技术赋能安全管理 谱写网络安全新篇

编者按：2024年陕西省第十一届国家网络安全宣传周网络安全技术应用论坛9月9日在宝鸡举行。本报对参加论坛的6位网络安全领域的专家学者进行了采访，听听他们如何解读当前网络安全的新形势、新任务、新特点，畅谈管网治网新技术新手段，进一步汇聚智慧和力量，以推动我市网络安全工作再上新台阶。

注重人才培养 筑牢安全屏障

——访西安电子科技大学网络与信息安全学院执行院长李晖

本报记者 罗锐

“没有网络安全就没有国家安全，就没有经济社会稳定运行。网络空间的竞争，归根结底就是人才的竞争，要下大力气加强网络安全人才的培养。”9月9日，在2024年陕西省第十一届国家网络安全宣传周网络安全技术应用论坛上，西安电子科技大学网络与信息安全学院执行院长李晖在接受记者采访时说。

西安电子科技大学是全国首批开设信息安全本科专业的高校之一，也是首批获得网络空间安全一级学科博士学位授权点的高校之一，多年来为国家培养了一大批网络安全人才。李晖作为西安电子科技大学网络与信息安全学院的负责人，在移动互联网安全方面曾获得省部级科技进步奖一等奖4项、发明专利80余项等。结合30余年的教学经历和深入调研，李晖认为宝鸡管网治网能力持续提升，网络安全协调指挥体制逐步完善，网络安全整体态势平稳有序。

怎样加强网络安全人才培养？李晖认为，网络安全是一个实战性非常强的学科，部分高校的网络安全专业教学存在重理论轻实践现象，要进一步加强和优化教学环节，切实增强实战能力和攻防能力培养。他建议建立“四层渐进”网络安全实战能力培养体系，即通过实验、竞赛、实践、实战四个方面，不断增强学生应对各种网络安全风险的能力，进而培养一批高水平人才。

网络安全形势瞬息万变，网络安全人人有责。李晖说，网络安全运营维护从业者要针对行业的发展规律，自觉加强网络安全技能的学习和应用，更好应对网络安全的各种风险挑战。普通公民作为共同守护网络安全的参与者，要保护好个人信息安全，这不仅是维护自身权益的有力保障，还为共建网络安全、共治网络空间奠定了基础。

以AI大模型助力安全运营

——访360数字安全集团副总裁余凯

赵益

9月9日，在陕西省第十一届国家网络安全宣传周网络安全技术应用论坛上，笔者对360数字安全集团副总裁、安全大脑负责人余凯进行了专访。

作为工信部安全中心技术委员会的特聘专家，余凯长期致力于网络安全核心产品的研发与技术管理，拥有丰富的网络安全实战经验。“AI大模型能够识别和分析更复杂的安全事件，实现自动化、智能化的安全响应，大幅提升安全运营效率。”余凯表示，数字化浪潮中，大模型作为新质生产力的代表，已经成为了新一轮工业革命的引擎。

西安作为国家重要军工企业和军工院校的聚集地，承载着重要使命，宝鸡市以制造业见长，拥有大量的中小微企业。余凯表示，在一定程度上来说，360数字安全集团的“上山下海”战略与两座城市未来发展十分契合：“上山”即攻克科技难题，保护国家重点单位；“下海”则是下数字化的蓝海，帮助万千企业实现数字化转型，提供普惠的安全技术服务。

那AI大模型是如何在提升城市安全运营方面发挥重要作用的？余凯举例说，无人驾驶汽车的出现，不仅降低了网约车的成本，也为人们出行带来了极大便利。然而，这种智能化的背后也隐藏着网络安全风险。360数字安全集团利用大模型技术，为这些智能化系统提供安全防护，使其在遭受恶意攻击时能够稳定运行。在谈到AI大模型对日常生活的改变时，余凯指出，通过大模型的训练与优化，可以实现医疗诊断书的快速筛查、提高制造业的生产效率等，从而为百姓带来更多实实在在的便利。

展望未来，余凯表示，随着技术的不断进步和应用场景的不断拓展，AI大模型将在网络安全领域发挥越来越重要的作用。同时，他也呼吁更多企业和个人关注网络安全问题，共同构建安全、可信的网络空间。

筑牢人工智能安全监管防线

——访西安交通大学网络空间安全学院副院长刘烃

刘小祥

“随着人工智能领域的不断进步，我们的生活和工作也越来越依赖于智能化设施，但人工智能的发展也带来了不同方面安全上的挑战，如大模型容易遭受欺骗、存在潜在的被攻击风险、数据泄露等，这些都会危及信息安全。”西安交通大学网络空间安全学院副院长刘烃在接受采访时说。

西安交通大学是国内最早从事网络空间安全研究的高校之一。刘烃作为该校网络空间安全学院的副院长，曾主持国家重点研发课题、基金重点项目等。他认为，在当前网络环境下，我们不单单要保护个人信息数据的安全，更重要的是建立起对于全社会数据保护的监管机制。

人工智能技术与大众在交互时，个人隐私泄露风险点在哪儿？刘烃认为，人工智能技术本质上就是从个人的数据或者世界运行的数据中去找到一些规律，通过大数据、深度学习、自然语言处理等技术，帮助我们完成许多过去需要人工完成的事情。大众手握的智能设备会收集、存储和分析我们的个人数据，如果这些数据被泄露或滥用会带来极大的危害，这就需要相关法律法规的不断完善。

刘烃说，目前我国及全世界都在针对人工智能的安全和隐私制定相关的法律法规，但依然面临着诸多挑战：一是该如何在智能时代既保证数据流通充分产生价值，又要保证其安全；二是算法平台和算法的基座在发生重大变化，这对我们的保护提出了新的要求；三是人工智能技术正在进行一个商业变现的过程，在这项技术的发展符合大众要求的同时，对于数据保护也提出了全场景要求。在这样的背景下，对于人工智能领域数据保护问题，法律法规的完善会一直在路上。

优化顶层设计 构建安全体系

——访奇安信科技集团股份有限公司态势感知事业部总经理杨召

本报记者 罗锐

奇安信科技集团股份有限公司态势感知事业部总经理杨召曾主导全国20余个网络安全态势感知与协调指挥平台建设，对网络空间安全治理体系有着深入研究和丰富的实战经验。9月9日，在陕西省第十一届国家网络安全宣传周网络安全技术应用论坛上，杨召接受记者专访时说：“网络空间是高度复杂的庞大系统，网络空间安全治理及应对要持续加强和优化顶层设计，建立完整的网络安全治理体系。”

网络安全形势瞬息万变，新技术新应用迅速迭代，新情况新问题层出不穷，未知远大于已知，使得网络安全具有鲜明的技术性、专业性、前沿性等特点。杨召不仅是奇安信科技集团股份有限公司态势感知事业部总经理，还是中国网络空间安全协会人才培养工委专家、中央网信办协调指挥平台建设负责人。他说，当前一些政府和企业对整体网络安全现状如“雾里看花”般掌握不全，虽然开展了大量的安全防护工作，但网络安全仍会出现漏洞。

针对上述问题，杨召建议从三个方面下功夫：一要建立一套完整的网络安全治理体系，确保网络空间安全治理能够实现全覆盖；二要设定网络安全的阶段性目标和安全指标，严格落实主体责任，分时段分步骤保质保量完成；三要严抓过程和闭环检查，形成政企安全自治的闭环管理，进而夯实网络空间安全治理工作。他希望借助陕西省第十一届国家网络安全宣传周的机会以及企业的专业优势，与宝鸡的政企以及陕西其他地市达成合作意向，共同筑牢网络空间安全的“铜墙铁壁”。

挖掘数据要素价值 守牢数字安全底线

——访西北大学网络和信息化室主任孙骞

赵益

如今，数据已成为第五大生产要素，正在为生产生活插上“数字翅膀”。西北大学网络和信息化室主任孙骞接受采访时，就数据要素的价值与数据安全谈了自己的见解。

孙骞指出，作为数字经济和信息社会的核心资源，数据已成为社会生产的基本元素，其重要性不亚于传统时代的矿石资源。他说：“数据要素的价值与我们的生活息息相关，无论是教育选择、工作资料筛选，还是技术研发和工作创新，都离不开数据的支撑。”孙骞进一步举例说明，当前工业数字化转型正以前所未有的速度推进，精密机床的数字化转型已占据重要地位，大中型企业纷纷加入这一行列，构建新型数字化生产线。智能驾驶、地铁和高铁调度的全面数字化，更是彰显了数据在提升社会运行效率方面的巨大潜力。

在享受数据带来便利的同时，数据安全问题也日益凸显。孙骞表示，随着网络安全威胁的增加，个人隐私和国家重要数据的泄露已成为不容忽视的问题。“数据安全是信息化发展的生命线，必须得到全社会的高度重视。”孙骞指出，我国已经出台了一系列法律法规，明确了互联网平台在数据建设、采集、传输、利用和加工等各个环节的安全责任和义务。同时，他还呼吁个人提高数据安全意识、加强隐私保护。

谈及未来，孙骞对宝鸡市数字化转型寄予厚望。他指出，宝鸡作为典型的工业化城市，拥有全面的工业链，具备从工业数据化入手、推动数字化转型的坚实基础。他建议，宝鸡应抓住国家重点战略机遇，探索工业未来制造的新模式，为城市发展注入新活力。

以人工智能赋能网络安全

——访杭州安恒信息技术股份有限公司副总裁张海川

刘小祥

在AI时代，数据安全治理如何做到全程管控？杭州安恒信息技术股份有限公司副总裁张海川认为，仅靠过去的一些技术去解决现在的数据问题是很难的，通过“用AI对抗AI”的方式才可能解决内容安全问题。

张海川曾任华为技术有限公司安全产品研发经理和产品专家。他认为，人工智能在威胁识别、告警研判、风险评估、安全运营等方面具有独特价值和先天优势，因此利用人工智能技术为网络安全领域赋能成为大势所趋。

张海川告诉笔者，当前AI是非常火爆的一个领域，目前国内主流的安全厂商都在做“AI+网络安全”“AI+数据安全”“AI+运营”等方面的一些探索。AI大模型在数据分类分级工作中展现出巨大潜力，可以在极短的时间内完成大量数据的分类分级工作。此外，AI大模型还在数据防泄露领域发挥了重要作用，通过深入理解业务、制度和内容，AI大模型能够实现对敏感文档的精准识别和动态防护，为企业数据安全提供更加坚实的保障。

AI大模型如何助力数据安全落地？张海川认为，在工业领域，数据安全、网络安全关乎着国家安全。宝鸡在工业制造方面有很强的优势，可以大胆尝试通过用AI的方式为工业制造领域的网络安全和数据安全赋能，守护企业信息安全。同时结合技术创新和产业协同，助力企业实现产能提升。

“随着技术的进步和应用场景的拓展，AI大模型将成为保障数字世界安全的重要力量。”张海川说，AI与安全的深度融合将为我们带来更加美好的数字生活。

网络安全为人民 网络安全靠人民