市七届人大一次会议第20210297号建议

案 由：关于加强智能网联汽车信息安全监管的建议

提 出 人：陈琳,周彬,陈琰超,陈湘宇,肖文杰,葛岩峰,何珊珊,曾俊英,邱小燕(共9名)

办理类型：主汇办

承办单位：市交通运输局(主办),市委网信办,市发展和改革委员会,市工业和信息化局

密 级：公开

内 容：

一、相关背景及现状

智能网联汽车，是指搭载先进的传感器等装置，融合现代通信与网络技术，具备智能决策等功能，最终实现替代人操作的新一代汽车。其包括有条件自动驾驶、高度自动驾驶、完全自动驾驶三个技术等级。一方面，随着汽车智能网联化的进一步发展，汽车将从单纯的出行工具进化为融合出行、娱乐和办公功能为一体的移动智能空间；另一方面，随着技术的不断升级发展，智慧城市基础设施与智能网联汽车的协同发展不断深化成熟，汽车L5级别的自动驾驶/无人驾驶技术正离我们越来越近。根据公开信息，我国智能网联汽车相关企业数量已超过4000家，其中约两成分布在深圳。目前，深圳已在9个区开放智能网联汽车测试道路里程144.69公里，发放道路测试牌照14张，累计道路测试总里程达18638公里，开放区域、开放里程及牌照发放数量都位居全国前列。

在智能网联汽车产业高速发展的同时，科技的发展加剧了信息安全的复杂性，智能网联汽车的信息安全问题不断凸显。根据360发布的智能网联汽车信息安全年度报告，2018年全年爆发14次智能汽车信息安全事件，其中包括5起数据泄露事件和9起汽车破解事件；2019年智能网联汽车发生了“十大安全事件”，其中包括基于通信模组信息泄露的远程控制劫持攻击、基于生成式对抗网络（GAN）自动驾驶算法攻击，特斯拉PKES系统存在中继攻击威胁，特斯拉Model S/X WiFi协议存在缓存区溢出漏洞，共享汽车APP存在漏洞，基于激光雷达的自动驾驶系统安全性存疑，Uber爆出存在账号劫持漏洞，后装汽车防盗系统存在漏洞，丰田汽车服务器遭到入侵，宝马遭受APT攻击。

二、存在问题及主要原因

当前智能汽车信息安全风险主要体现在如下四大方面：汽车攻击事件快速增长，攻击手段层出不穷；智能网联汽车缺乏异常检测和主动防御机制；数字钥匙成为广泛引起关注的新攻击面；自动驾驶算法和V2X系统将成为新的热点攻击目标。

相较于传统汽车安全，自动驾驶汽车安全的特征主要表现为网络数据系统通过感知层、通信层、软件层、云端等来判断和操作驾驶功能，但这些网络单元均存在被入侵的风险，一旦发生自动驾驶数据系统被入侵，摄像头和后台数据算法均无法很好地运行，可能导致失去车辆控制权，造成严重的交通事故。

此外，每一台无人驾驶汽车都会进行移动高清的视频采集，还有激光、雷达、毫米波等先进的数据采集系统，对整个城市的静、动态信息实时采集，数据泄露风险巨大，存在很大的信息安全隐患。如何保证个人信息、国家信息安全，是社会各界需要重点关注的问题。

三、具体建议

随着国内外智能网联汽车产业的发展，相关政策标准法规研究制定进入了密集期。2021年3月22日，深圳市人大常委会发布了《深圳经济特区智能网联汽车管理条例（征求意见稿）》（以下简称“《条例》”），征求意见于4月11日截止。《条例》第五章“网络安全和数据保护”规定深圳市互联网信息部门应当对智能网联汽车产品、服务及其供应链存在的网络安全风险进行监督管理，具体监督管理办法由市互联网信息部门另行制定，并要求智能网联汽车相关企业采取相应措施保证网络安全和实施数据保护。由于后续各部门的配套细则尚未出台，相关监管政策亟待细化，现对此提出建议如下：

1.建立智能网联汽车信息安全责任体系。建议明确汽车厂商对智能网联汽车信息安全保障的主体责任，促使厂商提高技术能力，开发车端安全通信模组、安全汽车网关等新型安全防护产品，主动发现攻击行为，并及时进行预警和阻断，通过多节点联动，构建以点带面的层次化纵深防御体系。

2.建立智能网联汽车信息安全全生命周期管理体系。建议相关部门在概念、开发、生产、运营、维护、销毁等阶段对汽车网络安全工作进行全生命周期的规范及监管，促进风险评估融入汽车生产制造的全生命周期，并逐步推进智能网联汽车信息安全强制测试，持续对网络安全数据进行监控。