你的汽车会被黑客远程操控开走吗？

智能网联车安全成焦点

你的汽车会被黑客通过远程操控开走吗？你的隐私数据会被上传到网络公布吗？行驶中的汽车，制动会突然失灵吗？这一切都不是科幻电影，而是智能汽车时代你将要面对的现实。

随着汽车智能化、网联化程度的加深，汽车在成为可移动、可交互的智能网络终端，为生活带来便利的同时，也产生了远程攻击、恶意控制、隐私保护、数据安全等问题。

智能网联车安全成为公众关注的焦点，万亿美元的市场规模也令业界关注。2021年全国两会上，来自电子信息及汽车行业的代表委员围绕构建智能网联车“系统安全”展开热议。

智能网联车安全问题集中产生

2020年以来，智能网联车安全问题集中爆发引发公众关注。2021年两会，代表委员提交了十余份提案、议案，深入审视车联网的安全风险。

2020年，一名黑客针对特斯拉汽车成功开发了新的密钥克隆中继攻击，不到5分钟，一辆价值70多万元的特斯拉就被远程控制开走了。2020年9月，国内网络安全龙头企业——奇安信的车联网安全研究员演示通过远程方式在线开启了一辆智能汽车的车窗、后视镜，随后汽车被启动、上路。

事实上，早在2015年，两名白帽黑客就远程入侵了一辆正在路上行驶的切诺基（自由光），并对其做出减速、关闭引擎、突然制动或者制动失灵等操控，克莱斯勒对此不得不在全球召回了140万辆车。

不仅如此，作为移动数据收集和发射器，每一辆智能车都可以获取车主身份、行动轨迹、驾驶习惯、与手机蓝牙绑定的通讯录、谈话等内容，车主行驶所到之处，人、地、事、物均一览无遗。汽车联网后，上述安全风险更为突出，车载数据过度采集和越界使用，不仅侵犯了用户隐私，更威胁到国家安全。

据Upstream报告数据显示，公开报道的针对智能网联车网络安全攻击事件，由2018年的80起激增到2019年的155起，2020年整车企业、车联网信息服务提供商等相关企业和平台的恶意攻击已达到280余万次。

“信息安全是继主动安全、被动安全、功能安全之后，汽车领域的第四大安全问题。智能网联车的信息安全不仅可能造成企业经济损失和个人隐私泄露，还可能对人身安全造成严重后果，甚至引发威胁国家的公共安全问题。”全国十三届人大代表、中电工业互联网有限公司党委书记、董事长朱立锋告诉记者。

“新安全底座”崛起的千亿级市场机遇

智能网联车发展带来的安全风险引起了政府部门、企业和用户的共同关注，也带来了巨大的市场机遇。

2020年2月，中央网信办等11部门联合发布《智能汽车创新发展战略》，明确提出要确保用户信息、车辆信息、测绘地理信息等数据安全可控。完善数据安全管理制度，加强监督检查，开展数据风险、数据出境安全等评估。

2020年12月，住房和城乡建设部、工业和信息化部联合发布《开展智慧城市基础设施与智能网联汽车协同发展》文件。2021年2月24日，《国家综合立体交通网规划纲要》印发，提出建设融合感知平台，推动智能网联车与现代数字城市协同发展。

国家政策的层层加码，让智能汽车安全这一细分市场开始崛起。麦肯锡曾预测，智能网联车产业生态链在2025年的经济规模将达到1.9万亿美元，而中国将是全球智能网联车产业发展的重要推动者和受益对象。中国工程院院士、国家智能网联车创新中心主任李骏形容智能汽车“将形成全新的、十万亿级的、对未来产生深远影响的新型产业生态体系”。多位行业专家预测，细分的智能汽车安全市场将是千亿规模。

2019年12月30日，一辆进行自动驾驶载人载物测试的汽车行驶在测试道路上（资料图）。 新华社发

全国人大代表、小康股份创始人、董事长张兴海认为，要确保国家数据安全，应将数据安全作为新的必备指标之一，推动和扶持自主品牌着力发展三电（电池、电驱、电控）及智能联网等核心技术。

“不仅仅是硬件安全，软件安全也将成为智能网联车行业的‘新安全基座’。”奇安信总裁、中电车联董事长吴云坤指出，“要为智能车辆构建起纵深防御的安全框架体系，汽车企业将与信息安全企业共同探索融合创新的智能汽车安全解决方案，共建车联网安全技术生态，这其中包括智能网联车网络安全技术中心、汽车行业工业互联网安全大数据运营中心等。”

据了解，奇安信先是在内部成立了奇物安全实验室，专注于智能网联车安全技术研究，其后在2019年11月的湖南网络安全智能制造大会上，奇安信联合北汽蓝谷信息、中电互联成立车联网安全体系实验室，研究方向包括安全技术、安全评测认证、汽车工业互联网安全等。

2020年，奇安信与中电互联合资成立中电车联，深度聚焦“5G+车联网+安全”领域，目前已研发了车联网安全评估评测、智能网联车示范安全产品和服务体系。同时，奇安信和北汽、长安汽车、广汽、吉利、上汽等十多家车企直接展开合作。

构建国家级的智能网联车“系统安全”

在保障智能网联车安全上，一方面车企和奇安信等安全企业开始进行探索实践，另一方面国家相关部门也加大了安全推广力度。

公开信息显示，在工信部公布的相关技术应用示范项目中，对于智能网联车系统安全就有明显的涉猎。其中，奇安信打造的车联网网络安全综合服务平台、车联网安全测评系统成为2020工信部网络安全技术应用试点示范项目。奇安信的车联网内生安全终端主动防御系统以及车联网安全运营管理中心两大项目成为2020-2021工信部科技司物联网关键技术与平台创新类、集成创新与融合应用类示范项目。

在今年两会上，代表委员纷纷建议中国智能网联车产业已然进入快速发展期，智能网联车的“系统安全”应提前布局、同步规划、协同发展。

“要以安全牵引全面推动智能网联车、智能网联道路与现代数字城市协同发展。”朱立锋说，建议前置智能网联车信息安全测试工作，进一步完善基于智能网联车行业数据对培育信息安全相关的规范、标准和技术监管，支持在智能网联车概念设计阶段将信息安全前置规划，提倡以先进技术保障过程安全。同时，应建设基于信创体系的智能网联车大数据安全态势感知等关键技术平台应用，探索基于智能网联车数据+区块链+保险+数字人民币的新模式，助推行业安全发展。

全国人大代表、上汽集团党委书记、董事长陈虹则表示，国家层面应建立准入制度，智能网联车的数据（包括高精地图数据）的采集、存储和商业用途需要经过相关部门备案管理。智能网联车的制造和销售企业应高度重视信息安全风险，要建立完备的数据安全管理和软件升级流程。

全国人大代表、广汽集团党委书记、董事长曾庆洪建议，发展智能网联车，法律法规要走在前面。须尽快完善现行交通安全法规，确认“机器驾驶人”的法律主体资格；加快自动驾驶相关技术标准的编制和发布；完善道路测试相关政策法规。

曾庆洪指出，在保障现有“单车智能”技术路线的同时，应大力支持“车端智能+网联共享”相结合的技术路线，鼓励互联网安全企业关注车联网安全，支持车企与信息安全企业联合研发，共同推动智能网联车产业的发展。

据《武汉晚报》