近日，特斯拉汽车的上海超级工厂已正式开始投产，据说这里生产的全新的Model 3汽车将装配高级自动驾驶功能，包括自动泊车、自动辅助变道、召唤即来等更多功能。看来，我们放心大胆地坐上一辆全自动驾驶汽车出门的那一天真的不远了。

但智能汽车真的可以让我们放下戒备之心了吗？事实上，并没有。你或许听说过“汽车黑客”的入侵已导致不少智能汽车出事故——恶意地远程控制车辆，让我们损失的可远不止是个人隐私，它对于个人生命安全甚至整个城市交通安全都会是巨大隐患。我们为自动驾驶时代到来而欢呼雀跃之时，更应该考虑到网络安全——它需要成为自动驾驶的绝对优先事项。

智能汽车的安全更让人担忧（资料图片）

网络安全需要成为自动驾驶的绝对优先事项

要小心“汽车黑客”

□克莉斯汀

被“黑”风险可不止丢失数据

上海超级工厂是特斯拉公司在美国以外的第一个超级工厂，也号称是最先进的超级汽车工厂。这里将大批量地生产智能汽车。据美国一家国际金融服务公司摩根士丹利的专业分析师估计，排除关税后，上海制造的Model 3智能汽车的利润率将高达30%以上。这意味着，智能汽车成本将越来越低，其使用范围自然会越来越广。

但美国一本名为《犯罪与正义》的杂志称，美国密歇根州立大学的研究人员的研究认为，智能汽车很容易受到网络攻击。因为智能汽车与Wi-Fi的连接会更加紧密，这恰好给了黑客更多机会，如果我们通过USB端口将智能手机连接到汽车，黑客还可以通过后门访问包括手机和汽车中所有的数据。如果这种情况发生，汽车便会不在我们的控制之中，甚至也不一定在黑客们的控制之中。这种风险便已远不止是丢失数据这么简单。它会直接关系到我们的生命安全，甚至影响到整个城市交通安全。

2016年的报道称，一位美国公民驾驶着他的2014款切诺基行驶在圣路易斯州的高速公路上时，该座驾的网络系统突然遭到了黑客的攻击——黑客用远程设备控制了该系统，切断了车主与外界的联系，随后汽车失控偏离道路，好在没有造成人员伤亡。

特斯拉公司刚推出智能汽车时，有两名黑客便“黑”入了其中一辆智能汽车，并让这辆车在马路上根据他们的意愿行驶，被发现后，厂家不得不紧急召回了100万多辆同款车型，又经过几个月的时间才将这辆车的漏洞给找出来并补上。

这些早已是公开的“秘密”。谁知道黑客还可以“黑”入多少辆智能汽车，而他们又可能会让这些智能汽车做点什么“高兴”的事呢？

做“汽车黑客”并没想象中那么难

麻烦的是，做“汽车黑客”并没想象中那么难。这不仅仅因为现在智能汽车中的计算机系统和嵌入式软件的脆弱，也因为“黑入一辆智能汽车”的诱惑太大。

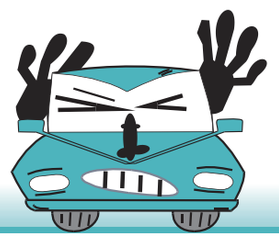
2013年在美国举行的“世界黑客大会”上，就有黑客在现场表演，如何“黑”入智能汽车，通过电脑上的数据让汽车进行了转向、刹车以及点火的操作，让这一辆车完全被自己操控；2014年，360公司也通过网络控制了一辆特斯拉汽车，能够进行让汽车开门、开窗等一系列的控制。当然他们这么做，只是在帮特斯拉公司找到智能汽车系统的漏洞，希望能够尽快地将其修复。

2014年的黑帽亚洲（Black Hat Asia）安全大会上，西班牙安全研究人员贾维尔·瓦兹奎兹－维达尔曾展示过他们打造的一种小型装置，通过这个装置便可以轻松入侵车载系统，并且在几分钟内获取他们需要的所有无线控制权。而这个装置只有一块仅略大于信用卡的电路板，通过四根天线与汽车的控域网连接，就能从车内电力系统获取能源，随时可以接收远程攻击者通过电脑发出的无线指令，影响从车窗、前灯、方向盘到刹车的所有部件。可怕的是，他们宣称，该装置的制作成本甚至不到20美元。

2017年1月清华大学出版社曾出版过一本《汽车黑客大曝光》的书，作者Craig Smith是一家致力于安全审计和软硬件原型构建安全研究的公司经营者。他曾就职于多家汽车商，并为他们提供公开研究。而这本书其实是一本“汽车黑客培训班教材”，课程中涵盖汽车黑客技术的基础内容，它原本也是想帮助汽车商更了解自己的产品，以做出更及时的防范措施。它在出版后第一周，就被下载了超过30万次。更多人因此了解了汽车的通信网络设置，也学会了如何拦截数据并执行特定的黑客手段，以跟踪车辆、解锁车门、进行发动机时钟脉冲干扰攻击及泛洪通信攻击等。说实话，这本书的公开出版还真不知是件好事还是件坏事。

11家公司联盟发布“白皮书”

智能汽车网络安全的问题其实早就引起了业内的足够重视，因为人们在网络安全问题上已有太多教训。大家都明白，随着汽车智能化、自动化程度的发展，网络黑客的威胁也肯定会一路随行。


本版制图/王军

2019年7月，一个由11家公司组成的联盟——Aptiv、奥迪、百度、宝马、大陆、戴姆勒、菲亚特克莱斯勒汽车、Here、英飞凌、英特尔和大众，发布了一份“白皮书”——《自动驾驶的安全第一》，描述了一个开发、测试和验证无人驾驶汽车安全性的框架。汽车行业目前采取的主要措施与当年验证计算机系统类似，通过攻防演练来寻找漏洞，以尽量排除潜在的威胁。

以后大家在选择智能汽车时，车辆所配备的智能车载系统应该会成为权衡的标杆之一。因此自动驾驶智能汽车的开发者们都会努力要求能在黑客之前发现自己所开发的智能车载系统的漏洞所在，并及时修补漏洞。为了提前找到漏洞，他们不惜出一笔不菲的奖金去鼓励那些黑客公开自己的发现。但目前制造商们所采取的种种措施是否能保证汽车的足够安全，仍有待观察。

这种做法当然是理想的，值得尝试的。但黑客的入侵行为仍然令人恐惧。实际上，如今的智能汽车已经成为了一个装有大规模软件的高度集成化的信息系统，除了努力提高技术防范黑客，还有很多方面的发展都是漫长而艰辛的。比如导航系统的精准度、车辆之间的通讯安全，还有交通事故责任权限的明确、人们对自动驾驶的信任度等。

技术的进步其实也总是在刷新我们对世界的认知程度。不管怎么说，网络安全始终是我们最需要关注的问题，在开发自动驾驶技术方面，它也是绝对需要优先的事项。

奇趣生物

你知道昆虫怎么过冬吗？

□黄晓东


棉铃虫幼虫


蝼蚁

很多物种无法在低于0℃的温度下存活，一旦体温降低到冰点以下，细胞中的水就会使细胞受损，甚至导致细胞死亡。形形色色的昆虫究竟是怎样挨过寒冷肃杀的严冬的呢？

越冬的确是生活在温带和寒带的昆虫必须经历的一次危险历程，而昆虫们在此过程中展现出了高超的生存艺术。

虫态篇——昆虫有各式各样的过冬形态

在北风呼啸、滴水成冰的季节里，为了避免寒冷的伤害，昆虫会通过寻找相对较舒适的小环境进行越冬。但是沉睡中的它们却各有形态，也许是只毛虫，可能是粒蛹，抑或是某种幼虫形态。

昆虫越冬的“虫态”千差万别，各有奇妙。从卵到蛹，从幼虫到成虫，不同的昆虫发展出了各自独特的越冬虫态。有些昆虫还能以各种不同的虫态越冬，比如甘蓝夜蛾的蛹会躲在地下5厘米的土壤中过冬；美国白蛾的蛹在树皮下或地面枯枝落叶处越冬；白边地老虎以卵态越冬；天牛、玉米螟的幼虫会在植物的茎秆或者根茬内越冬；蝼蛄的成虫可以钻到地下1米深的地方静待春天的到来。

行为篇——昆虫越冬招数不一

为了应对严寒，昆虫们必须采取行动做点什么来保护自己。

招数一：迁飞

昆虫作长距离、大规模的迁飞是自然界普遍存在的一种现象。迁飞的目的就在于躲避不良的生存环境，开拓新的生存空间。

由于季节的更替，大多数迁飞昆虫为了逃避冬季的低温环境，形成了南迁北回的迁飞规律。亚洲东部地处季风带，其春、夏季的偏南气流和秋季的偏北气流是形成昆虫逐代北迁南回、远距离季节性迁飞的气流条件。

我国地处典型的东亚季风气候区，为害虫跨区域迁飞提供了有利条件。冬末春初，在中南半岛（老挝、越南、柬埔寨）安全越冬的害虫会随盛行西南风通过湘桂走廊向江淮和黄淮农业区迁飞汇集；春末夏初，随着上述地区早稻和小麦的逐步收割，大批害虫又通过渤海湾通道向东北地区迁移。渤海湾已成为我国北方最重要的昆虫迁飞通道。

招数二：滞育

昆虫在不利于其生存的自然环境下，会进入一个滞育阶段。在这个阶段，昆虫的新陈代谢会变缓慢，发育也极其缓慢。

一般认为，光照、温度和食物等条件是影响昆虫进入滞育状态的主要外在因素。例如，导致河南新乡地区棉铃虫滞育的环境条件是短光照和低温，在18℃以下，棉铃虫的滞育率高达96.35%，而在30℃以下则降到了7.98%。

滞育可出现在昆虫发育的某一特定时期，又可以分为卵滞育、幼虫滞育、蛹滞育和成虫滞育。除了冬季滞育以外，夏季也会发生滞育。

生理篇——冷到一定程度时虫儿身体也会结冰

昆虫是变温生物，它们的体温会随着环境温度的降低而下降。在温带和寒带地区，冬季温度通常低于冰点，但昆虫的体液却能在冰点以下保持液态——这被称为过冷却现象。只有当昆虫体温进一步下降到某一个特定的温度时，昆虫的体液才会开始结冰。使昆虫体液保持液态的最低温度被称为昆虫的过冷却点。面对严寒，一些昆虫在进化过程中会尽量降低自身的过冷却点。

自从俄罗斯科学家巴赫梅捷夫首次发现昆虫的过冷却现象以来，世界上有许多学者对此展开了研究。人们普遍认为，过冷却点是描述昆虫耐寒性的主要指标之一。

有时候，昆虫的过冷却能力相当惊人。飞蝗虫卵的过冷却点约为-26℃；幼虫通常为-30℃左右，个别种可达到-60℃以下；鳞翅目昆虫蛹的平均过冷却点（MSCP）很少低于-30℃。

为了降低过冷却点，昆虫们采取了多管齐下的策略。比如昆虫们会降低身体的含水量，水分的排除无疑增加了体内溶质的浓度，从而降低了体液的冰点和过冷却点。例如，桑蟆越冬幼虫的体内含水量会随气温下降而逐渐减少，过冷却能力却随之增强。此外，由于含水量的降低，体内连续较大的整体水相可以被一些组织或某些高浓度的物质分离，从而有利于昆虫体液的过冷却。

（文/图 来源：蝌蚪五线谱）


飞蝗