

自动驾驶陷信任危机 “行业黑话”亟待规范

□ 孟佳惠

连日来,全球新造车行业的顶尖公司都过得不太自在。

中国这边,蔚来汽车卷入了一起“年轻创业者开着自动驾驶出车祸身亡”的案件。目前,事故尚无定论,众说纷纭。

而在美国这边,在特斯拉 Autopilot 辅助驾驶引发接连不断的事故之后,美国国家公路交通安全管理局宣布,美国政府对特斯拉自动驾驶系统启动正式调查,称该系统“难以识别停放在路边的紧急车辆”。

特斯拉存在安全隐患

根据美国国家公路交通安全管理局提供的相关数据显示:自2018年1月起,已经发生至少11起由特斯拉 Autopilot 引发的交通事故,撞上有闪烁灯光、发光箭头指示牌或反光锥形牌的警车等其他紧急车辆,鉴于其安全性问题,目前已对特斯拉展开调查。

据了解,此次调查涉及特斯拉在美国发售的2014~2021款,包括 Model S、3、X、Y 在内的全部车型。也就是说,自从2014款发布之后,在美国交付的全部特斯拉车辆,都属于本次调查的范围。

需要明确的是,这次美国政府

的调查,并非涉及一般性质的交通事故,而是专门针对特斯拉汽车在开启 Autopilot 或其他辅助驾驶功能的情况下,仍然无视应急车辆(比如警车、消防车、救护车等)所造成的车祸事故。

面对应急车辆,特斯拉依然“瞎眼”,或许这表明其辅助驾驶功能确实存在设计安全隐患。

“大部分事故发生于夜间,并且现场已经开启了警告措施,包括车辆闪灯、燃烧照明棒、亮灯的告示牌和交通锥等。”美国国家公路交通安全管理局有关负责人提到,上述事故中的特斯拉汽车都开启了 Autopilot 或交通感知巡航系统(TACC),仍然会毫不犹豫地撞上去,就好像没有收到系统的警告信息一样。

将视线转移回国内,其实近两年来,国内也发生了很多关于特斯拉车辆自动驾驶的安全事故。其中有一部分正是由于智能系统出现问题,这让公众对特斯拉的车辆安全打了一个问号。

据报道,在国内发生的数十起特斯拉交通事故中,有 Model 3 失控冲入加油站的,有失控冲向停车场门禁杆,有连续撞到多辆车后发生侧翻的;也有 Model Y 在街道上正常行驶,突然加速撞翻车辆和行人,造成多人伤亡的。另外,一

些车主在停车场尝试唤醒 Model Y 时,不料车子与停车场地面石球或柱子发生撞击,造成车辆受损。

对于这些事故,虽然特斯拉方面将原因归结为路面湿滑或车主操作不当等。但业内人士普遍认为,这些事故频繁而集中的出现,实在摆脱不了品控质量的问题。

自动 or 辅助亟待明确

8月12日下午2点多,年仅31岁的福建籍蔚来ES8车主、美一好品牌管理公司创始人林文钦,驾驶一辆蔚来ES8在沈海高速涵江段追尾前方工程车后不幸去世。事故发生后,引起了广泛的关注,关于自动驾驶和辅助驾驶的讨论也越来越激烈,多位汽车品牌创始人都在社交平台上发表了对自动驾驶的看法。

理想汽车创始人李想表示,呼吁媒体和行业机构统一自动驾驶的中文名词的标准:L2=辅助驾驶,L3=高级辅助驾驶,L4=自动驾驶,L5=无人驾驶,避免夸张的宣传造成用户使用误解。

随后,360创始人、董事长周鸿祎也发了朋友圈表示赞同。他认为:“人工智能不是营销话术,没有那么神奇,自动驾驶、无人驾驶还有很多路要走、很多坑要填,不能为了营销而误导用户,

L2~L5都是‘行业黑话’,行业内部自娱自乐没有问题。但是面对消费者,还是应该使用可以望文生义的简单概念。”

据了解,在汽车标准化组织SAE International 于2021年4月最新发布的《SAE驾驶自动化分级》中将驾驶自动化等级划分为L0~L5共六个等级。其中L0~L2级驾驶自动化被定义为驾驶员支持功能,L3~L5级为自动驾驶功能,其中L3级自动驾驶可视为高阶自动驾驶与低阶自动驾驶的分界线,其要求驾驶员需要时刻准备接管。若是基于这一等级划分,当前造车新势力们在量产车中搭载的辅助驾驶功能,大都介于L2~L3级自动驾驶之间。

事实上,辅助驾驶功能的出现,有效地提升了驾驶安全性。欧盟委员会的有关研究表明,如果在欧洲市场销售的新车全都配置自动紧急制动系统,交通事故可以减少27%,每年平均能够挽救大约8000人的生命,还能够很大程度上降低重伤率。

这一数据,证明了辅助驾驶功能的有效性。专家也提醒,在现阶段技术条件下,盲目信任汽车厂商们推出的辅助驾驶功能,完全将驾驶操作交给辅助驾驶功能是完全不可取、极为不安全的。

过度宣传或为罪魁祸首

目前,世界各国的法律法规并没有对智能汽车的辅助驾驶系统做出明确责任的规定,这就仿佛进入了一个灰色地段,也是舆论风向摇摆不定的重要原因。比如,很多网友就吐槽车企的营销,“买前自动驾驶,出事辅助驾驶”。

上海因伽律师事务所主任杜伟也表示,按照我国现行法的规定,汽车在公路上行驶需要遵循《道路交通安全法》《公路法》等相关法律法规的规定,但是针对具有自动驾驶或辅助自动驾驶功能的汽车,目前并没有具体的法律规定。

“车企在大力宣传自动驾驶功能的同时,用户对相关功能概念又并没有很好的认知,造成双向错觉,最终使得不少驾驶员因为过度信任‘自动驾驶’,惨丢性命。”专家表示,作为车企,他们自身对“自动驾驶”与“辅助驾驶”之间的区别再清楚不过,然而在对外宣传时,各种夸大现象依然不断出现。

2019年8月,蔚来汽车副总裁沈斐曾在ES8里,开着NIO Pi-lot 吃星巴克外卖,还拿手机拍了一段7秒的小视频上传到社交网络,让人感觉自动辅助驾驶真的不用司机了。小鹏汽车也在一段宣传视频中表现了类似的情景,开启NGP功能后,驾驶员可以在车上自拍甚至喝咖啡。目前,尽管这两段视频均已被删除,但给广大消费者留下的印象依然深刻。

特斯拉在宣传自家的 Auto-Pilot 时,一开始也是直接用上了“自动驾驶”四个字。在国内外不断有用户因为使用 AutoPilot 发生车祸遇难后,特斯拉(中国)才把宣传中的“自动驾驶”改成了“自动辅助驾驶”。

“无论是L2还是L3,都有个功能叫‘自动紧急制动’,理论上讲汽车在遇到障碍物时应该会紧急制动,但还是发生了车祸,说明技术不成熟有缺陷。现在的车企就是希望通过‘自动驾驶’作为卖点来卖车,特别是造车新势力们也都是靠智能汽车作为亮点来卖车的,卖车过程中通过模糊的概念,来向消费者传递自动驾驶功能特别强。”上海大学悉尼工商学院创业导师、汽车分析师张翔说道。

面对接连出现的因使用辅助驾驶系统出现安全事故,专家普遍认为,与其反思、批判辅助驾驶技术,更应该规范的是业内对于辅助驾驶技术的种种宣传。

通过浏览各车企官网和宣传片可以发现,大部分车企在对外宣传辅助其产品搭载驾驶技术时,都存在对其功能性的部分夸大以及对功能使用的错误示范,从而给用户释放了一种可以完全信任辅助驾驶系统的错误信号。正是这种错误示范和信号,使得部分用户在盲目技术信任以及求新、求奇心态驱使下,做出了将驾驶权完全交给辅助驾驶技术的错误选择,从而造成交通事故乃至悲剧。

“机器进入人类社会和人类共生的时候,机器是一定会造事故率的,只是我们要竭力将其降到最低。”前华为智能驾驶部门高管苏青曾表示,车企厂商们在进行功能宣传时,还是需要保持克制,站在实事求是的立足点上理性宣传,致力于让用户拥有更好、更安全的驾驶体验。



罗马尼亚启用欧盟数字新冠通行证

罗马尼亚从8月13日开始启用欧盟数字新冠通行证。按照规定,所有前往其他欧盟成员国旅行或从欧盟成员国返回罗马尼亚的人员必须出示欧盟数字新冠通行证。图为一名女子在罗马尼亚首都布加勒斯特的亨利·科安德国际机场出示带有二维码的欧盟数字新冠通行证。新华社发(克里斯泰尔 摄)

海外传真

法国对谷歌开出“天价罚单”

本报讯 新加坡《联合早报》网站近日报道称,法国反垄断监管机构近期又对谷歌开出5亿欧元的天价罚单,原因是这家科技巨头未能遵守与当地新闻机构与出版商达成公平协议,以在其平台上使用新闻内容的命令。

报道称,这是法国有史以来针对单个公司开出的金额第二高反垄断罚款。根据法国监管部门发布的信息,谷歌必须在接下来的2个月内,提出如何补偿新闻机构和其他出版商的建议,否则它将面临每天高达90万欧元的额外罚款。

法国监管部门称,5亿欧元的罚款考虑到了其所观察到的违规行为的异常严重性。谷歌发言人则表示,对这一决定“非常失望”,并认为公司“在整个过程中都是善意的”。谷歌补充说,它即将与法新社达成协议,其中包括一项全球许可协议。谷歌可对此次的处罚提出上诉。

今年6月初,谷歌同意支付2.2亿欧元,与法国反垄断监管机构达成和解。根据和解条款,谷歌承诺改善其广告服务与第三方广告服务器、销售平台的可交互性。(何欣)

价值6亿美元加密货币被盗

本报讯 据西班牙《经济学家报》网站近日报道,价值6亿美元的加密货币被盗,这可能是史上最大规模的加密货币盗窃案。黑客利用了 Poly Network 中的一个漏洞,该平台旨在连接不同的区块链,以便它们可以协同工作。

据美国消费者新闻与商业频道报道,该平台谴责黑客实施的攻击。但是最新消息显示,这些网络犯罪分子已经开始归还部分赃物。Poly Network 发布了致黑客的一封信,请求他们归还属于“人民”的资产。

报道称,尽管如此,加密货币市场近日依旧平静。更令人惊讶的是,比特币和以太币等大型加密货币的涨幅超过1%,价格创下最近几个月的新高。

Poly Network 在致黑客的信中表示,希望与肇事者“建立联系”,并指出“其盗窃金额是‘去中心化金融’历史上最高的”,成千上万该平台用户受到了影响。据英国《金融时报》报道,Poly Network 被盗的代币价值总计约为6亿美元,其中以以太坊区块链损失价值超过2.7亿美元。(朱晓)

微软抗议亚马逊获政府百亿订单

本报讯 亚马逊旗下云服务部门(AWS)被曝出获得美国国家安全局(NSA)价值百亿美元业务合同后,美国媒体近日报道称,亚马逊竞争对手微软已提出抗议,希望取消美政府部门与亚马逊的合同。

微软提交的抗议文件显示,亚马逊拿到的合同是由美国情报部门在过去一年中授予的第二份价值10亿美元以上的云业务合同。美国共有17个情报部门,国家安全局是其中之一。美国国家安全局几乎没有提供上述云业务项目用途的细节。这家机构一名发言人拒绝说明哪家企业赢得这份合同。这名发言人说:“国家安全局将依据恰当的联邦规定应对抗议。”

有报道认为,国家安全局将如此巨额合同授予单一企业,必然会在国家安全生态系统引发争议。

去年11月,中央情报局(CIA)已经将其C2E合同授予AWS、微软、谷歌、甲骨文和IBM,价值总计约几十亿美元。(闫磊)



纽约现代艺术博物馆举办“汽车狂潮”展览

8月18日,“汽车狂潮”展览在纽约现代艺术博物馆举办,展览通过10余辆汽车实物、广告海报、生产视频等形式,探讨汽车对人们生活的影响。图为观众在参观一辆1963年生产的捷豹E型敞篷跑车。

廖攀 摄

“深度造假”为战争叠加“智能迷雾”

□ 吴敏文

继美国政府问责局于2020年2月20日发布《深度造假》分析报告后,美国国会研究服务处今年5月发布更新版《“深度造假”与国家安全》报告,新报告将“深度造假”上升到了国家安全的高度。技术决定战术,也是推动战场面貌发生改变的关键因素。“深度造假”这一新的智能对抗技术,又将给军事领域带来什么?

天作之合

“深度造假”可简明解释为“深度学习+造假”。深度学习是人工智能(AI)技术中的一种,是机器学习的新发展。在军事领域,隐真示假历来是迷惑敌人、克敌制胜的一种基本手段。深度学习与隐真示假相结合,就变成了“深度造假”。从某种意义上说,在军事应用上二者堪称天作之合。

“深度造假”的目的是通过造假

误导和迷惑对手,其包括两大对抗性技术措施和手段。一是生成器,负责创建伪造数据(包括照片、录音或视频);二是鉴别器,负责识别伪造的数据。根据每次对抗试验的结果,生成器对造假数据进行调整,以生成更具欺骗性的数据,识别器则通过优化不断提高识别能力。

由于目前“深度造假”技术大多可从公开渠道获取,一般的社会成员即可方便获得,使得“深度造假”呈现迅速蔓延和创造能力活跃提升的趋势,甚至成为某些人展示才华与能力的大众化技术创新活动,造假与打假呈现出对抗循环和螺旋攀升的状态,被用于政治和军事目的在所难免。

军事应用逻辑

可从三大方面对“深度造假”的军事应用逻辑做出解析。

一是在战略和社会层面,“深度造假”可通过制造虚假视频、音频、图像等,实现大规模认知误导乃至

心理战效果。

在信息网络社会,因为传播媒介的多样性和传播效果的快捷普遍性,心理战得到了更大的重视和更广泛的使用。“深度造假”在这方面可谓大有作为。比如,美国华盛顿大学的研究人员通过采集美国前总统奥巴马的视频和音频资料,用“深度造假”技术制造出一个“合成的奥巴马”发表演讲,演讲中奥巴马的扭头、注视和眨眼等身体动作惟妙惟肖,不仅观看者无法辨别真假,就连计算机的智能鉴别软件都没能发现造假。

二是在作战指挥方面,“深度造假”可以让敌方指挥员发布完全违背其意愿的作战命令。

在伊拉克战争中,美军运用EC-130H电子战飞机临空强行接管伊拉克的广播电视系统,向伊拉克民播送“放下武器,接受美军接管”的劝降电视和广播节目。这种方式所使用的主要是在无线电信号、功率上进行压制和夺取的技术手段,不包含任何智能化内容。在“深度

造假”技术加入后,美军完全可以制造出对方国家和军方领导人下令“放下武器、放弃抵抗”的“真实”视频、音频信号,通过强行切断和接管对方国家的电视、广播系统的方式,播送这些造假信息,对方军民几乎无法分辨信息的真假。

三是在具体战役、战斗中,“深度造假”更可以渗透进情报、分析、决策和行动的任何环节,造成不可估计的严重后果。

无论是情报数据造假还是情报分析造假,都具有现实的可能性,而鉴别造假却难以有效实施。由于获取的是假情报、分析结论被人操控,决策正确的可能性微乎其微。

假作真时真亦假

在二战盟军诺曼底登陆作战中,为了让德军相信盟军的登陆点在加莱方向,盟军情报机构不仅采取大量措施隐蔽其在诺曼底方向登陆的作战准备,还在加莱方向设立假指挥部,用角反射器等模拟登陆

作战部队的大规模集结。发展到今天,想要达成这样的欺骗效果,不仅可以采取一些实际行动,还可以更加逼真地制造出战场效果。

比如,用“深度造假”技术制造的“合成指挥官”发表理直气壮的演讲、制定天衣无缝的计划、下达无可置疑的命令;各军兵种“合成部队”展开声势浩大的战前集结和艰苦的战前演练,打造势如破竹的战前演习效果。这些活动还可以与真实的作战地域、环境和阵地融为一体,足以让人坚信不疑。

目前,检测工具还不能自动、完整、高效地检测出“深度造假”。研发检测和鉴别“深度造假”的工具,需要积累大量数据,而且这样的数据只有在与“深度造假”的对抗中才能获得,即检测某种“深度造假”总是在其出现之后。也就是说,“深度造假”具有主动性和先机之利,检测与鉴别“深度造假”则具有被动性和滞后性。

正是“深度造假”,使得“战争迷雾”又迭加上“智能迷雾”。能否穿透“智能迷雾”,最终取决于一方能否在智能技术方面取得优势,以及造假和鉴别技术的此消彼长。