微软实现深层神经网络重大技术突破

□ 本报记者 刘 燕

日前，微软亚洲研究院视觉计算组在2015 ImageNet计算机识别挑战赛中凭借深层神经网络技术的最新突破，以绝对优势获得图像分类、图像定位以及图像检测全部三个主要项目的冠军。同一时刻，他们在另一项图像识别挑战赛MS COCO（Microsoft Common Objects in Context challenges，常见物体图像识别）中同样登顶，在图像检测和图像分割项目上击败了来自学界、企业和研究机构的众多参赛者。

据了解，在此次挑战赛中，微软亚洲研究院的研究团队使用了一种前所未有的深度高达百层的神经网络，这比以往任何成功使用的神经网络层数多5倍以上，从而在照片和视频物体识别等技术方面实现了重大突破。

事实上，该研究团队早在今年一月就首先实现了对人类视觉能力的突破。当时，在题为“Delving Deep into Rectifiers: Surpassing Human-Level Performance on ImageNet Classification”的论文中，他们系统的错误率已降低至4.94%，今年微软亚洲研究院视觉计算组的系统错误率已经低至3.57%。此前同样的实验中，人眼辨识的错误率大概为5.1%。

微软全球资深副总裁、微软亚太研发集团主席兼微软亚洲研究院院长洪小文表示：“微软亚洲研究院视觉计算组在此次ImageNet挑战赛中所取得的出色成绩，不仅是微软在深层神经网络的研究和应用上所取得的科学突破，同时也代表着计算机视觉技术在目标识别方面的又一次飞跃。我对这一突破对其他研究领域的推动以及相关产品的转化充满期待。”

微软亚洲研究院视觉计算组首席研究员孙剑博士带领的团队在深层神经网络方面进行了算法的更新，并称之为“深层残差网络”（deep residual networks）。目前普遍使用的神经网络层级能够达到20到30层，在此次挑战赛中该团队应用的神经网络系统实现了152层。该研究团队还使用了一个全新的“残差学习”原则来指导神经网络结构的设计。“残差学习”最重要的突破在于重构了学习的过程，并重新定向了深层神经网络中的信息流。它很好地解决了此前深层神经网络层级与准确度之间的矛盾。孙剑表示：“从我们极深的深层神经网络中可以看出，‘深层残差网络’力量强大且极为通用，可以预见它还能极大地改善其他计算机视觉问题。”

微软亚洲研究院多年来在计算机视觉领域的研究成果已经转化到众多微软的智能产品和服务中，包括微软牛津计划中的人脸识别和图像识别API、Windows 10中的Windows Hello“刷脸”开机功能、必应的图像搜索、微软小冰的多个图像“技能”，OneDrive中的图片分类功能，以及广受好评的口袋扫描仪Office Lens等等。

ImageNet是一个计算机视觉系统识别项目，也是目前世界上图像识别最大的数据库。ImageNet挑战赛每年举办一次，由来自全球顶尖高校、企业及研究机构的研究员组织举办，近年来已经成为计算机视觉领域的标杆。MS COCO数据库由微软资助建立，其挑战赛目前由学术界几所高校联合组织，独立运行。

首届北京市中小学生创客秀活动开幕

12月12日，首届北京市中小学生创客秀活动在北京市第八十中学体育馆开幕。

青少年创新活动培训中心的执行董事来源先生展示了由3D打印机和激光切割机制作的新能源赛车模型。来自八一中学的学生创客王丰冀，刘哲同学展示介绍了由他们设计制作的3D打印机、激光雕刻、数控雕刻一体机。来自清华创客空间的导师齐默·巴恩斯（美国纽约主动精神的设计师）作了如何帮助学生享受创意的演讲，刘竹生院士寄语青少年要不断探索，不断创新，真正成为推动社会发展和技术进步的小创客。

作为本次活动的合作伙伴，Autodesk集团不太尔时代科技有限公司对本次活动在软件（Inventor 3D建模）硬件（UP 3D打印机）上给予了支持。在为期两天的活动中，来自全市100多所中小学校参赛者围绕节能环保、科技创新、手工制造等主题，在“创客秀场”、“8小时互动设计马拉松”两个竞赛项目展开了激烈的角逐。“F1在学校科技挑战赛”作为展演项目也在大赛中进行了精彩演示。

（安吉）

华硕A751LX诠释高性价比

华硕日前推出A751LX高性价比笔记本，专为提高生产力和娱乐而设计，能够为用户打造高清多媒体效果和多任务处理操作。五代i5-5200U处理器，GTX950M独显，17.3英寸超大全高清1080P屏幕，华硕A751LX用极佳的处理性能与极具吸引力的多媒体娱乐体验，诠释“高性价比”。

华硕A751LX，配备17.3英寸超大全高清1080P屏幕，逼真画质缤纷呈现。华硕A751LX搭载GTX950M独显，具有视频展现力与图形表现力。加上华硕Splendid靓彩技术，可满足极其严苛的观看标准。该技术可以根据应用程序优化显示属性，还可以调整色域和对比度。

华硕A751LX拥有1T存储的海量硬盘，照片、电影、工作资料，通通装进来。既然存储着海量的信息，就免不了要时常进行拷贝与传输的工作。华硕A751LX配备USB 3.0接口，10倍于USB 2.0的理论传输速度。帮助客户在单位时间内传输更多的文件，更快速的复制和备份所有的文件和内容，从此告别冗长的等待时间。 （向阳）

中国闪存联盟助力行业转型升级

日前，中国闪存联盟第四季暨周年庆典活动在京召开。一年来，该联盟在助力中国行业转型升级方面效果渐显。

中国闪存联盟秘书长晓黎表示，一年来闪存联盟共举办了12场行业深化活动，联盟会员超过150家，覆盖金融、制造、电信、零售、政府等十大行业；187家合作伙伴、企业用户参与走进总代活动。

去年12月，IBM携手产业伙伴共同成立中国闪存联盟，通过协调产业各方的合作，促进生态系统的发展，推动闪存技术在中国市场的应用普及。“软件定义存储和闪存技术将解决目前存储领域面临的两个重要挑战：可管理性和性能制约。这是目前存储市场发展最重要的两个趋势。”IBM大中华区硬件部存储系统部总经理黄永志说。 （陈杰）

锐捷网络推出RG-AP630室外专用AP

近日，锐捷网络推出了一款WLAN场景化产品——室外增强型802.11ac无线接入点RG-AP630。该产品采用802.11ac协议标准，可以提供高达1.75Gbps的接入速率，以及最大接入256个用户的超强性能，同时采用IP67防护等级、金属外壳及整体散热设计，能够在极端恶劣的室外环境中满足室外Wi-Fi覆盖需求。

作为一名全天候的“室外工作者”，AP630需要完美胜任在各种室外恶劣自然条件下的工作。为此，该产品采用了IP67防护等级的外壳设计，在极端的室外环境中可有效避免室外恶劣天气和环境影响，能轻松胜任-40℃～+65℃的工作环境，适应中国北方的寒冷天气、南方的潮湿天气。除了工业级的品质保障之外，锐捷的研发人员还采用内置高规格防雷器，用户无需外接防雷设备，高度简化了部署成本。

在性能方面，RG-AP630支持最新11AC协议，支持2.4GHz、5GHz双频应用，通过采用先进的多天线3×3 MIMO技术，整机性能达到1.75Gbps，在全面支持高清视频传递的同时，保证了其他网络业务的有效传递。另外，RG-AP630还继承了锐捷网络一贯领先的智能本地化转发技术，彻底突破了无线控制器产品的流量瓶颈的限制。通过锐捷网络RG-WS系列无线控制器产品的配合，RG-AP630智能地将延迟敏感、传输要求实时性高的数据分类通过有线网络转发，更好地适应了802.11ac网络高流量传输的要求。 （陈杰）

3D打印技术展望及未来发展趋势

3D打印技术目前已经步入了飞速发展的时代，3D打印被赋予了“第三次工业革命”的大背景，以3D打印技术为代表的快速成型技术被看作是引发新一轮工业革命的关键要素。目前，在3D打印技术领域，虽然国内与国外存在较大的差距，但是，国内在某些方面已经领先全球，并且从“国家领导人”到“普通民众”对3D打印技术给予了高度的关注和极大的热情，这为提升“中国制造”整体实力提供了一个绝佳的机会，为3D打印的普及应用与深化发展提供了一个良好的平台。

3D打印技术未来趋势之一——设备向大型化发展

纵观航空航天、汽车制造以及核电制造等工业领域，对钛合金、高强钢、高温合金以及铝合金等大尺寸复杂精密构件的制造提出了更高的要求。目前现有的金属3D打印设备成形空间难以满足大尺寸复杂精密工业产品的制造需求，在某种程度上制约了3D打印技术的应用范围。因此，开发大幅面金属3D打印设备将成为一个发展方向。

3D打印技术未来趋势之二——材料向多元化发展

3D打印材料单一性在某种程度上也是制约了3D打印技术的发展。以金属3D打印为例，能够实现打印的材料仅为不锈钢、高温合金、钛合金、模具钢以及铝合金等几种最为常规的材料。3D打印仍然需要不断地开发新材料，使得3D打印材料向多元化发展，并能够建立相应的材料供应体系，这必将极大地拓宽3D打印技术应用场合。

3D打印技术未来发展趋势之三——从地面到太空

NASA是美国政府机构中较早研究使用3D打印技术，已利用3D打印技术生产了用于执行载人火星任务的太空探索飞行器（SEV）的零部件，并且探讨在该飞行器上搭载小型3D打印设备，实现“太空制造”。“太空制造”是NASA在3D打印技术方向的重点投资领域。为实现“太空制造”，美国已在太空环境的3D打印设备、工艺及材料等领域开展了多个研究项目，并取得多项重要成果。

3D打印技术未来发展趋势之四——助力深空探测

3D打印技术的快速发展和远程控制技术为空间探测提供了新的思路。月面设施构件3D打印技术是利用月球原位资源，采用3D打印技术就地生产月面设施构件，是未来建立大型永久性月球基地的有效途径。该方法能够最大限度地利用原位资源制造3D打印所需的粉末材料，继而采用3D打印设备直接打印出月面设施构件，大大降低地球发射成本，并可利用月球基地的原位资源探索更远的空间目标。

3D打印技术未来发展趋势之五——走入千家万户

随着3D打印技术的不断发展与成本的降低，3D打印技术走入千家万户不无可能。也许，未来的某一天，你便可以在家里给自己打印一双鞋子；也许，未来某一天，在你的车子里就放着一台3D打印机，汽车的某个零件坏了，便可以及时打印一个重新装上，让你的车子继续飞奔起来，而不是站在路边苦苦地等着别人来把你的车子给拖走……

3D打印正因为它的独特魅力逐渐融入我们的生活；3D打印正因为它的独特优势逐渐改变这个世界；3D打印正因为它的无所不能可以让你的“异想天开”变得“实实在在”；3D打印正因为它的快速高效可以让你的“驾车旅游”不再孤单；3D打印正因为它的巨大魔力让建立“月球家园”不再是一个梦想，这就是“3D打印”。

（上海3D打印产业联盟理事长 王联凤）

主动防御系统在网络信息安全中的应用

网络信息系统中的计算机终端能否保持安全运行至关重要，它既是网络攻击的目标，也是网络攻击的源头。

作为网络系统中最薄弱环节，同时也是出现问题最多的环节，计算机终端安全面临着巨大的挑战：操作系统以及应用系统漏洞层出不穷；现有的防病毒软件都是以黑名单的机理处理病毒，出现新病毒无法及时解决；混合型威胁越来越多，针对计算机的威胁越来越不可预见；企业中对客户端的管理越来越难。

笔者作为计算机工程师在报社网络信息化岗位上工作近30年，面临最多也最难处理的工作便是处理计算机安全问题，花费在解决计算机客户端问题的时间占到了整体工作的时间比例超过60%。

如何安全高效地管理众多计算机客户端，使IT管理者能腾出更多时间去研究和思考更重要的技术问题，同时保障报社整体网络环境安全高效运转，是工程师面临的重要课题。经过长期考察实践，笔者发现，问题主要集中在如下几点：

被动防御方式：目前终端主要基于扫漏洞、打补丁和利用特征库识别恶意行为等被动防御机制，不能满足高等级的安全需要，特别是针对渗透攻击缺乏有效的防御手段。

安全机制脆弱：现有安全防护产品“重功能，轻保障”，安全保障能力欠缺，自身安全机制容易被篡改和旁路。

管理分散低效：当前安全建设采用分散管理的方式，一方面各产品难以联动，不能构成整体防御，另一方面运维效率较低且缺乏预测能力。

如何解决这些问题？

金融时报社采取了计算机主动防御系统来应对，主要可以实现如下效果：定制计算机终端能够运行的应用程序并生成白名单，通过安全管理平台能够根据安全要求制定策略，并对终端操作行为实施控制，使得终端能够防范计算机启动过程中操作系统相关部件的篡改和破坏，保证终端动态服务的真实可信，能够防范RootKit式攻击，能够根据策略对应用类型加以限制，对木马、病毒等恶意代码具备主动防御能力，对流氓软件的非法安装和运行具备控制能力。也就是说，哪些程序可以在计算机上运行是可以由网管人员定义的，白名单以外的任何程序都无法启动，从而，确保终端系统环境对病毒、木马、漏洞的攻击免疫，实现“进不来”、“拿不走”、“改不了”、“瘫不了”、“赖不掉”的安全效果。采用白名单主动防御机制，提供执行程序可信度量，阻止非授权及不符合预期的执行程序运行，实现对已知/未知恶意代码的主动防御，可以做到免补丁升级，免病毒、木马查杀。

该技术如同在网络信息系统中有效筑起了一道安全防火墙屏障，为安全出报起到了积极作用，对于有效的企业IT安全管理起到了重要的规范作用。通过5年多的长期应用与改进，金融时报社的计算机、网络运行稳定，未出现重大病毒爆发。

（张占成）

家电业迎来行业标准换代期

继9月份颁布空气净化器新国标以来，国家标准委又在不久前发布了全新修订的《家用电冰箱耗电量限定值及能效等级》强制性能效国家标准，新能效等级标准将于明年10月1日起实施，随后，又宣布启动洗衣机性能国家标准的修订工作。业内人士表示，家电业正迎来行业标准换代期，而国标迭代将成为家电产业升级的关键推动力。

一组数字则表明，家电业寒冬的根本原因是结构性失衡，而非消费动力不足。今年上半年，在冰箱市场上，单门零售额同比下降26.6%，两门零售额同比下降22.2%，三门零售额同比下降12.4%，但代表高端产品的品式多门（也称为十字多门）零售额实现了247.8%的同比增长。

而在洗衣机市场，滚筒洗衣机零售额比重由2012年46.6%上升到2015年58.8%，变频洗衣机零售额比重由24.6%上升到53.6%。大容量洗衣机也受到了市场欢迎，7KG以上波轮洗衣机零售额占比71.8%，7.5KG以上滚筒洗衣机零售额占比为83.7%，都实现了10个百分点以上的同比增加。

未来，随着经济的发展和消费需求的升级，高附加值、高品质产品将成为市场热点，如三星一般具备先进技术的企业将占据有利地位。

生活水平的提升使得消费者存储的食物种类越来越多样，不同品类的食材对冰箱的制冷和控温提出了更高的要求。三星品道家宴系列，采用品式多门结构，集“精准控温”与“创新制冷”于一体，无论是“3-2-1”制冷方案，还是精控保鲜技术，都大幅提升了冰箱的制冷效率和保鲜能力，最大程度保证了食物存储品质，更好地适应了消费者日益提升的食物存储需求，因此受到了市场的青睐。

而在洗衣机市场，洗净度仍是消费者关注的核心要素。三星水晶系列洗衣机的”泡泡净“技术，可以充分激活洗涤剂的活性，深入渗透衣物，大幅提升洗涤效率，缩短洗涤时间，且通过冷水洗涤即可实现热水洗涤的洗净效果，进一步提升了节能性能。这种高附加值的产品，因能够满足消费者额外升级需求而获得更多关注。 （何乐 马爱平）

智能电视或面临感染勒索软件

赛门铁克研究人员近期针对新型智能电视进行实验研究，以了解其抵御网络攻击的能力。实验结果显示，被感染勒索软件的全新智能电视均遭受无法使用的后果。

智能电视如何受到攻击？

将恶意软件安装于电视中是最常见的攻击形式。除了通过电视USB端口手动安装恶意软件或从官方市场意外下载感染应用以外，攻击者还可能采用以下几种方法：

MitM攻击 攻击者通过实施中间人（MitM）攻击将恶意软件安装于电视中。他们需要在相同网络路径上实施该攻击，但这也可以通过获取Wi-Fi密码或截获DNS请求等方式达到攻击目的。并非所有电视连接都采用SSL加密，即使部分电视采用SSL加密，也无法彻底验证证书。例如，攻击者能够轻松创建自签名证书以应对部分接受自签名SSL证书的电视。避免电视不安全通信的另一种方式是利用实体可信根设备证书（Solid Roots of Trust），现在有线电视行业已经采用这种方法来实现内容保护。

当用户下载应用时，攻击者会拦截下载请求，并将其重新定向至其他服务器。此时，电视将不能从合法服务器下载真正的应用，而会被重新定向至其他服务器使电视下载恶意应用。当下载完成，用户需要接受恶意软件应用的运行请求。由于用户并不知道所下载为恶意应用，因此他们很可能会接受并安装该应用。

利用漏洞 攻击者还能够利用软件漏洞攻击电视。由于智能电视拥有浏览网页的功能，攻击者可以引导用户访问恶意网站，该恶意网站能够检测电视中存在漏洞的软件，并利用漏洞，实现有效载荷。由于智能电视本身会具有多种不同媒体格式及文件格式漏洞，例如近期的libpng漏洞，它们是攻击者理想的利用目标。

系统更新或未进行更新 现在，许多智能电视都能够在设备空闲时提供自动检查、更新并下载的功能。即使电视操作系统开发人员定期发布软件更新，用户仍旧需要依靠电视制造商为设备发布更新，这意味着，在等待发布更新的期间，用户的电视会非常容易受到攻击。

此外，一些智能电视会从非SSL网站下载固件更新，MitM攻击者可以拦截并丢弃这一网络流量。这意味着，攻击者能够阻止电视更新，使其容易受到现有漏洞的攻击。从另一个角度说，修改更新程序包本身非常困难，因为在安装之前需要进行加密和验证。但我们也看到，一些设备的更新并不能起到保护作用。

电视远程应用 由于能够被安装于移动设备，电视远程应用程序将会受到用户的欢迎。这种应用由质询响应PIN码（Challenge-Response PIN）授权。处在相同网络中的攻击者可以探测到已认证的远程控制设备，重新播放命令，从而进行更改电视频道、调整音量或关闭电视等攻击举动。任何网络可访问的服务都存在风险，目前已发生多起拒绝服务（DoS）攻击以及利用智能设备上的UPnP漏洞所进行的远程执行代码事件。一般而言，攻击者需要访问本地网络或在相同的网络中的电脑上运行恶意软件，以便实施此类攻击。

为何攻击智能电视？

攻击者可能会出于各种各样的原因攻击智能电视，例如：**点击欺诈** 攻击智能电视获利的方式之一是在电视上安装广告软件或恶意软件以实施点击欺诈。由于电视长期保持打开状态，攻击者能够在未经用户同意的情况下在幕后持续进行广告点击，从而获益。

僵尸网络 攻击者能够在智能电视中添加僵尸网络，利用其实施分布式拒绝服务（DdoS）攻击。对于这种攻击，路由器是更好的攻击目标。使用默认密码的路由器更容易遭受攻击。

数据盗窃 盗取线上流媒体服务或应用商店（例如Google Play）的账户凭证也是攻击者攻击智能电视的原因之一。虽然用于Android电视中的Android版本很难使应用程序盗窃此类账户数据，但攻击者却能够通过其他智能电视操作系统实施盗窃。

加密货币挖掘 新型智能电视装有高性能显卡芯片，攻击者以其作为攻击目标来挖掘加密货币（例如比特币）。但相对于专用ASIC芯片，受到攻击的智能电视并不能为网络罪犯创造大量利益，仅有部分大型电视网络能被攻击者所利用。

勒索 利用勒索软件感染智能电视是攻击者获取利益的方式之一。电视勒索会造成电视用户大量金钱损失。与电脑和智能手机勒索事件相同，无法访问设备所产生的威胁以及攻击者所掌握的数据都足以让受害者心甘情愿地交付赎金。此外，这种攻击实施起来十分容易。

访问其他联网设备 攻击智能电视可以作为罪犯访问家庭网络环境或商务环境中其他设备的中继站。

隐私 智能电视能够收集大量隐私信息，例如录音及视频数据等。在智能电视上传至后台之前或期间，网络罪犯会试图盗取用户数据，以便利用此类数据调整后续攻击或对用户进行勒索。

智能电视如何感染勒索软件？

有些电视设有预安装游戏门户网站，用户能够在此门户网站上选择并安装游戏。但这些网站在与服务器通信时并未使用加密的网络请求。这使MitM攻击者能够修改已显示的所有应用信息以及应用本身的位置，以便诱导用户安装恶意应用。例如，用户认为自己在安装新的赛车游戏，但实际上攻击者已将安装请求重新定向至外观相同却具有木马病毒的应用版本。

在实验中，赛门铁克研究人员使用的电视运行Android系统。由于勒索软件能够蔓延至移动设备甚至智能手表，该实验希望了解攻击者是否能够利用勒索软件感染电视。

实验将采用上述MITM攻击为设定场景，赛门铁克研究人员设法挟持游戏安装程序，并请用户在电视上安装和启动恶意应用。不出所料，几秒钟后，恶意应用开始运行并锁定电视，并在屏幕上显示勒索信息，导致电视无法使用。该勒索软件每隔几秒便会显示勒索信息，用户无法执行任何与电视的其他交互动作。

智能电视如果采用常见的Android安全设置，在默认情况下，该安全设置会禁止从第三方市场安装，并要求验证下载应用。这些设置会帮助用户最大程度地降低意外安装恶意软件的风险。用户需要在修改设置前认真考虑安全风险。

（李国敏）