

二〇二六北京网络安全大会举办

AI时代 以技术创新守护网络安全

李贞 吴杏雨



日前，2026全球数字经济大会数字安全论坛暨第八届北京网络安全大会（BCS 2026）在北京国家会议中心举办。来自全球三十多个国家和地区的3000余名学者专家、行业嘉宾会聚一堂，分享前沿观点。大会上，超200场峰会、论坛、特色活动为千余家企业搭建起产品展示和业务交流对接的平台。

今年的大会以“AI时代，攻防先行”为主题，各界嘉宾共议AI时代网络安全形势之变，共商AI安全技术创新之策，共谋合作共赢产业生态发展之路。

格局重塑： AI催生网络安全新模式

AI技术发展对当前维护网络安全有哪些影响？大会期间，这是与会嘉宾讨论的焦点话题。

中央网信办网络安全协调局局长高林将AI时代网络攻击的特征概括为“智能化升维、效率突破性增强、范围急剧拓展”。“深刻重塑网络安全体系和治理格局，已经成为无法回避、亟须回答的重大命题，迫切需要从思路、理念、方法、手段、防御体系、关键技术等各方面系统变革升级。”高林说。

“当AI智能体具备了自主感知、决策和执行能力，安全责任应当如何分配？智能体的越权与欺骗行为，在法律上如何定性？”AI技术发展为网络安全带来新的挑战。对此，中

国互联网协会副理事长赵志国表示，中国正在加快构建智能时代网络安全治理体系，呈现出法规先行、技术赋能、生态协同等3个鲜明的走向，初步形成了覆盖AI的研发、落地、应用、运维的全生命周期的防护合力。

针对AI技术引发的网络安全格局变化，奇安信集团董事长齐向东结合实战经验给予了解读。“过去，网络安全是人与人的对抗。AI大模型、智能体的出现，让网络攻击进入工业化时代，攻防进一步失衡。”在他看来，传统“发现漏洞、修补漏洞”的模式已经难以适配当前网络安全环境。单纯比拼漏洞挖掘能力，或者完全依赖AI原生安全技术，都无法破解当下难题，依托技术创新重

数据筑基： 探索智能网联安全路径

网络安全的问题与许多智能网联产业的发展息息相关。

今年5月，比亚迪推出国内首款4纳米车规级智驾芯片“璇玑A3”，夯实了汽车智能化核心优势。然而，作为人工智能落地的核心实体场景，智能网联汽车在加速迭代的同时，网络安全风险也随之加剧。基于这一行业现状，比亚迪详细分享了依托高质量数据构筑网络安全壁垒的实践路径。

对于AI带来的网络安全之变，比亚迪股份有限公司首席信息安全官罗小平深有感触：

“利用AI大模型进行网络攻击，突破安全防线的时间从几十分钟压缩到27秒。”罗小平认为，破局关键在于以AI对抗AI，同时不能迷信算法、忽视数据，“没有高质量的数据集，AI就是空中楼阁”。

因此，比亚迪没有急于引入大模型，而是打造“i迪犬”平台安全数据湖底座，在打通数据孤岛确保数据安全的前提下引入AI安全智能体，推动高质量数据与智能体的深度协同。罗小平将“i迪犬”安全一体化平台形象地比喻成“信息安全水厂”，整套数据治理

构安全体系才是破局之路。

齐向东提出，可以打造低、中、高“三位一体”、协同联动的安全体系：低位安全能力是全栈AI化的安全产品，负责执行，是“肌肉”和“手脚”；中位安全能力是智能体，负责运营、指挥、调度，是“神经”和“躯干”；高位安全能力是大模型底座，负责情报共享和决策，是“智慧”和“大脑”。三级能力共同支撑起AI时代的网络安全纵深防御体系。

“网络安全是AI时代的基础性产业，产业规模会伴随数智化规模水涨船高，网络安全面前摆着的是千亿级增量空间。加速网络安全升级改造，追平攻防失衡差距，是AI时代的必然选择。”齐向东说。

工作严格按照“引水、净水、用水”三大阶段推进。他表示：“我们接入23类数据源，日处理原始数据超过50亿条。”依托标准化处理与数据关联能力，破除数据壁垒，构建起安全威胁从发现到处置的全流程闭环。

在此基础上，比亚迪上线了3款AI安全智能体。“我们每天处理邮件超过30万份，钓鱼邮件研判准确率达到99.96%。依托这套智能防护体系，企业安全事件处置时长从45分钟缩短至5分钟。”罗小平说。



场景拓展： 构建具身智能安全生态

以服务机器人、智能终端等产品为代表的具身智能设备，正从酒店、楼宇等普通商用场景，拓展至政务、能源、金融等高安全领域。如何构建具身智能产品的网络安全生态，也是与会嘉宾关心的重点议题之一。

本届大会配套举办的具身智能安全分论坛以“具身智行，安全筑基”为主题。中国网络空间安全协会副理事长卢卫指出，具身智能正推动人工智能从虚拟空间走向物理世界，其风险形态已从传统的内容输出风险升级为自主行动风险。“缺少稳固的安全底座，具身智能的规模化落地终是空中楼阁。”为此，卢卫建议，应坚守全生命周期安全理念，构建零信任安全防护架构，推动治理从事后应急转向全生命周期闭环。

北京云迹科技首席执行官李全印认为：“越是关键的现场，客户越不会只问机器人能不能跑、能不能送、能不能扫、能不能巡；还会问，它的身份是不是可信，行为是不是可追溯，数据是不是能防泄露，远程运维是不是可管可控。”在他看来，要保证具身智能产品的高安全，“不是一次交付就结束了，而是在部署、运行、监测、预警、处置、复盘的过程中进行持续迭代”。

李全印介绍，云迹科技与奇安信共同发布高安全机器人产品实现了安全能力的联合升级。“我们的目标，是让机器人在高安全要求场景中做到可信可用、可管可控、持续防护。”比如，高安全机器人可以进入政府、能源、电力、工厂园区等高要求的业务环境工作；机器人的设备身份唯一，谁下达了指令，访问了哪些区域，采集和传输了哪些数据都可追溯；出现异常情况时能及时被发现、被告警、被处置，安全管理流程更加完备。

除具身智能安全分论坛外，本届大会还围绕AI技术、智慧能源、企业安全运营、协

同办公等不同行业赛道，开设多场专题分论坛与主题活动，同步举办多项网络安全实战赛事，丰富交流形式，覆盖产业多个维度。

图①：奇安信工作人员演示讲解安全智能体产品。受访者供图

图②：2026北京网络安全大会现场。受访者供图

图③：近日，江苏省海安高新区实验小学，民警向小学生讲解网络安全知识。

图④：云迹科技高安全机器人产品。受访者供图



人工智能时代催生新型数字流量形态

词元套餐便利数字生活

本报记者 姚雪青

6月1日上午，江苏南京昱鼎科技有限公司创始人王鹏来到办公室，第一件事就是打开江苏移动“晓伴·算龙头”平台，登录账号并充值。“每月充值40元，可用2000万词元（Token），对我来说够用了。”王鹏说。

作为“一人公司”创业者，王鹏从事语言类和图文类客服产品的开发生产，需要用到六七种人工智能大模型，调用词元、反复测试，看哪个效果更好。“以前要给每种大模型充值，平均每月各花30—50元，有的花不完，有的不够花，管理和维护账户费时费力。”王鹏说，3月起，他订购了江苏移动推出的“Token包”词元套餐，开一个账户就能在不同大模型间随意切换、灵活选择，用算力就跟用手机流量一样方便。“不仅成本低了，我也可以腾出手来，把更多时间花在产品研发、市场调研和客户拓展上。”王鹏说。

词元是人工智能交互的计量单位，文字、指令、问答、代码、图文生成等每一次和大模型的交互，都会消耗相应数量的词元。词元套餐是大模型平台以及运营商整合算力资源、大模型调用权限的标准化计费产品，即“算力+人工智能模型”使用权的组合套餐。

中国移动江苏南京分公司云智算中心副主任汤咏介绍，随着人工智能行业蓬勃发展，各式各样的大模型层出不穷，它们分属不同平台，用户在使用时需单独注

册、登录。为了整合资源，打造统一使用入口，近期，三大运营商纷纷推出词元套餐，免去了多平台登录的繁琐，让使用体验更便捷高效。

汤咏举例，目前江苏移动推出4款词元套餐：5元体验包，适合新手体验；20元标准包，可满足日常学习与办公需求；40元进阶包，支持深度创作及复杂办公场景；编程专属包，精准服务技术研发人员。

高频使用人工智能、算力消耗较大的用户，是词元套餐的主要消费群体。例如，师生在学习与教学中，会借助模型完成课业学习、备课教研；自媒体从业者依靠大模型高效产出各类内容；程序员与研发工程师将其作为开展专业工作的帮手。

对于企业用户来说，最大的感受是降本增效。南京中兴信雅达信息科技有限公司副总经理倪玥介绍，公司专注企业员工及高校师生电子信息类技能培训，深耕编程能力培养、软件开发、接口测试等教学工作。学员代码编写、程序调试、漏洞排查、测试演练等环节都离不开人工智能辅助，对算力支撑的需求量不断增加。

“大模型调用和词元计费方式正快速迭代。”倪玥算了一笔账：2024年，企业若要开展相关应用，往往需要租赁专门的算力服务器或进行本地化部署，一次性投入较高，服务器租赁等成本可能达到数十万元；2025年，各家大模型平台更多按词

元调用量或交互次数收费，公司40多名技术人员每月在多个大模型平台上的充值费用，少则三四千元，多则七八千元；随着三大运营商推出词元套餐，公司为员工办理套餐，调用成本降至每月不到2000元。

“词元计费产品，是人工智能时代催生的新型数字流量形态。当下，运营商集中推出词元商用产品，是人工智能产业高速扩容与通信行业转型升级双向作用的结果：大模型调用规模持续攀升，传统电信业务增长放缓，行业需要培育全新增长极。”东南大学移动通信国家重点实验室教授宋铁成介绍，随着网络服务从传统数据传输转向智能能力调用，大模型与智能体逐步成为信息生产的新增重要来源。参照早年语音套餐、移动通信流量包的普及发展路径，词元正走出专业技术圈层，将成为企业数字化经营、大众日常数字消费的基础配套。

宋铁成认为，目前国内各大运营主体结合自身情况形成了差异化的发展路径。部分主体深耕算力网络与安全底座建设；部分依托用户资源与产业优势灵活定制资费；还有部分参与聚焦垂直行业，努力打造场景、终端与算力一体化打包方案。“随着行业日趋成熟，市场将告别简单粗放的定价模式，会依据大模型性能、服务时延实行分级计价。”宋铁成分析，运营商也将深化和各大模型厂商合作，拥抱最新大模型技术，推动词元普惠落地。



科普市集 精彩纷呈

▲近日，新疆维吾尔自治区乌苏市科学技术馆走进文林路社区，开展科普集市主题活动。图为仿生机器人上演顶球表演，孩子们近距离领略科技乐趣。
李仁锡摄（人民视觉）

►近日，内蒙古工业大学附属小学第二届校园科技节开幕，现场设置科普集市等环节，学生们在沉浸式趣味互动中激发科学探究热情。图为活动现场，学生在教师指导下进行VR体验。
丁根厚摄（人民视觉）

