

蟑螂机器人：“踩不死”的“小强”

■本报见习记者 程唯珈

还记得电影《复仇者联盟》中的“蚁人”吗？这种机器人可以利用它们微小的体积，钻进常人进不去的空隙，检验并进行相关作业。在令人叹为观止的操作背后，各类微型机器人携带着它们专属的“超能力”，蓄势待发。

蟑螂因其顽强的生命力被戏称为“踩不死”的“小强”。近日，一款蟑螂机器人就凭借其“踩不死”的功能受到大众关注。这款由清华大学、美国加州大学伯克利分校和北京航空航天大学科研人员组成的团队联合研发的新型微型柔性机器人，可同时实现机器人的高速运动和耐挤压。

实验中，这款机器人背着有自身6倍重的坚果爬行自如。“如果不出意外，这可能是目前国际上运动速度最快的昆虫类机器人。”谈及成果，论文通讯作者之一、清华—伯克利深圳学院、加州大学伯克利分校教授林立伟向《中国科学报》表示，不过这个蟑螂机器人并非完美，因为它还需要被拴在一根电线上才能移动。“未来我们想在‘蟑螂’身上加一块电池，这样它的移动可以更自由。”

蟑螂君，就是你了！

众所周知，蟑螂能够挤进很窄的缝隙，但它们是如何做到的呢？这一切可能还要从蟑螂的身体结构说起。

早在多年前，论文作者之一、美国加州大学伯克利分校教授 Robert J. Full 就通过高速摄影机观察美国蟑螂。结果发现，这群昆虫在通过很窄的缝隙时，几乎能把自己压扁到平面。

“令人印象深刻的是，这些蟑螂通过 1/4 英寸（6.35 毫米）高度的缝隙时，它们会调整它们的腿，看起来好像完全在身体外侧。它们在自由爬行时约有 1/2 英寸（12.7 毫米）高，不过在缝隙里却能把身体压扁到 1/10 英寸（2.54 毫米）左右，这个高度大约相当于两个叠在一起的硬币。”Robert J. Full 说，研究还发现，蟑螂的连接式外骨骼能保护它的身体，在穿过裂缝时，承受自身重量 900 倍的压力而不受伤。

不过，若论最令人惊叹的技能，恐怕就是当它们把自己身高缩到平时的一半水平时，将会达到短距离上最快的移动速度。

“蟑螂的爬行速度快、身体可变形能力强，可以承受足够大的压力而不受伤。这些能力在灾后搜救、环境监测、侦察监听等隐蔽狭小空间作业场合具有很大优势。”论文通讯作者之一、清华大学深圳国际研究生院副教授张旻告诉《中国科学报》，当发生地震等灾害后，搜救现场一般较为复杂，有许多现有手段不能触及的地方。倘若使用像蟑螂一样灵活的机器人，将会在发现率

首款通过 BCTC 测试的活体相机诞生

■本报见习记者 程唯珈

本报讯 8 月 20 日，记者从中国科学院旗下创企重庆中科云从科技有限公司（以下简称云从科技）获悉，由该公司研发团队自主研发的两款“比邻星”系列红外活体相机以及核心算法，已于近日通过了银行卡检测中心（以下简称 BCTC）的技术检测，并获得 BCTC 颁发的测试通过报告。云从科技“比邻星”系列也成为国内唯一过检 BCTC 的红外双目相机。

BCTC 由中国人民银行总行批准成立，是金融行业内的国家级检测机构。在由 BCTC 颁发的测试通过报告中，检测内容包括活体检测、人脸采集、人脸处理等模块全方位多角度的测试。值得一提的是，在假体识别最为复杂的“三维头模”场景下，“比邻星”系列的假体拒绝率达到了 100%。

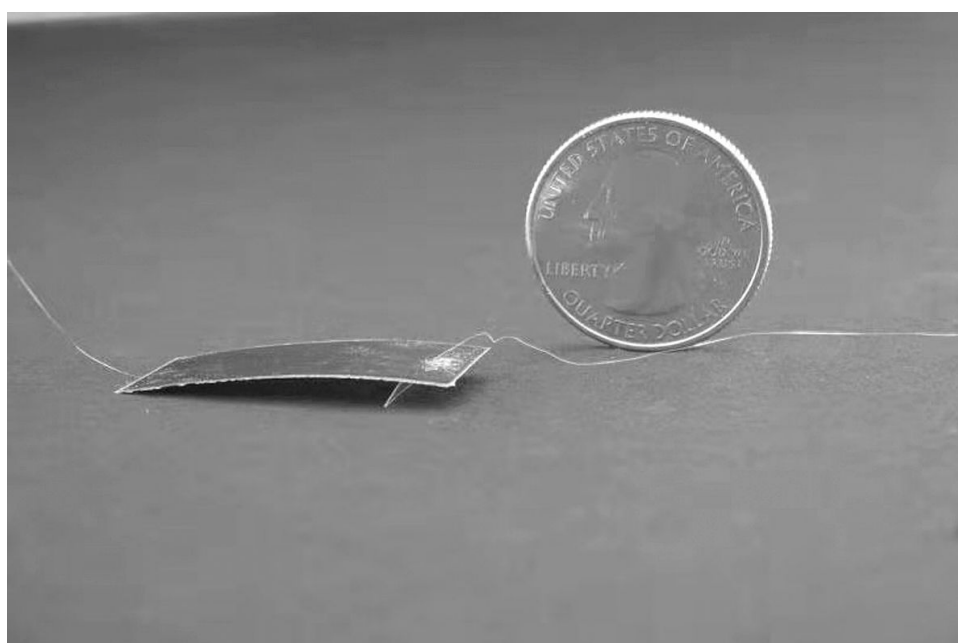
“比邻星”系列的活体检测性能已达到金融支付标准中的最高安全等级——增强级。”云从科技金融产品总经理张兴旺向《中国科学报》介绍，测试结果显示，在不同距离、光线和人脸角度下，比邻星相机不仅能够有效防御二维静态纸质图像、二维静态非纸质图像、二维静态电子图像、二维动态图像，也能有效防御三维面具、三维头模、不完整人脸图像等不同方式的假体攻击。

在“刷脸”时代，如何保障生物识别技术的应用安全，是技术提供方需要解决的一大难题。张兴旺表示，为保障人脸识别技术在支付领域的安全应用，中国人民银行组织 BCTC 与商业银行、银联、支付机构、算法及终端厂商等单位一同编写了行业标准《人脸识别线下支付安全应用技术规范（试行）》，云从科技也是该行业标准的主要起草单位。

数据显示，云从科技已经发展成为我国银行业智能服务第一大供应商——国内有能力自建生物识别平台的银行约为 148 家，已经完成招标的银行约为 128 家。云从科技称，截至 2018 年 12 月 15 日，已中标其中 106 家总行平台，市场占有率约为 82.8%。（赵鲁）



云从科技过检的两款“比邻星”系列相机



新型微型柔性蟑螂机器人

项目组供图

“蟑螂的爬行速度快、身体可变形能力强，可以承受足够大的压力而不受伤。这些能力在灾后搜救、环境监测、侦察监听等隐蔽狭小空间作业场合具有很大优势。”

存者并为救援者确定安全出入口方面发挥重大作用。

柔性 & 高速并存

尽管蟑螂拥有敏捷和健壮等优良品质，但是想要开发出仿生机器人并非易事。

张旻介绍，目前大部分昆虫类机器人都是由刚性部件组成，结构脆弱，容易因挤压破坏而失能。而目前出现的柔性机器人虽然可以承受一定的挤压，但是柔性材料存在驱动力弱和动态响应慢的特点，普遍运动速度较慢，限制了在实际场合中的应用。

如何实现机器人的柔性 & 高速并存？这需要一种柔性压电材料和聚合物骨架相结合的驱动结构。

论文通讯作者之一、美国加州大学伯克利分校博士钟俊文告诉《中国科学报》，这款机器人的基本结构由一个弯曲的“甲壳”和一个“前腿”构成，均采用柔性材料，可实现弯曲变形。

在电子显微镜下，这款蟑螂机器人的结构一目了然：一个薄薄的截面间有数层材料，其中热塑层夹在钽电极之间，用黏合剂硅橡胶黏合在底部的塑料件上。

那么，如此单薄的“身子”又是怎么跑起来的呢？原来，秘密在于它的压电材料——聚偏氟乙烯（PVDF），其两端加上电压后就会收缩或膨胀。

钟俊文介绍，当给 PVDF 加上交流电后，该机器人就会反复在弯曲和伸直的状态之间变化，这样“甲壳”的形状也就随之变化，通过“前腿”撞击地面，进行弹跳运动，甚至能爬上斜坡，完成一系列运动。

林立伟回忆道，在研究的初始阶段，最大的瓶颈在于机器人运动速度太慢。“最初，它每分钟只能移动 1 厘米。”而后，该团队又输入不同频率的交流电进行数次实验，最终发现用接近共振频率驱动蟑螂机器人可以大大提升其速度。

团队最终设计的机器人昆虫体长

1~3cm、重量 20~60mg。最高运动速度可达 20cm/s，在现有报道的微型运动机器人中速度最快。同时，由于采用全柔性折叠结构，在承受 100g 重物（约为体重的 1600 倍）挤压后，运动能力不变；在承受一个成人（约 60 公斤）踩踏后（约为机器人重量的 100 万倍），仍然具备 50% 的运动能力。

“人们可能已经历过，如果你踩到蟑螂，你可能需要把它磨碎一点，否则蟑螂可能仍然存活下来并逃走。同样的，如果有人踩了我们的机器人，它仍然可以工作。”林立伟说。

“我们都是超能力者”

“小强”并不孤单，像它这样具有特异功能的微型机器人并不在少数。它们或能“上天入海”，或能“飞檐走壁”，分散在世界的各个角落。

例如不久前，哈佛大学 Robert J. Wood 团队研制了仿昆虫无缆飞行机器人 RoboBee X-Wing。这种小型机器人重量仅为 259 毫克，采用太阳能电池供电，可以实现短时间的无缆飞行。

瑞士和英国研究人员则研发了一款可在有黏性或快速流动的液体中“游泳”的柔性微型机器人，未来有望将药物送达体内的病灶组织，且不会引起身体的排斥反应。

在我国，上海交通大学教授宋向阳与麻省理工学院教授赵进贺等研制了由介电弹性体人工肌肉和静电吸附脚掌构成的软体爬壁机器人。其中，介电弹性体人工肌肉用于驱动机器人本体的快速周期运动，静电吸附脚掌用于产生时间和空间可控的静电吸附力。该软体机器人拥有垂直爬壁、水平爬行、原地转弯等运动能力。

不过，在钟俊文看来，微型机器人想要真正进入人类生活，还有以下技术难点需要攻关。

“比如电源问题，大部分机器人需要外接电源才能工作。而且机器人的移动速度也有待提高。还有负载问题，目前小型机器人的载重一般比较小。”他说。

张旻表示，刚柔结合、多功能化、集群化、与 AI 结合是微型机器人的发展趋势。未来团队将继续优化蟑螂机器人的结构设计，增加弹跳、爬壁等功能，并且尝试集成柔性传感器和执行器，制造具有自主能力的多功能机器人昆虫，实现侦察、循迹、测量、监控与分析等功能。

这一想法已得到了初步证实。“目前，我们已经初步做到将一个气体传感器与该机器人整合，并用其探测了有害气体。未来有望进入人类或搜救犬难以进去的各个角落侦察或搜索，挽救民众生命。”张旻说。

相关论文信息：

<https://doi.org/10.1126/scirobotics.aax1594>

深信服董事长兼 CEO 何朝曦：

未来安全保护的“变”与“不变”

■本报记者 赵广立

“网络安全有三大驱动力：合规、事件、业务保障。合规是安全底线，事件驱动的是投资方向，保障业务稳定是根本需要。不过，过去几年这三大驱动力都发生了变化，这也导致业界的安全理念发生了变化。”8 月 16 日，在以“畅想”为主题的 2019 深信服创新大会上，深信服科技董事长兼 CEO 何朝曦畅想未来的安全：未来的安全将是动态的、多维的、多场景的、全局并重视体验的。

安全保护之“变”

“过去的安全非黑即白、二元分明，主要用静态规则隔离‘好和坏’‘内与外’。但随着攻击手段的多样化，‘好的’也会被利用变成‘坏的’，以往的静态规则没办法适应这种快速变化，需要动态的安全防护来持续地检测和响应，改变攻防不对称的状态。”何朝曦表示，当前动态的安全防护已成为主流。

随着云端、移动互联应用等丰富的数字化产品涌现，网络安全的场景不再单一。对此，何朝曦说：“安全产品和方案要匹配更多场景，过去通用的合规标准，要变成分场景定义保护措施。”

同样的，安全防护也正面临着从局部向全局的演进。“以前 PC 上的杀毒软件、网络设备的防火墙彼此不相关，但随着 APP 攻击、勒索病毒的泛滥，网络攻击的扩散能力越来越强，这要求安全保护要有全局能力，实现多层级的立体防护。”

此外，过去“为了安全可以牺牲便利性”，并不注重用户体验，这导致安全产品很“难用”。在数字化时代，终端用户对体验要求越来越高，甚至会因体验差而抵制安全。

“现在的安全体验做得越来越友好了，不仅界面越来越漂亮，操作也越来越简单。”何朝曦说，未来的安全体验还会更方便。



何朝曦

用户需求发生变化，安全产品的交付也随之而变。“现在安全产品已经从几十年前的‘老三样’，变成了数十种。另外，安全交付的形态也更加丰富。”何朝曦援引信息调研机构 IDC 在 2018 年发布的《全球网络安全分析报告》说，过去安全产品主要是软硬件设施，如今除了软硬件，还有安全服务、安全 SaaS 平台的交付，共有 51 个品类的安全产品，“未来只会变得更加丰富”。

从“不变”看安全之未来

亚马逊创始人杰夫·贝佐斯曾有一句名言：洞察在接下来的十年里面什么是不变的，比洞察什么会发生改变更重要。何朝曦也深谙此道，“安全产业虽然发生很多变化，但也有不变：用户对安全的诉求不变、对性价比的追求不变、对业务开展的便捷性需求不变”。

了解用户不变的诉求，再结合时下发生的变化，何朝曦畅想的未来安全将具备这样的特点：自我更新与演进、高度集成、融入业务、进一步自动化。

“未来的安全防护应该能够自我更新与演进，不管是通过云服务、软件定

义、机器学习或是其他什么方法。”何朝曦举例说，就像 AlphaGo、AlphaZero 一样，通过安全博弈平台让攻防两端不断对抗，经过长期训练锻造可应对各类安全风险防御手段，达到持续更新演进的效果。

另外，何朝曦提出，未来安全还要做到高度集成。“攻击越来越多，需要保护的客体越来越多，安全技术和产品也会越来越多。但用户要求尽量简单，这就要求未来的安全能力应在相同的场景下高度集成，最好每个场景只有一套安全平台”。

“用户对真正有效的集成接受度很高。”何朝曦说，这在网关场景下已经验证。“所以未来的安全平台要有机地集成多种安全保护能力，通过简单的界面操作，实现全局安全的可视可控，并且可编排、按需部署。”

此外，何朝曦认为，未来的安全能力还要融入业务，嵌入到业务开发之中，成为业务的一部分。“这样才能有更好的安全效果 and 用户体验。”他举例道，通过在业务中加入安全 SDK，可得到更丰富的行为检测效果等，以实现更好的保护。

而随着人工智能技术的演进，何朝曦预言未来的安全“一定会进一步自动化”。“人工智能等技术可帮助实现快速响应和动态防御，再加上更高级的人工服务，将成为安全服务交付的主流方式。”

“为减少用户在安全上的无效投资，未来还会出现按能力计费的安全，用安全效果来定价的模式也会成为可能。”何朝曦说。

让畅想成为现实，靠的是不断的创新。何朝曦表示，目前深信服每年投入超过 20% 到研发当中，努力从战略、抓手、组织流程等方面建立创新支撑机制，力求“推动组织由内而外的系统创新”，拥抱畅想中的安全未来。

开放零售倡议落地中国

■本报见习记者 程唯珈

本报讯 8 月 20 日，在北京举行的英特尔开放零售倡议合作伙伴峰会上，英特尔物联网事业部零售、银行、酒店餐饮及教育行业首席创新官 Stacey Shulman 宣布，开放零售倡议（ORI）正式落地中国，京东及 VMware 已作为早期合作伙伴加入该倡议。

近年来，随着物联网技术的发展，零售行业正在迎来新一轮变革。如何跨越因缺少行业标准而造成的阻碍，如何在“堆砌式”建设的应用系统上作进一步的创新，成为该行业亟待解决的难题。为应对这一挑战，零售行业迫切需要一个共同的开放框架，以更加便捷地部署智能零售的生态系统。

Shulman 告诉记者，这正是英特尔推出开放零售倡议的初衷。该倡议致力于凝聚行业力量，共同搭建并创新零售门店整合平台，打通智能门店不同设备的数据，将零售应用的不同场景整合，并具有向使用者提供数据分析和远程运营的能力。

据介绍，在倡议愿景中，EdgeX Foundry 将是零售整合平台的核心模块。借助这一物联网边缘解决方案的开源服务框架，倡议的参与者可以更轻松地加入到这一计划中，并能在零售场景下更好地实现工作负载整合。

以 POS 机为例。当前，不少智能门店都安装了可供消费者自助结账的 POS 机。然而，自助 POS 机在为消费者提供便利的同时也为商家带来了隐患。开放零售倡议和 EdgeX 的介入使得基于数据融合的防损 POS 成为了可能。防损 POS 可以根据门店需要，借助摄像头、重力传感器或 RFID 传感器等为购物车验证算法提供数据来源，进而对顾客购物车商品实现无延迟的交叉认证，在保证用户体验的同时有效规避商家风险。

京东零售技术运营平台部负责人罗焱告诉《中国科学报》，在英特尔开放零售倡议的支持下，京东已推出了面向线下门店的统一的零售物联网中台——京东星链零售物联网平台。该平台的开发使用了英特尔的边缘计算技术和 EdgeX，旨在将线下零售终端及应用相连接，进而实现业务的全链路数字化。

VMware 中国研发中心总经理任道远向记者介绍，VMware 于今年 1 月加入了开放零售倡议。在此期间，英特尔与 VMware 在共同推动开放零售倡议、加速行业协作等方面开展了密切合作。今年 5 月，VMware 物联网部门推出了基于 VMware Pulse 的商业版 EdgeX 支持计划。该计划能够对全物联网组件谱系，包括开源软件提供端到端的软件支持。（计红梅）

速递

粤港澳大湾区人工智能与机器人联合会成立

■本报见习记者 程唯珈

本报讯 为推动粤港澳大湾区内人工智能与机器人技术的高效发展，增强三地产学研的交流和合作协同生态建设，近日，在澳门举行的国际人工智能联合会之 AI in China 论坛上，粤港澳大湾区人工智能与机器人联合会（以下简称联合会）宣告成立。

联合会由中国工程院院士、广东省人工智能与机器人学会理事长高文倡议发起，由广东省人工智能与机器人学会、香港人工智能与机器人学会、澳门大湾区人工智能学会组成。三个学会各自汇聚本地人工智能与机器人领域的高水平学者。此次联合将进一步发挥人才的凝聚作用，增强科技创新的化学效应，推动科研交流和产业发展，促进中国在关键核心技术上的研发与应用。

高文表示，中国的人工智能发展具备政策、数据、场景、人才等优势，但也有理论原创、高端器件、领军人才、开源开放等短板，取长补短是联合会的重要使命。（田瑞颖）

第七届互联网安全大会在京召开

■本报见习记者 程唯珈

本报讯 “网络空间是维护国家安全的战略要塞，要依靠全社会的力量共同发展网络安全事业。”8 月 19 日，在北京怀柔雁栖会展中心举行的第七届互联网安全大会（ISC2019）上，中国科协名誉主席、中国科学院院士韩启德在致辞中表示，网络安全技术已成为万物互联时代的核心技术，只有把握这一核心技术，才能把握自己的命运、提升我国在网络空间的话语权、真正建成网络强国。

然而，随着 5G 商用、万物互联时代的到来，新形势下的安全问题日益严峻。“5G 对安全来说是把双刃剑。”本届大会的名誉主席、中国科学院院士贺卫华随后在致辞中提到，基于 5G 网络实现的智能化监控有利于提高网络安全防御水平，但 5G 协议的互联网化等因素也会引入新的安全风险。因此，在为 5G 带来的想象空间欢欣鼓舞的同时，必须正视其带来的安全挑战。贺卫华还特别提及，针对工业互联网的网络攻击“会造成比过去更严重的影响”。

“网络安全对人类经济与社会的影响很大。不管大国还是小国，必须在网络安全方面携手交流，共同应对网络对人类命运共同体的威胁。”大会主席、360 公司董事长兼 CEO 周鸿祎表示。（赵鲁）

中科视拓再度开源人脸识别算法

■本报见习记者 程唯珈

本报讯 8 月 19 日，孵化自中国科学院计算技术研究所（以下简称中科院计算所）的人工智能创业企业中科视拓通过 GitHub 开源了其开发的商用级人脸识别算法“SeetaFace2”。据介绍，这是在 2016 年 9 月开源 SeetaFace1.0 人脸识别引擎之后，中科视拓在人脸识别领域的又一次“自我革命”。

中科视拓人脸组研发总监李凯周介绍说，SeetaFace2 包含了完整的人脸检测、面部关键点定位和人脸特征提取以及对模块，之后还将陆续开源人脸跟踪、闭眼检测等辅助模块。目前，SeetaFace2 所有算法均提供全部源代码、注释、接口文档以及样例程序，可帮助开发者快速基于 SeetaFace2 开发应用。

记者了解到，SeetaFace2 堪称面向于人脸识别商业落地的“里程碑”。它的人脸检测模块在人脸检测算法评价标准（一款专门针对人脸识别算法的评测方法与标准）上的 100 个误检条件下可达到超过 92% 的召回率，面部关键点定位支持 5 点和 81 点定位，1:1 N 模块支持数千人规模数据库的人脸识别应用。

李凯周表示，与 2016 年开源的 SeetaFace1.0 相比，SeetaFace2 在速度和精度两个层面上均有数量级的提升。（赵广立）