第二届网络空间安全(天津)论坛圆满闭幕

共话安全 参与国家人数规模空前

昨日,为期3天的第二届网络空间安全(天津)论坛在天津滨海新区圆满闭幕。其间,近800位国内外嘉宾围绕“共建网络安全 共治网络空间”主题,共话网络空间安全形势、共享网络空间安全理念、共商网络空间安全对策。

中国工程院院士邬江兴进行专题报告 新华社发

专题报告主题演讲汇聚智慧力量

据介绍,本次论坛参与国家和人数规模空前盛大,国际刑警组织、国际反病毒测试标准化组织、亚洲反病毒研究者协会代表,以及美国、俄罗斯、韩国、新加坡等8个国家网络安全领域知名企业专家,83家中央国家机关部委单位,111家央企和金融机构,18家科研院所和高校,68家信息安全企业等近800名嘉宾参会。与会单位和嘉宾通过专题报告和主题演讲,进一步凝聚了全球网络空间治理共识,共创携手构建网络空间命运共同体新局面,进一步汇聚了全球智慧力量,推动网络安全技术革新实现新突破,进一步搭建了高端专业对话平台,为推进互联网前沿技术深度交流合作注入新动力。

俄罗斯卡巴斯基公司创始人尤金·卡巴斯基、大蜘蛛公司总监伊戈尔围绕关键基础设施系统网络免疫、恶意软件检测等方面分享应对策略,提出多种安全解决方案;韩国安博士公司病毒分析中心主任杨河英、新加坡IP认证公司总监博扬·埃里克、美国欧普斯安公司总监游承岳和美国泽斯科勒公司总监袁蔚豪,围绕网络安全威胁和移动认证等方面分享成功预防案例,从不同角度分析了存在的突出风险隐患。安天集团董事长肖新光、亚信安全科技公司副总裁吴湘宁从专业领域对网络空间对抗、网络勒索治理进行深度解析;曙光、华为、小米、阿里、绿盟、360等国内企业代表也围绕应对网络安全风险挑战进行了精彩演讲,共同分享网络安全领域的生动实践和真知灼见,引领网络空间安全技术变革创新风向,为加快形成网络安全新质生产力、推动网络空间治理贡献了智慧和力量。

网络安全大赛3个赛道攻防对抗

作为论坛的重要成果展现,第二届“天网杯”网络安全大赛,吸引来自全国近百支队伍的380名选手,围绕安全漏洞、大模型、智能网联车等新兴技术和产业设置3个赛道开展攻防对抗,进一步促进完善安全防御机制,为国家监管部门开展网络安全治理提供了重要参考范例与技术支持。其间,举办了网络安全法律专家咨询委员会专家聘任仪式,为加强国内外网络安全法律政策研究和网络法治建设建言献策,为公安机关开展网络犯罪防治等工作提供法律支撑。国家计算机病毒应急处理中心发布了《网络空间安全态势分析报告(2024)》《移动互联网应用安全统计分析报告(2024)》,分析梳理网络空间和行业领域出现的风险威胁,研究提出有针对性的防御措施和策略,为网络安全主管部门、行业机构和研究人员提供了系统全面和专业科学的信息参考,并联合十余家头部互联网企业发布移动互联网应用开发者自律公约,进一步规范移动互联网应用开发者行为,促进移动互联网应用行业健康发展。国家计算机病毒协同分析平台正式上线运行,集成国内外知名商业和开源计算机病毒检测分析引擎,为全球互联网用户提供优质产品的同时,加快推进计算机病毒治理国际合作,推动建立多边、民主、透明的互联网全球治理体系。

选手参加网络安全大赛 新华社发

网络与数据安全法治主题论坛

南开大学法学院副院长王强军教授提出,人工智能的快速发展,让人们看到其超越人类的可能及随时会带来的风险,而刑法基于扩张的本性对于人工智能可能产生的风险具有规制的强烈冲动,而且学术界已经表现出刑法介入人工智能风险规制的兴趣。从刑法介入的必要性到犯罪主体地位的确立,从刑事责任能力的程度到刑罚制度的设计,都已经有所论述。刑法过早地介入人工智能的风险规制存在一定的潜在弊端:一方面刑法规制的人工智能的风险并不明确、具体,有可能只是一种幻想;另一方面刑法过早介入人工智能的风险规制,可能会促使人工智能设计者和制造者在技术创新和刑法风险之间进行理性的选择,反而有可能不利于人工智能的发展。人工智能的风险规制应首先依靠伦理规范、技术控制以及法律保障,只有在上述规制措施失灵并且人工智能的风险成为现实时,才能让刑法被动地介入,而且应当进行刑法理论的积极准备。

天津市人民检察院第四检察部副主任杜晓霏介绍,随着涉网络犯罪总量不断攀升,传统犯罪也开始以网络为媒介,空间、手段升级翻新犯罪形式,对司法实务提出了挑战,检察实务中对于网络犯罪作出了应对与转变。一是对网络空间中有关概念理解的转变。对财产的理解需要结合现实与网络进行重塑;对人的理解需要结合网络取证特点认定。二是网络空间中有关规则适用的转变。传统共犯理论由共谋变为协作,情节认定规则也发生变化。三是网络空间中有关构成要件审查方法的转变。DDOS攻击类案件、提供VPN“翻墙”服务案件、爬虫软件类案件等均需要技术判断与法律评价双层切入。

大模型与数据安全主题论坛

围绕大模型与数据安全制度建设、数据安全保护技术发展、网络数据人工智能安全治理实践等热点话题,先进计算与关键软件(信创)海河实验室主任龚克、贵州大数据安全工程研究中心主任杜跃进等知名专家学者以及国家部委、科研院所、知名高校、业内前沿企业代表进行深入探讨,分享产业成果和先进经验。

“发展人工智能新质生产力是硬道理,不发展是最大的不安全。占据技术高地,才能相对安全。”龚克认为,人工智能的突破在于技术体系而非单个要素,不仅是数据和算力的支撑、模型规模的扩大,更是“机器学习”的进步,学会了语义的表达(词嵌入)、语义的理解(注意力机制),从而跨越了模态,相信人工智能仍将继续沿着深度学习的路线向前发展。当前,人工智能的所有风险主要来自两个方面,一是技术问题,缺乏坚实理论基础,存在基于概率的本征性问题等。二是应用问题,主要是误用、滥用、恶用和盲目依赖。对此,人工智能的治理要促进创新、确保安全和教育公民驾驭而非依赖人工智能。

杜跃进表示,数字经济、数字社会、数字政府,均将深度依赖数据和数据处理技术(人工智能技术),数字安全将影响人们的生产方式、生活方式和社会治理方式。目前除存在网络安全、数据安全的风险之外,数据污染和投毒、模型和算法安全、不可解释性及生成式AI的泛化特性用于业务决策等也存在着相应风险。在快速发展和变化中,唯有加强研究和实践,快速迭代和改进,并在充分利用数字革命带来的技术,发挥新的工作模式优势的前提下,才有可能应对大模型安全特有的新问题。

本版撰文 新报记者 张艳

与会嘉宾在论坛现场 新华社发

新报

新报微信平台