共话数据安全 共谋行业发展

没有安全，何来发展？9月5日，在2023中新国际数字合作论坛数字安全分论坛上，中国工程院院士、高校专家学者、行业企业代表“綦”聚一堂，围绕“共建国家网络安全产业园 筑牢数字变革安全防线”主题，分析数字挖掘与数字安全、展望人工智能发展方向、探讨加强数字安全防护保障、分享创新理念与技术突破，助力推动中新数据安全跨境合作。

在用好网络的前提下保障网络安全

中国工程院院士谭建荣说，要用好网络就必须保障网络安全，但是安全不是为了安全而安全，而是要在用好的前提下安全。网络安全包含信息安全、网络安全、数据安全三个层面。数据挖掘是对海量数据的分析应用，对数据安全提出了更高的要求。数据挖掘作为发现有用信息的高效手段，使得出现数据安全问题时的后果进一步加重。数据安全的发展经历三个阶段：第一个阶段是以“数据库安全”为核心，第二个阶段是以“数据场景化”为核心，第三个阶段是以“数据安全治理”为核心。目前，生成式人工智能安全防范是新的课题，要更多地去研究去应用去防范，相信綦江一定能在新一轮发展中把大数据和人工智能技术运用好，做好网络安全，更好地发挥网络的作用、人工智能的作用，推进高质量全面发展。

融合人类认知的AI是未来研究方向

“人工智能超越了人类视觉识别能力、人类博弈决策思维能力、许多人的语言交流沟通能力，这几个方面的突破让人工智能进入到人类生活的方方面面。人工智能的‘智能’包括计算智能、感知智能、认知智能。但是，面对没有现成答案的‘高深问题’，ChatGPT无法通过思索给出答案，仅能列举人类已有的观点和结论。以众多实例证明，数据驱动的‘大数据+大模型+大算力’大系统，由于对人类知识与认知的缺失，仅能实现从个体智能到群体智能的量变，却不能够实现从群体智能到涌现智能的质变，也不能实现从专用智能到通用智能的跨越。”重庆邮电大学副校长王国胤在演讲中谈到，计算机的信息处理是从细粒度到粗粒度，而人类认知规律是从粗粒度到细粒度，因此深度学习的识别计算机理不等于人类大脑的识别认知机理。融合人类认知原理与计算机信息处理空间变换过程的多粒度认知计算，是挑战也是必然方向，未来我们的研究方向即为融合人类认知的AI。

数字城市安全以“零事故”为目标

“试想一下，随着数字化改革的发展，任何人都会访问达到业务系统的核心，这种情况怎么保证业务系统安全性？”奇安信集团副总裁罗海龙以提问的方式展开演讲，他说，数字城市安全应以“零事故”为目标，“零事故”的三条标准为业务不中断、数据不出事、合规不踩线。首先，要从业务视角看到不同的安全风险，建设安全防护体系，保障业务不中断。其次，要用内生安全方法建设数据安全体系，确保数据不出事。再者，要构建自证清白+第三方监管的技术保障体系，实现合规不踩线。安全运营是实现“零事故”关键，网络安全运营中心是实现数字城市安全“零事故”的关键。奇安信集团在綦江区做了一个大胆尝试：建设数字重庆安全运营中心（綦江），即通过一个大网络安全管理平台，把全区的安全信息和数据汇总在一起，进行分析找到问题，再通过流程下发企业促进产业发展。该运营中心不仅能提高区域网络安全产业的发展和防御水平，还肩负着社会责任，帮助没有能力建设的单位开展建设，并搭建起城市安全人才网络，是一个作战指挥平台，这样一个平台能汇聚集体力量打赢网络安全战争。

实现国产化办公全阶段服务能力

“外设、应用兼容性差，安全性要求高，办公应用匮乏，协同效率低，要求符合相关规定，满足芯片及操作系统要求……国产化办公之路筚路蓝缕，仍需披荆斩棘。”天翼云行业专家田林青表示，天翼云科技有限公司自主研发的云桌面，具备性价比高、兼容性强、一站式安全套件、高效协同等产品特征，高效解决国产化替代过程中的软硬件适配的突出问题，以及国产化操作系统兼容已有Windows应用的问题，通过GPU二次虚拟化技术，攻克了NVIDIA的vGPU系统内核隔离技术，低成本满足用户对GPU算力的需求。同时，还构建起了一站式全链路安全防护体系、国产环境协同办公体系，能提供可视化应用搭建服务。如今，天翼云电脑进入XC工委“产品技术图谱”，天翼云电脑实现国产化办公全阶段服务能力。

共建共享共通共赢网络安全新生态

联通数字科技有限公司重庆市分公司首席网络与信息安全官杨玲说，在数字经济下，网络安全建设和数字化建设是一体两翼、双轮驱动，网络安全和数字化建设的进展相互牵动，任何一方的滞后都会对整体造成影响。随着数字化浪潮的到来，网络安全已不再是单纯的技术问题，而成为了一个新的战略保障问题。中国联通致力成为值得信赖的国家网络空间安全守护者，勇担网络安全产业链链长，当好数字经济“护航员”，致力在优化数据安全能力体系、加大个人信息保护力度、构筑云网安全能力体系、增强网络安全原子能力、提升安全感知分析能力、交付安全可信运营平台、构筑云网端数产品服务、丰富一体化安全产品运营服务体系等方面发力有为，进一步携手产业伙伴，打造共建、共享、共通、共赢的网络安全新生态。

为物联网平台及行业解决方案赋能

“物联网作为一种新技术，行业标准以及相关管理都还处于初级阶段，在安全方面厂商重视程度不足、防护方案不成熟、用户安全意识薄弱成为普遍现象，同时，产业链各方安全责任不清晰，物联网在管理和技术方面都存在较大安全风险。”中移物联网有限公司副总经理柏洪涛说，面向物联网安全防护需求，中移物联网有限公司打造了OneSec品牌，构建分层次、多机制的防护能力，及安全态势感知和解决方案能力，充分发挥央企在安全、可信方面的差异化竞争优势，为物联网平台及行业解决方案赋能。为应对物联网复杂的安全威胁，该公司开展了物联网安全态势感知平台的建设实践，全面感知包含物联卡、智能设备、业务安全、基础资产等领域安全态势，及时响应和处置物联网安全风险。基于大数据和人工智能技术，深度融合各类型安全测评工具，实现覆盖物联网产品“云”、“管”、“端”的智能化、一站式安全测评，降低业务安全风险。基于区块链技术为多行业多品种商品提供全供应链溯源服务，通过智能合约记录商品从原产地到消费者的全生命周期每个环节的重要数据，同时保障数据的可追溯不可篡改及隐私保护性，实现全流程溯源。

西部网络空间靶场成对外开放新引擎

重庆国科量子科技有限公司CEO黄勇说，随着第三次网络安全技术革命浪潮的掀起，各国已开展国家级的网络靶场建设，网络靶场已成为各国家进行网络空间安全研究、学习、测试、验证、演练等必不可少的网络空间安全核心基础设施。我们中国广电重庆网络公司有幸取得了“西部网络空间安全公共服务靶场”的运营权，西部网络空间靶场主要为党政军及企事业单位提供面向实战的网络安全对抗服务，全面打通产学研用协同创新通道，建成国际一流的网络安全研发、人才培养、技术转移基地，成为深化对外开放的新引擎，聚集高端产业的新平台，成为国家网络靶场在中国西部地区的重要支撑点，推动重庆网络安全产业实现跨越式的发展，为产业升级和发展起到支点和抓手的作用。我们依托网络空间安全靶场，争取国家网络安全中心、中国计算机学会、市网信办、公安网监等单位的支持，广泛与安全公司开展立足重庆，面向全国的网络安全教育、培训、测评、演练、研究、防御、应急、管控等体系化服务。现已入选重庆市全民数字素养与技能提升基地(首批)名单。

备灾备战备难要未雨绸缪有备无患

“灾备(Disaster Recovery)是指利用技术、管理手段以及相关资源确保既定的机构关键数据、关键数据处理系统和关键业务在灾难发生后可以恢复，而建立的系统化的数据应急方式。灾备新技术包括基于容器化应用平台的灾备技术，超融合架构的灾备技术、云平台的灾备技术、多云跨云的灾备技术、物联网‘边缘’灾备技术、区块链灾备技术、智能化灾备技术、容灾感知技术。Market-sand Markets的相关数据显示，全球备份和恢复市场总额将从2017年的71.3亿美元上升到2022年的115.9亿美元，相比备份与恢复市场，云灾备即服务(DRaaS)全球市场呈现出快速增长的态势。我国宏观经济发展稳定，各行业对灾备产品需求快速增长；据IDC预测，数据灾难备援服务和业务连续性服务将成为中国信息服务市场中增长最快的部分。”北京邮电大学教授辛阳说，根据灾备人才和人才培养现状，急需培养适应于我国灾备领域技术应用和科研创新方面的新型专业技术人才。灾备是网络信息安全建设的最后一道安全屏障，灾备不只是一个业务，更是一个生态。备灾备战备难，要未雨绸缪，有备无患。

文图/记者 成蓉 王京华 陈星宇