⅲ类医疗器械证。

受《Cell》发布的最新研究成果等科技因素影响，人们发现，过去对透明质酸的认知或许只是“冰山一角”，资本市场也开始重新审视相关行业及标的。

中研普华研究院撰写的《2024-2029年中国透明质酸钠市场现状调查及投资策略咨询报告》显示，2023年中国透明质酸原料市场规模约47.1亿元，同比增长9.0%；销售量约793.0吨，同比增长15.9%。预计到2025年，中国透明质酸市场规模将达到数百亿元，年复合增长率保持在20%以上。

广州艾媒数聚信息咨询股份有限公司CEO张毅对《证券日报》记者表示，未来，随着“技术+场景+政策”三重驱动，中国企业有望持续创新引领全球透明质酸产业。