Tel:0311-88629263 责编:金明 美编:刘亚钦

外商争相“赶集”链博会,说明了什么?

新华社北京11月26日电(记者郭宇靖 吉宁)“我非常重视他们,没有中国的合作伙伴们,我们做不了现在做的产品。”11月25日,美国苹果公司首席执行官库克现身链博会现场,浏览展台。

用库克自己的话说,这是他第一次参加链博会。“很高兴来到这里,我很自豪苹果和我们的合作伙伴在这里参展。”

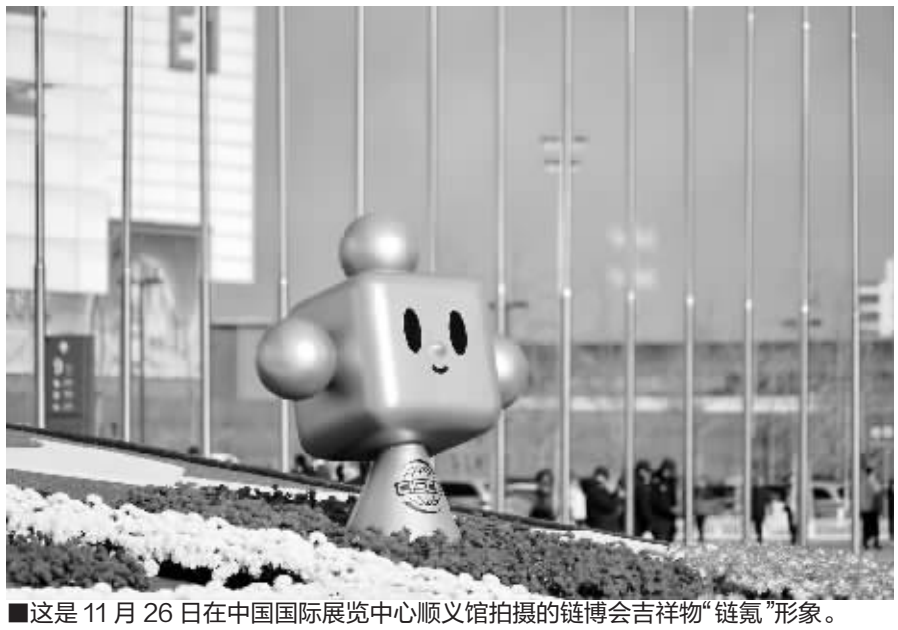
不止于苹果公司,本届链博会迎来了来自69个国家和国际组织的近700家展商,其中世界500强和行业龙头企业占比超过60%。在境外参展商中,欧美参展商的比重达到50%。

翻开嘉宾名单,记者看到了一长串跨国公司的高管:力拓集团董事长鲍达民、正大集团资深董事长谢国民、德国思爱普全球高级副总裁骆才、住友电气工业株式会社会长松本正义……

来到展台,马士基、住友电工、强脑科技等陆续首发首展首秀70多项产品,苹果、特斯拉、高通、星巴克……一个个耳熟能详的企业纷纷在展台亮出“绝活”。这里面不但有首次参展的“头回客”,也有尝到了甜头的“回头客”。

主办方透露,第二届链博会的展览面积由首届的10万平方米增至12万平方米。尽管如此,展区仍然“一位难求”,不少有意愿参展的企业遗憾未能成行。

知名外企及高管争相来“赶集”,链博会到底有啥魅力?



■这是11月26日在中国国际展览中心顺义馆拍摄的链博会吉祥物“链氪”形象。

新华社记者 肖恩楠 摄

链博会,全称是中国国际供应链促进博览会,是我国举办的全球首个以供应链为主题的国家级展会。从本届链博会“链接世界 共创未来”的主题,就可以看出实现各方携手合作、互利共赢的初衷。

跨国公司纷纷参展,首先看重的是中国完整齐备的供应链体系,在这里他们能够寻找到全球配置资源中最佳的供应链合作伙伴。例如,过去5年,苹果公司在中国智能制造和绿色制造的投资超过200亿美元,此次不仅携带4家供应商参展,而且展台醒目标出:“Apple的200家主要供应商中有超过80%在中国生产”。

链博会展示的不是散点式的零部件或者产品,而是完整的产业链条,这就给产业链上的企业,提供了携手合作的绝佳机遇。

以智能汽车链为例,一辆新能源汽车,超过1万个软硬件才能联珠成串。从核心原材料、关键零部件,到电池、电机、电控,再到智能网联整车产品和服务,链博会覆盖了智能汽车产业全生命周期的展示,一下打通了产业的价值链。

外商纷至沓来,还看好持续向好的中国市场。全面取消制造业领域外资准入限制、大幅缩减外商投资准入负面清单、加强外商投资服务保障……我国政策释放了持续扩大高水平开放、利好外商在华投资兴业的积极信号,参展外资企业对中国经济前景投出信任票。

麦当劳中国首席执行官张家茵对链博会信心满满:“这个平台能让供应链‘朋友圈’合作进一步深化,不断提高效率,这必将大幅提升产品质量,更好地服务餐厅和消费者。”

外商云集链博会,也展现出各国企业对加强产供链合作的需求和期待。

力拓集团首席商务官巴特尔说:“中国在电动汽车等新能源领域占据领先地位,持续推动全球能源转型的需求,为公司与中国伙伴拓展合作带来更多机遇。”

通过链博会,中国正向世界发出积极的信号——愿与各界携手合作,共同构筑安全稳定、畅通高效、开放包容、互利共赢的全球产业“共赢链”。

AI接管方向盘,能更安全吗?

□半月谈记者 郭方达

让AI接管方向盘,把车辆行驶安全托付给电脑,这样的场景如今不再稀奇。伴随车联网技术在社会生活中的加速渗透,“无人驾驶”的应用场景势必不断扩容。但从安全角度而言,针对车联网平台的网络攻击连年攀升,网络安全、数据安全等现实挑战依旧制约着“聪明的车”与“智慧的路”。回答好安全这道必答题,才能给车联网的发展系紧安全带。

智能网联下的网络安全和数据安全

截至7月底,我国已建设17个国家级智能网联汽车测试区、7个车联网先导区、16个智慧城市基础设施与智能网联汽车协同发展试点城市,开放测试道路32000多公里。

智慧出行不断有新进展,这背后是近年来我国在5G网络、高速公路、智慧城市等方面的持续投资。但悄然而生的安全隐患也与日俱增。中国信息通信研究院监测数据显示,2023年针对车联网服务平台等攻击达805万次,同比增长25.5%。

中国汽车技术研究中心有限公司首席专家张亚楠认为,与过去聚焦于车辆自身的安全不同,随着智能网联汽车行业的快速发展,更多来自驾乘主体之外的相关方能够对系统施加影响,衍生出一系列新的安全问题,其中又以网络安全和数据安全为甚。

在车联网环境中,车辆之间通过数据交换和信息共享来更新道路状况、车辆位置等信息,以此来改善交通状况、避免事故。然而,网络环境的开放性使传输的消息面临大量安全威胁,包括但不限于假冒攻击、重放攻击、修改攻击和签名伪造等。

天津大学无人驾驶汽车交叉研究中心主任谢辉举例说,如果恶意车辆接入网络中,可以生成并发送虚假的紧急消息,误导周围车辆的行驶路线、行车速度和前进方向等,从而制造交通拥堵与混乱,甚至可能主动制造交通事故。

在网络安全风险之外,数据及隐私泄露同样是消费者关注的问题。借助蓝牙、网络或者其他接口,不法分子能够侵入车辆系统,进而控制组件并盗取数据。从驾乘人员的面部表情、动作、目光、声音数据,到车辆地理位置、车内及车外环境数据,汽车数据隐私泄露所引发的争论愈发常见。“由于通信环境的开放性,被窃取的隐私数据会轻而易举地散布出去。”谢辉说。

行驶安全,不可“亡羊补牢”

受访专家认为,车联网具有“五危一体”的安全特性,即与人身安全强相关、风险范围异常广泛、数据庞大流通难控、智能联网监督难管、多网融合风险蔓延等特性。

有别于传统网络安全“附加性”“亡羊补牢”的技术定位,车联网的安全技术应该处于关键且前置地位,其挑战存在于三个方面。

一是新场景新技术带来的不确定性尚待研究。张亚楠举例说,自动驾驶或者高级辅助驾驶功能应用中,可能会出现场景无法识别、误识别、目标丢失等传统车很难遇到的新问题。由于相关技术直接关系到驾乘人及行人的生命安全,因此技术演进相对谨慎,相关问题也需要更多场景和时间进行数据收集及分析研究。

二是固有的网络安全模式风险防范能力不足。谢辉认为,“天天打补丁,周周OTA(车辆功能与车机系统的在线升级)”已经成为不少车企的常态,但沿袭自互联网企业的“亡羊补牢”式防御对于驾乘人而言并不安全。谢辉举例说,不久前微软因一款软件更新错误导致全球范围内出现大规模蓝屏,多个国际航司遭遇停飞,波及金融、医疗等多个领域。“如果类似的事件突然发生在大量高速行驶的汽车上,后果难以设想。”

三是部分信息边界模糊权属不明,法律界定存在真空地带。目前,车辆及零部件工况类数据,道路、天气等与外部环境有关的数据,不与具体个人相连接,在数据处理上相对简便,但一些车控数据、应用服务数据则难以界定权属。“比如驾驶员的驾驶习惯、对车载应用的偏好等等,还需要在法规上予以明确。”上海澄明则正(北京)律师事务所律师刘慧磊说。

产业“安全带”还需进一步系紧

——持续完善顶层设计,厘清责任链条。刘慧磊建议,在目前的行业共识基础上,由主管部门与行业协会牵头,制定车联网领域网络和数据安全风险评估办法、重要数据识别等细则文件,确保智能网联汽车产品开发、测试、上路等全生命周期以及数据全流程的合规性和安全性。此外,还应将监管链条延伸至全产业链,提倡从整车向零部件环节前移的安全检测规范,构建全面覆盖硬件、软件、通信和数据等方面的综合性安全监管体系。

——聚集行业力量,形成风险数据库,加速安全技术迭代。张亚楠认为,与传统汽车产业的研发过程不同,车联网领域亟需构建协同的安全生态,应颠覆过去封闭的技术研发体系。要开展安全漏洞库的行业共建,通过汇聚业内的经验数据,提升风险资源反馈度,为行业安全产品与攻防技术提供更为广阔的应用场景和迭代演进的机会。

——加速形成产学研合作等技术攻关机制,丰富人才供给。谢辉建议,一方面,结合企业实际用工需求,开设智能网联汽车网络和数据安全相关学科专业和培训课程,设立安全实训基地,规模化培养高水平对口人才。另一方面,企业、高校及科研机构,也应将安全技术作为未来研发的重点,“尤其是数据开放层级问题,车辆位置、用户信息等关键数据如何掌控,如何做到实时有效监管,都是未来技术发展的必答题”。

——鼓励金融领域创新,持续赋能行业发展。受访专家认为,应积极引入外部风险保障体系,如加快推动保险等金融工具在智能网联汽车领域的试点工作。通过提供风险分散工具,加快铺开相关技术的应用场景,降低实践过程中的风险损害,为安全技术的发展成熟提供有力支撑。

(据新华社)