筑牢“防火墙” 拧紧“安全阀” 拓展“新蓝海”

院士专家学者企业家齐聚2022重庆网络安全高峰论坛，为做大做强网络安全产业建言献策

□本报首席记者 周尤 记者 何春阳

近年来，大数据、云计算、物联网等新技术不断涌现，给人类社会带来深刻变革。万物互联的时代，机遇与挑战并存，便利和风险共生，新技术形态的迅猛发展也带来了诸多挑战：“数字鸿沟”不断拉大，网络诈骗频频发生……广泛开展网络安全宣传教育成为迫切需要。

没有网络安全就没有国家安全，没有信息化就没有现代化。

9月6日，在2022重庆网络安全高峰论坛上，中国工程院院士倪光南、重庆邮电大学校长高新波、奇安信集团总裁吴云坤等8位院士、专家学者和企业家，围绕网络安全发展趋势、人工智能对网络安全的影响以及网络安全产业前沿技术等领域展开探讨。

谭晓生（市委网信办供图） 武春岭 段书凯 吴云坤 倪光南 杜跃进 高新波 王涛（市委网信办供图）

本组图片除署名外均由记者齐岚森摄/视觉重庆

谈法治防线 不断筑牢网络安全法治防线

第50次《中国互联网发展状况统计报告》显示，截至2022年6月，我国网民规模达到10.51亿，互联网普及率达到74.4%，中国已经是一个名副其实的网络大国，网民人数达到了全球第一。

中国工程院院士倪光南带来了题为《健全的法律和法规为国家网络安全保驾护航》的主旨报告。他说，网络安全问题不仅关系国家安全和发展，还关系到广大人民群众切身利益。

在他看来，近几年国家战略层面对网络安全进行了全面部署，出台了以《中华人民共和国网络安全法》为代表的一系列法律法规。“实际上，影响网络安全的法规覆盖很广。例如，政府采购法就对网络安全有重大影响。”

今年7月15日，财政部公布了新版的《中华人民共和国政府采购法（修订草案征求意见稿）》。这次征求意见稿总结以往的经验，针对相关问题提出解决方案，同时借鉴国际经验，完善我国政府采购制度。

倪光南认为，网络基础设施建设和网络系统采用的硬件、软件和服务等，都涉及政府采购环节，所以政府采购法也必须根据形势发展，及时修改完善，保证政府采购的科学性、有效性、合法性和公平性，充分发挥其对网络安全的支撑和保障作用。“在当前形势下，政府采购强调安全保障是很有必要的，这也是对我国已有的国家网络安全一系列法规的重要补充。希望政府采购安全审查制度能够尽快出台，或者可以先引用信创工作的相关安全审查制度，以便及时填补这个空缺。”倪光南说。

“健全的法律法规是网络安全的基础。”北京赛博英杰科技有限公司创始人谭晓生对此深有同感。他表示，数据安全法、个人信息保护法等法律法规的颁布，对于网络安全市场是非常大的利好。

谈人工智能 推动实现人工智能可信可靠可解释

“人工智能”成为论坛上各位专家学者口中的高频词汇。

“人工智能技术正在不断暴露出由其自身特性所引发的严重隐患。”重庆邮电大学校长高新波表示，人工智能带来变革性社会进步的同时，也蕴含着巨大的风险和挑战。今天的人工智能系统只有当出现错误时才想办法进行弥补和修正，存在现有模型解释技术的精确性不够等问题。目前，人工智能在可信、可靠、可解释性上的隐患已经成为人工智能作为一个先进科学技术继续发展的巨大障碍。

例如，当用户与人工智能系统进行交互时，可能会涉及到一些敏感信息和个人隐私数据，这些数据有可能会被人工智能系统恶意窃取或者是无意泄漏，这会使个人隐私受到侵犯。又例如，以深度学习为核心的人工智能系统所依赖的训练数据中，往往会出现数据投毒、数据偏见、数据不均衡、标签噪声等，这些不良的训练数据将会误导人工智能系统，从而降低其可靠性等。

“我们必须加强对人工智能潜在风险的研判和防范，加强对可信、可靠、可解释人工智能的研究，以增强人类对人工智能系统的信心、信任和信赖。”基于此，高新波提出六点建议。

一是构建人工智能系统的自我监测机制；二是实施复杂大数据的解析计划；三是建议专项探索可解释性技术以解析网络运行和决策机制；四是建议针对可信可靠可解释人工智能构建产学研一体化的产业发展体系；五是产业界对人工智能系统存在的潜在风险需做足准备和应对；六是加速交叉学科人才培养形成国家战略科技力量。

“2021年全球网络空间安全态势严峻，随着新冠肺炎疫情肆虐，远程办公、网络社交等急剧增长，数据大量向云端迁移。同时，人工智能、大数据等新技术涌现，为网络犯罪开辟了新的途径。”西南大学人工智能学院院长段书凯说，按照国务院印发的《新一代人工智能发展规划》，到2030年，我国将成为世界主要人工智能创新中心。人工智能是新一轮科技革命和产业变革的重要驱动力量。

段书凯说，在AI赋能网络安全监管上，国内多个平台正在开展基于AI的网络舆情分析及响应研究，核心功能包含舆情监测、舆情预警、舆情分析、舆情报告四个方面。他认为，利用人工智能，可以防控网络水军和机器人散播的虚假舆论信息、检测虚假视频、伪造视频和假新闻等。使用AI领域的深度学习算法，可以高效识别社交平台中的违法信息，使用AI领域的卷积神经网络可以实现对违法图片和语音信息进行识别过滤，通过AI领域的贝叶斯分类算法，可以对恶意软件进行分析。

谈数字安全 以新技术支撑数字化安全稳定发展

活跃在网络安全防控一线的重庆市网络安全专家咨询委员会委员、奇安信集团总裁吴云坤，一直在研究数字化给网络安全带来的挑战。

他表示，网络安全发展的主脉络其实和信息化发展、信息化业务的发展紧密相关。如今，数字化已经深入到经济社会发展的全领域、各层级，而网络安全、数据安全与业务安全紧密相关，成为保障业务运营的基础，没有网络安全和数据安全，就没有数字化业务的正常运行。

随着数字经济发展，数字化带来的信息化环境的变化，使得整个网络安全保护对象发生了巨大的转变。“以前，我们需要保护的是云边端基础设施，现在延伸到了数据和应用，传统的保护方法、技术和模式都无法适应数字化下新环境的保护要求，保护难度明显加大。”鉴于此，吴云坤建议，从联合作战、精准防护、深度运营三个方面着手，不断提升网络安全免疫力，更好地解决日益复杂的网络安全难题。

重庆市网络安全专家咨询委员会委员、360集团副总裁、首席安全官杜跃进在主题演讲中开门见山地说，网络空间里面存在一个“谁来了不知道，是敌是友不知道，干了什么不知道”的现象。在今天，如果我们看不见对手、看不见新的方法，那所有的安全工作其实都是盲目的，效果不佳。

“新时代下，网络攻击者变得非常复杂，攻击手法也很复杂。随着中国的数字化发展，我们的网络环境也变得很复杂，在这种环境下，我们必须增强‘看见’的能力。”杜跃进表示，现在很多攻防已经变成全网的对抗，可能会利用供应链上的弱点，或团队里面人的薄弱环节进行攻击，所以面对一个威胁时要能够看到威胁背后的组织到底是谁，这个组织的动机到底是什么。

他建议，在面临日益复杂的数字世界和日益专业的网络攻击组织时，应建立起“安全大脑”，从而提升“看见”自己、“看见”他人的能力。

“人工智能、大数据等新技术涌现，为网络犯罪开辟了新的途径。”重庆市网络安全专家咨询委员会副主任、重庆电子工程职业学院人工智能与大数据学院院长武春岭认为，现在的漏洞或攻击层出不穷，防护代价也越来越大，如果单靠找漏洞、打补丁来解决，不利于整体的安全，必须构建基于主动免疫保护的一个新体系。他说，主动免疫是可信计算，是一种在运算的同时进行安全防护的计算模式，能及时识别“自己”和“非己”成分，从而破坏与排斥进入机体的有害物质，相当于在网络信息系统中注入了免疫的疫苗，起到免疫能力。

谈产业发展 网络安全迎来十大产业创新方向

北京赛博英杰科技有限公司创始人谭晓生和他的团队一直在关注网络安全产业的问题。在本次论坛上，他带来关于网络安全产业热点与发展趋势的主题演讲。

“现在正是网络安全产业投资的好时机。”谭晓生说，当前上市网络安全公司估值区间整体呈现收敛下降的趋势，带来了网安产业投资的好时机。

谭晓生认为，随着去年网络安全上市公司估值的下杀，使得网安上市企业总市值缩水50%，一些头部企业市值只有高峰时期的1/3，估值水平随之也处于历史低位。在企业处于价值被低估的阶段，恰恰是外界投资的好时机。

通过调研，谭晓生认为未来网络安全的头部赛道将聚焦于公共安全、隐私计算、数据安全、安全资产与测绘、综合安全等领域。

谭晓生说，网络安全的本质是攻防对抗，需要的是创意、创新。随着近年来网络攻击手段的翻新，网络防御也出现了一个空前的创新高峰，使得扩展检测与响应、入侵与攻击模拟、攻击面管理、安全运营、软件供应链安全、数据安全、云计算、SAES、API安全防护、欺骗技术成为了中国网络安全十大创新方向。

北京大学重庆大数据研究院副院长王涛介绍，在北京大学副校长张平文院士的带领下，北京大学大数据分析与应用技术国家工程实验室推动成立了“数字生态协同创新平台”，建立了科学评估数字生态的方法体系，开展了数字生态研究。“2021年，平台上的合作单位增加到20家，在重庆联合发布‘数字生态指数2021’。在数字生态指数的研究中，数字能力是数字生态的骨干支撑，包括数字人才、数字创新和数字安全等。数字安全是稳定数字生态的重要基石，这其中重要一项就是网络安全生态发展。”

在研究过程中，王涛发现，数字安全的发展是“政产学研用融”六大生态要素共同推动的整体发展。六大生态要素相互影响、相互促进、相互作用既是产业发展的客观规律，又是网络安全产业作为国家安全战略性产业的行业特点。

王涛说，北京大学重庆大数据研究院与重庆的企业、高校保持了紧密联系，打通了需求从产生到解决的关键链路。“我对重庆未来的发展充满了信心，希望能为推进重庆乃至全国的大数据智能化引领创新驱动发展贡献一份力量。”

网络安全，靠我们每一个人

□臧博

近日，2022重庆网络安全宣传周在巴南区正式启动。活动将在一周时间内推出重庆网络安全高峰论坛、六大主题日宣传等活动，帮助市民群众提高安全意识，增强防护能力。

安全是发展的前提，网络安全关系到经济社会发展，关系到政府、机构、企业和个人。守好网络安全防线，时刻不能松劲；保障网络安全，要靠我们每一个人。

网络安全，就在你我身边。对许多人而言，可能认为网络安全就是一个诈骗电话或钓鱼邮件，只需提高警惕就不会上当。其实，运动轨迹、人脸信息、消费记录等敏感信息，甚至快递面单、外卖消费单等，同样关联着网络安全。移动互联网和智能终端的普及，将每个人都置于网络触达的地方。近年来频频见诸报道的失密、泄密案件，就是个人身上出现了网络安全缺口，以至造成不同程度的损失。

网络安全面临的态势，从未像今天这样严峻。近日，西北工业大学遭受美国国家安全局网络攻击的报道刷了屏。外交部发言人也在发布会上指出了美国长期无差别监听中国手机用户的事实。面对内在和外在的网络安全问题，外来的安全风险可以通过国家力量主动防御来消除，内部的安全隐患则需要通过修炼好内功来击退。今年宣传周主题中的“网络安全靠人民”，就为我们保障网络安全，提供了思路和方法。

网络安全为人民，网络安全靠人民。最新数据显示，我国互联网普及率74.4%，网民规模10.51亿。面对这样的规模，筑牢网络安全防线，不是几个部门单打独斗能办成的事，而是需要凝聚共识，建立社会广泛参与机制。通过网络安全宣传周这样的专题活动，将相关知识送进机关、企业、学校和社区，送进青少年、中老年人等重点群体。广泛发动人民群众，让人人都置身事内，担起责任，从我做起，从良好的网络使用习惯做起，自觉做网络安全的维护者。依靠人民群众，汇聚起维护网络安全的强大力量，构筑起守护网络安全的长城。

网络无声，安全有界。以今年的网络安全周为契机，用通俗易懂、人民群众喜闻乐见的方式，普及网络安全知识、增强网络安全意识、提升网络安全防护技能，推动网络安全理念在重庆落地生根，筑牢全民网络安全“防火墙”，让市民在网络空间有更多获得感、幸福感、安全感。

2022重庆网络安全宣传周首推线上“云展馆”

本报讯 （记者 周尤 何春阳）9月6日，2022重庆网络安全宣传周活动在巴南区正式启动。

市委网信办有关负责人介绍，除开展网络安全高峰论坛外，今年的网络安全宣传周活动将举办网络安全体验展、网络安全赛事、网络安全优质服务企业（机构）推荐活动、网络安全普法短视频作品征集等10大类重点活动。

值得一提的是，为集中展示重庆市网络安全技术创新、产业发展、人才培养、宣传教育等各方面取得的丰硕成果，网络安全体验展将首次以线上“云展馆”（http://cq.cqnews.net/cqqx/html/col1810828.html）的方式和观众见面，集中展示重庆在网络安全产业方面取得的丰硕成果。展馆中包含了北斗卫星导航系统、华为鲲鹏高性能计算平台、城市安全运营大脑、云安全、智能网联汽车、区块链电子签章、星地一体量子通信、数字人民币、未来银行智慧营业厅、3D双目结构光学成像、智能车联网等“黑科技”。除了网络安全成果，观展者还能通过观看趣味动漫学习《数据安全法》《个人信息保护法》等网络安全法律法规。

与此同时，今年重庆网络安全宣传周将继续举办六大主题日活动。分别是：9月6日由市教委牵头组织开展校园日活动；9月7日由市通信管理局牵头组织开展电信日活动；9月8日由市公安局牵头组织开展法治日活动；9月9日由人行重庆营管部牵头组织开展金融日活动；9月10日由团市委牵头组织开展青少年日活动；9月11日由市总工会、市妇联、国家网信安全中心重庆分中心共同组织开展个人信息保护日活动。

宣传周期间，主办方还将利用江北“十屏联动”及渝中、沙坪坝、渝北等重点商圈户外大屏，轨道灯箱广告屏、公交车车载显示屏、机场航站楼显示屏、社区电梯广告屏等，广泛开展公益视频、标语和海报宣传，以线上与线下结合的形式，深入普及网络安全知识，增强群众网络安全意识和防护技能。