目录

[2018国际智能科技峰会31号 1](#_Toc511308152)

[1. 何晓冬：多模态智能 1](#_Toc511308153)

[2. 李新社：聚焦 AI 安全 1](#_Toc511308154)

[3. 杨强：人工智能和普惠金融 1](#_Toc511308155)

[4. 刘荣：智能外科的机遇与挑战 1](#_Toc511308156)

[5. Karthika Mohan：Causal Knowledge in Artificial Intelligence 1](#_Toc511308157)

[6. 丁军：看清神经系统 1](#_Toc511308158)

[7. 付英波：用 AI 构建「五度」城市感知 1](#_Toc511308159)

[8. 李航：今日头条的愿景与实践 1](#_Toc511308160)

[9. 阎镜予：构建人工智能产业园 1](#_Toc511308161)

[3/31pm 1](#_Toc511308162)

[10.深信服：机遇与挑战 1](#_Toc511308163)

[11. 人工智能的法律法规 1](#_Toc511308164)

[12. 基于人工智能的风控与反欺诈引擎 1](#_Toc511308165)

[13. 电子科技大学——智能汽车与网络安全（罗蕾） 1](#_Toc511308166)

[14. 360 人工智能的应用安全风险--李康 1](#_Toc511308167)

[15. baiduAI模型与Paddle对抗工具 1](#_Toc511308168)

[16. 顶像--用户画像 1](#_Toc511308169)

[17. 阿里ML安全--施亮 主机异常行为智能检测 1](#_Toc511308170)

# 2018国际智能科技峰会31号

2018国际智能科技峰会31号 1

1. 何晓冬：多模态智能 1

2. 李新社：聚焦 AI 安全 1

3. 杨强：人工智能和普惠金融 1

4. 刘荣：智能外科的机遇与挑战 1

5. Karthika Mohan：Causal Knowledge in Artificial Intelligence 1

6. 丁军：看清神经系统 1

7. 付英波：用 AI 构建「五度」城市感知 1

8. 李航：今日头条的愿景与实践 1

9. 阎镜予：构建人工智能产业园 1

3/31pm 1

10.深信服：机遇与挑战 1

11. 人工智能的法律法规 1

12. 基于人工智能的风控与反欺诈引擎 1

13. 电子科技大学——智能汽车与网络安全（罗蕾） 1

14. 360 人工智能的应用安全风险--李康 1

15. baiduAI模型与Paddle对抗工具 1

16. 顶像--用户画像 1

17. 阿里ML安全--施亮 主机异常行为智能检测 1

在 31 号单天的 17 个演讲中

涉及到 AI+医疗、AI+金融、AI+安防、大数据、脑科学等领域

还有国家工业信息安全发展研究中心代表上台演讲，不同角度来看待AI安全

有 5个 提到了 深度学习，

有 3个 展示其 人工智能实验室 的一些结果，

有 8 个提到了人工智能安全问题（360李康：安全的核心是对抗）

以下是提到的一些关键的一些关键点：

* 何晓冬：多模态智能
* AI 安全态势感知--李新社
* 李新社—有红就有黑，AI 安全评估测试平台建设，建立攻防的环境
* 维度，精度，密度，关联度，集成度 五个维度来看AI
* 今日头条—人工智能实验室研究成立
* 开源、开放、免费、创新 --星河-阎镜予
* 深信服—Model的鲁棒性，与文件检测的精度
* 半监督的机器学习- AHI Fintech 创始人—黄铃
* baiduAI模型与Paddle对抗工具github : https://github.com/PaddlePaddle/models
* 阿里-主机异常行为智能检测（沙箱，溯源，计算，迁移学习，批量标注，情报，行为序列，NLP，Embedding,复杂网络）

## 何晓冬：多模态智能

《多模态智能：语言和视觉的感知、推理及表达》

他表示，多模态智能包括文本、图像、结构化知识等。谈到为什么要做多模态智能，他简单回顾了视觉感知方面的进步。他说到，由于深度学习技术的进步，计算机很早就在一些测试上达到人类水平。但是，计算机对真实世界的理解仍然是一个巨大挑战。其中，语义理解与认知是难点。

「首先要建立语义空间，联结图像与文字；然后要加入结构化知识来帮助深度认知，识别人名、地点等信息。最后，可以深入模型内部，用语言来表达对图片内容的理解。」

他表示，AI 会持续关注场景中的各个局部，并生成对应的语言描述。他举了一个棒球运动员在扔球的例子，并详细描述了计算机的处理过程。接下来，他还举了一些真实的场景应用——利用 AI 用文字来形容照片。

进一步，他们从生成一个句子发展到生成一篇短文。比如给 AI 一系列照片，让其描述照片之间的关联，说出一个故事。他表示，为了做到这一点，他们推出多重深度增强学习来保证句子间的逻辑性。而再往后，他们试图在语言表达中加入情感和风格。

他说到，前面描述的例子都是感知和一般认知，接下来有趣的工作是从感知到推理，例如让计算机回答关于一副图片的问题。他提到推理的难点，「为了回答问题，需要识别和理解物体间微妙的关系，还要能结合问题进行分析和推理等等。」为了模拟推理，他们做了一个基于多重关注神经网络的系统，主要涵盖四个模型，语言模型、图像模型、多重关注模型、答案预测模型，他也进一步讲解了这些模型具体的功能以及整体推理过程。

他谈到他们希望计算机能理解语言，并能用绘画来表达。比如智能绘画机器人。他表示，最近一两年，技术迎来飞速发展，对文字中没有提及的细节，AI  绘画机器人还能自动想象填充。

在演讲的最后，他表达了自己的展望，希望能通过这一系列技术，把人和世界更好地连接在一起。

## 李新社：聚焦 AI 安全

第二位演讲嘉宾是国家工业信息安全发展研究中心副主任李新社，他主要谈到我国人工智能发展态势以及 AI 安全方面的问题。

演讲伊始，他指出，随着信息技术等的发展，数据呈现出年度倍增的发展态势，而 AI 技术也逐渐向产业渗透并得到广泛应用，目前运算能力大幅提升，算法模型不断优化。

他表示，可以将人工智能产业链分为三个层次——基础支撑层、中间技术层、上层应用层。他进一步提到 AI 在全球的发展，「各国政府将 AI 上升为国家重要战略，中国也不例外。我们中心对多个省、市进行了调研，发现我国很多产业园区把人工智能作为发展方向。」他总结到，产业技术不断涌现，不断出现新的产品，接下来，把人脑能做的事情变成 AI 能做的事情也不再遥远。

他强调，我国从产业、标准、安全技术政策都在关注 AI 发展。「如果把 17 年当 AI 元年，那 18 年 AI 将会呈现井喷式的发展。」

他也提到，我国在语音、图像识别等技术方面领先，但底层芯片发展还有很大发展空间。目前来说，产业环境比过去好很多。而伴随着人工智能的发展，安全问题无处不在。他表示，AI 安全涉及到数据、智能电子产品等多个方面。他举了一系列实际案例，比如生物特征识别方面的问题，智能网联汽车方面的问题。接下来，他具体描述了数据层面、芯片层面、软件层面的风险。

之后，他对国家工业信息安全发展研究中心进行介绍，他表示，中心是支撑我国工业领域信息安全国家级研究与推进机构，他也具体描述了中心的工作，主要包括产业调研与分析、技术标准研究等。

他们下一步工作设想如下：加强 AI 安全技术的研究与应用，推动重点领域 AI 安全评估测试平台建设，开展 AI 安全态势感知，构建检测预警机制，加强技术交流与合作等。最后他提出期待与愿景，希望大家一起做好安全工作。



## 杨强：人工智能和普惠金融

在李新社的演讲结束之后，香港科技大学讲座教授杨强带来了主题为人工智能和普惠金融的演讲。

杨强提到，前面出场的两位嘉宾，一位从技术角度，一位从产业发展趋势的安全角度谈 AI，他目前比较关注的是普惠金融，想结合自己的关注方向讲讲对人工智能落地的看法。

杨强先是提到 AI 的发展历史，智能体的特征，AI 需要的技术，然后探讨如何促进 AI 落地。他具体谈到监督学习和强化学习。

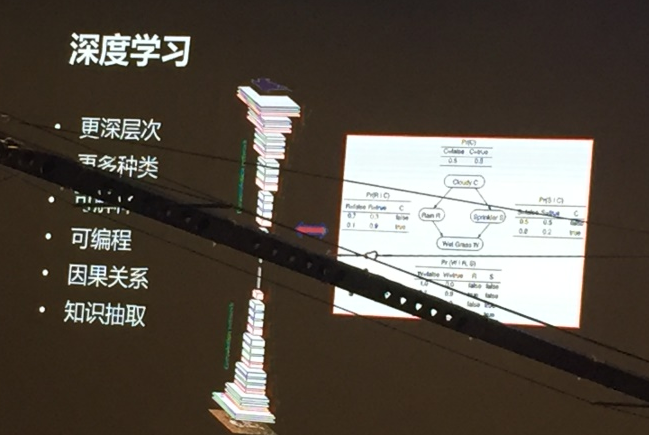
他表示，基于以上种种谈到的技术，我们探讨 AI 落地时，未来企业的发展应该是以机器智能为核心。而他也描绘了人工智能落地的过程——目标在哪里？数据在哪里？问题边界在哪里？特征在哪里？持续的反馈、自学习方法在哪里？

杨强说到，人工智能的落地，需要有三点，一是很短的商业闭环，二是高频交互，三是快速迭代。在金融领域主要关心两个方向，即成本和效率。

当 AI 介入之后，模型由简单变复杂，控制由手工变为自动，服务由通用变成自动化。在这个趋势之下想象 AI 可能的落地爆发点，有智能客服、销售，新闻写作、分发，物流、仓储、定价系统等。

而杨强进一步谈到人工智能的挑战。「深度学习的可解释性是一个巨大的挑战，此外模型需要具备可编程性，另外，对于语言模型中自动摘要、自动文本的生成，我们还处于比较初级的阶段。」

他接下来提到普惠金融方面的一些实例，他们着重强调如何利用强化学习、深度学习、自然语言处理来提供个性化客服。他表示，在互联网金融的背景下，有很多人工智能场景，比如人脸检测、声纹检测等。



## 刘荣：智能外科的机遇与挑战

接下来，解放军总医院 (301) 全军肝胆外科研究所所长、肝胆外二科主任刘荣为现场观众科普了智能外科。

演讲伊始，他表示，今天在座的基本都是做人工智能研究的，可能对外科感兴趣的非常少。他对智能外科下了个定义，即利用人工智能的工具和方法，辅助或替代人类进行外科诊疗行为。主要特征有诊疗行为标准化，诊疗设计个性化。

谈到为什么要发展智能外科，他表示，「老龄化增加了医疗需求，优秀的外科从业人员稀缺，智能外科可以减少对人力资源的依赖。此外，分级诊疗落地难，智能外科有望实现医疗行为标准化。而从政府角度来看，国务院、卫计委等机构出台的一系列政策也在支持智能外科。」

他表示AI 投资热度不断上升，人工智能和大数据技术不断得到发展和进步，这些都有助于推进智能外科的发展。

而智能外科主要有哪些应用呢，他也一一举了例子。例如智能影像诊断系统、多模态影像融合分析、影像识别和器官分割、三维重构、术前仿真、手术视频解析、手术导航等等。他表示，术前仿真可以帮助外科医生规划手术路径，进行手术模拟，远胜于以前的动物模拟手术。手术视频解析可以帮助医生在手术中做出合理选择，规划下一步手术操作。手术导航可以降低手术难度，提升手术质量，辅助新医生培训等。

而实际应用，他提到达芬奇手术机器人，他表示，达芬奇是目前比较成熟的手术机器人，他为大家展示了达芬奇做手术的视频，可以看到机器人的手非常灵活。此外，还有美国去年十月上市的腹腔镜手术机器人、STAR 自动缝合手术机器人、谷歌和强生开发的手术机器人系统等。

演讲最后，他提出对智能外科的近景和远景展望，他表示，在以后，希望能实现智能手术，利用人工智能驱动手术系统进行手术操作，医生在其中起到监督作用。他同时也列举了一些挑战，比如存在数据壁垒，此外医工结合专业背景的人才非常少。

## Karthika Mohan：Causal Knowledge in Artificial Intelligence

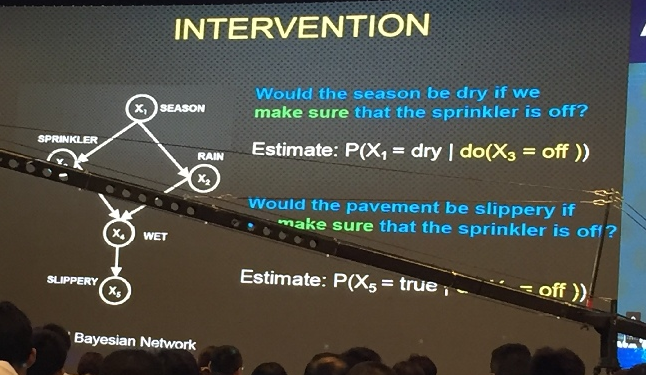
之后是加州大学洛杉矶分校博士 Karthika Mohan 带来的一场学术报告，她的演讲主题为 Causal Knowledge in Artificial Intelligence。

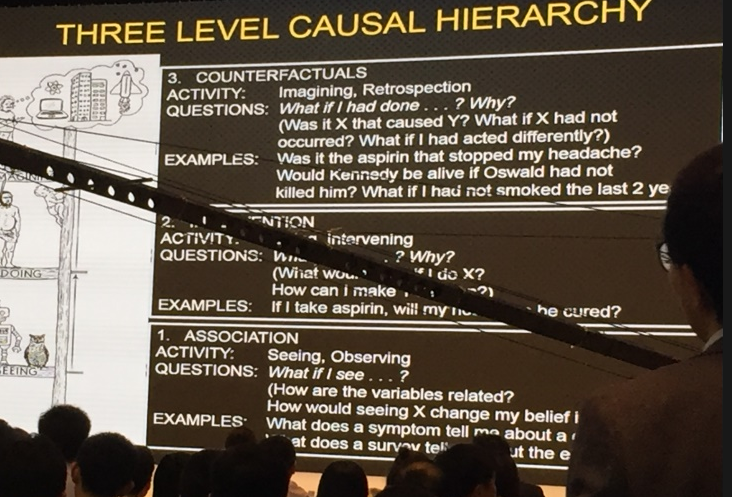
演讲伊始，她表示，建立一个与人类似的 AI 系统，因果知识非常重要。她接下来提到三层因果关系，即 Counterfactuals，Intervention，Association，之后，她说明了因果模型能解决目前 AI 系统的局限性，最后，她详细描述了来自因果推理的七个启发。

值得一提的是，Karthika Mohan 是图灵奖得主、贝叶斯网络之父 Judea Pearl 的学生，原定来到现场进行学术报告的 Judea Pearl 因故未能抵达，她作为参会代表，在简短的十五分钟内展示了在 Judea Pearl 带领下做的一系列工作以及他们面向 AI 的解决方案。

她详细描述了这七个启发，一是因果假设的透明性和可试性，二是介入性疑问分析，三是反事实算法，四是调解分析和直接、间接效应的评估，五是外部效度和样本选择偏差，六是数据丢失，七是挖掘因果关系，对于每一个启发，她都引用一系列案例，展开详细的说明和总结。

演讲的最后，她表示，Judea Pearl 教授等人的《The Book Of Why》即将会有中文版呈现，希望大家能够喜欢。





## 丁军：看清神经系统

下一位带来演讲的嘉宾是美国斯坦福大学神经科学研究所丁军，他的演讲主题是看清神经系统。他表示，他们实验室用光学手段来进行神经网络系统的研究。他提及，各国都提出发展脑计划，比如美国、欧洲、日本等，这证明大家对脑科学的重视。

接下来，他回归正题，谈到神经回路和类脑计算。他说到，神经回路和 AI 网络的不同点大于相同点，人体的神经回路很难研究，其中有百亿神经元，万亿级的突触连接。他们在实验室比较常见的研究对象是老鼠、猴子等。

他表示，其实，一百年前对神经回路就有相关研究，但今天神经科学仍然处于原始数据采集阶段。他接下来展示了脑中的图像，他解释道，图像看起来很美丽，但实际上是经过处理的。

之后他介绍了如何看清神经网络的工作，他们通过一系列技术，可以看到老鼠的整个脑区，比如海马体、皮层神经元。他表示，这样只能看处理过的脑区，他们想要看到活的脑区，而这里他们应用了一系列最新技术，成功观察到结果。他也提到如何建立细节性的神经元模型，对神经元的活动进行模拟。目前，用迷你显微镜结合内窥镜，可以看到非常深入的脑区。

而他表示，之后的目标是形成机器和人脑之间的共连接。其中的挑战是机器和人脑的信息传递方式不一样，他也为大家阐明了解决方案。

## 付英波：用 AI 构建「五度」城市感知

下一位演讲的嘉宾是旷视科技总裁付英波，他介绍了如何用 AI 构建城市大脑，让社会更安全。

他先是介绍了旷视科技的研究方向以及他们一系列的融资，他表示，旷视是一家专注于计算机科学的企业，主要做计算机视觉技术工程化的研究和方案的落地。他详细讲解了计算机视觉场景在安防领域的落地。

付英波表示，中国安防市场非常大，也有非常多的摄像头资源，但之前在公共场所建的大量摄像头没有实时分析功能，更多的是事后排查，他们希望引入计算机视觉相关技术，让摄像头由看见变成看懂。

他解释道，看懂这一块分五个度——维度，精度，密度，关联度，集成度。接下来他具体展开讨论。

* 对于维度，他先是谈到人脸，比如分析年龄、性别表情等；此外有行人特征，其中有分析轨迹、停留、行进方向等；对于车辆，包括看清车辆车标、车型、号牌、颜色、撞损情况、驾驶员行为分析等；最后是电子信号，包括设备 Mac、电子证件、RFID 等。
* 接下来是精度，他表示，他们在人脸识别上的检验精度两年间提升 10 倍并超越人类，图像识别及动作识别夺得了三项世界冠军。在实际应用场景下，他们主要关心首位命中率和抓拍检出率。
* 对于密度，他表示，这决定了数据连续性，想要做到跨摄像头的分析需要有一定密度。
* 至于关联度，付英波谈到，他们会将人脸和人，车牌和车结合起来，希望通过关联度的分析，为公安提供重要的依据。

之后，他总结到，希望通过五度感知+数据应用，创建城市大脑，在五度感知下，做存储和计算。

而他也提到他们在全国的战果，截至目前，他们已在全国协助抓捕在逃犯超 3000 人。此外，他表示，他们刚推出一款全球最快单帧人脸抓拍机，集成度非常高。

演讲的最后，他表示，希望赋能城市之眼，构建城市大脑，赋予终端思考能力，让社会更安全，让全民有更好的安全体验。

## 李航：今日头条的愿景与实践

之后迎来今日头条人工智能实验室主任、东京大学计算机科学博士李航的主题报告。

李航先是展示了头条在人工智能方向的工作。他表示，我们现在处于 AI 和移动互联网时代，数据量呈现指数级增长，而现在 AI 技术依赖大数据也得到快速发展。

他说道，头条的愿景是做全球内容创作与交流的平台，这里的核心技术是推荐引擎，包括大数据以及先进的人工智能算法，希望能促进大家创作和交流。他也提到头条母公司字节跳动 2017 年底的新产品抖音，他表示，抖音在春节之后日活跃用户几千万，在抖音的创作中，有些让大家感受到生活气息，有些让大家感受到艺术创作的魅力。「抖音是头条 AI 科技创新力的体现，体现了头条既有算法创新，又有产品开发和运营的能力。」

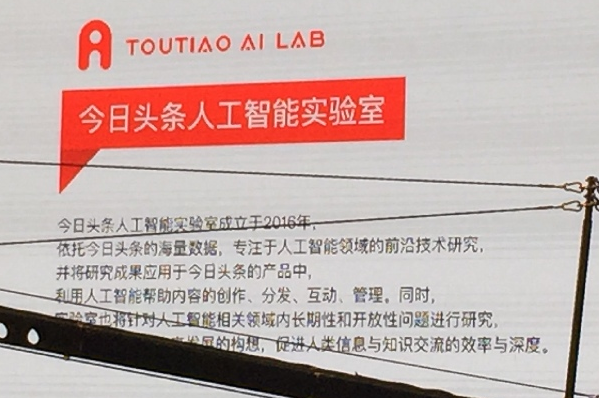
接下来，他强调，头条不光是在中国推出产品，在全球也在进行布局。

他们的关键技术是推荐引擎，共有四代。第一代基于策略，到现在发展为第四代，具有丰富层级的特征、复杂的模型组合，目前线上模型参数已经达数千亿，数据也非常大，每日请求数超过 100 亿次，算法的更新每天大概 750 次。

李航表示，他们的商业模式主要是广告，比如开屏广告、信息流广告、详情页广告。他们有广泛的观众覆盖范围和丰富广告位置，AI 驱动的精准营销带来极好的回报。

而之后，他简单介绍了今日头条人工智能实验室的成立历史和成立背景。他表示，实验室的主要研究领域有机器学习、计算视觉、自然语言处理、语音处理。核心优势在于拥有海量数据以及丰富多样的实际应用场景，在人、数据、算法、内容上有完整的反馈闭环等。

演讲最后，他介绍了头条的写稿机器人（小明机器人），他表示，未来希望通过机器人写作辅助我们更好地写作。



## 9. 阎镜予：构建人工智能产业园

最后一位带来演讲的嘉宾是星河产业集团副总裁阎镜予，他介绍了星河集团在人工智能产业园上的布局与规划。

他表示，前面出场的各位嘉宾都是各个行业的专家，他将作为地产商与行业的投资者与大家进行分享。

他先是提到人工智能发展的几个瓶颈：

* 一是稳定性，可以发很好的 paper 并不意味着可以做出很好的产品；
* 二是可解释性，目前很多模型都不可解释；
* 三是结构性，比如如何在非结构化的场景里更好地做出判断；
* 四是目标函数，比如单目标优化和多目标优化，如何在多个目标函数中得到最优；
* 五是人类评价，人类评价标准非常不同。

他们目前在做人工智能产业园，试图打造出全天候海陆空人工智能测试基地。他表示他们有专业强大的人工智能投资能力，致力于在园区打造丰富的人工智能圈层建设和主题活动。政府的扶持对人工智能发展非常重要，他们园区内部有便利的政策资源对接。此外，他们为人工智能初创企业提供很多相关的创业培训。

在演讲最后，他强调，他们会针对人工智能行业提供最低折扣优惠，以及租金换股权等方式降低企业成本。他表示，大家要是来龙岗，可以选择他们的园区。

在所有嘉宾的演讲结束之后，迎来启智开源许可证 1.0 发布仪式。北京大学计算机系主任、新一代人工智能产业技术创新战略联盟秘书长黄铁军作为仪式主持人，在现场对启智开源许可证进行详细介绍。

黄铁军表示，新一代人工智能产业技术创新联盟的重要目标是创立人工智能开源开放平台，这也是他们发布启智开源许可证的目标。

启智开源许可证定位如下：

* 新一代人工智能重大科技项目的成果汇聚平台；
* 新一代人工智能发展规划的产学研合作桥梁；
* 中国人工智能产业和应用坚实可靠的基础设施；
* 全球人工智能产业和应用发展的最佳选择；
* 人类命运共同体开放可信的智能大陆。

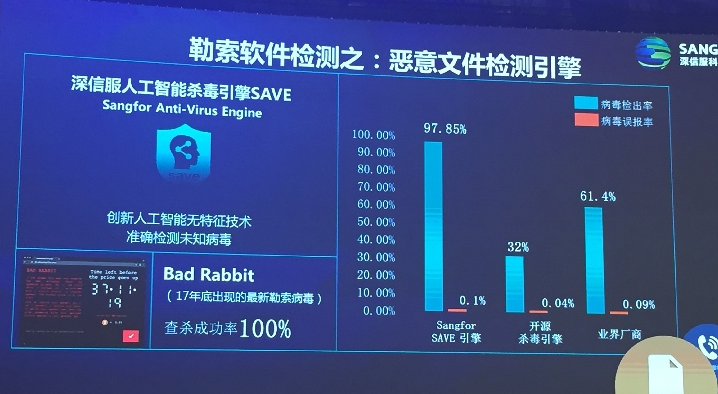
许可证的原则是完全开源、完全开放、完全免费、尊重创新。

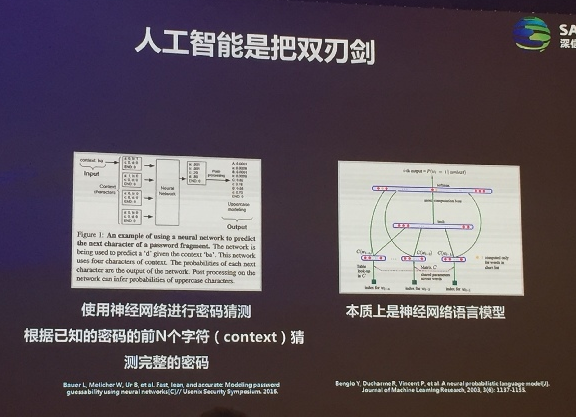
黄铁军说到，有很多专家为许可证的出台做了贡献，其中包括北京大学法学院知识产权专家张平教授，中国开源软件推进联盟专家委员刘明博士，开源中国社区创始人 CTO 红薯（刘东），而刘明与刘东也上台参与了此次发布仪式。

## 3/31pm

## 10.深信服：机遇与挑战

Model的鲁棒性





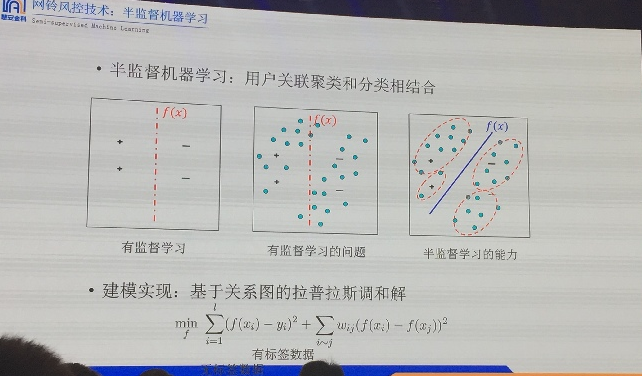
## 11. 人工智能的法律法规

## 12. 基于人工智能的风控与反欺诈引擎

用户模型创建于安全分析，AHI Fintech 创始人—黄铃

企业面临有组织的攻击，how do feac it ?收集有标签的数据是很宝贵的，建立机器学习的 模型，发现新的病毒变种。

有监督的机器学习 or 半监督的机器学习(近似计算，主动寻找意外行为)半监督建模-----聚类分析



## 13. 电子科技大学——智能汽车与网络安全（罗蕾）

Safety【安全可靠】 and Security「安全保密」

自动驾驶的发布in USA.....相关标准的发布

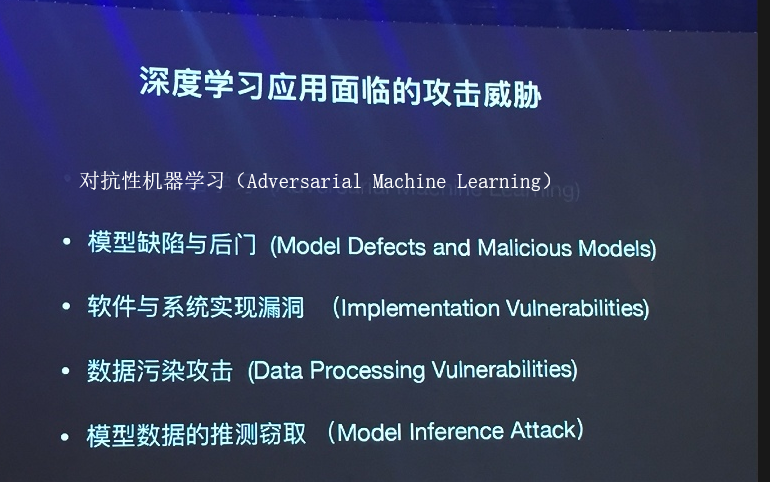
## 14. 360 人工智能的应用安全风险--李康

智能攻防，安全对抗战与培养。

为什么要关心AI安全，，，深度学习的应用（刷帖，班级的迟到早退）

AI 破解验证码，，

安全的核心是对抗



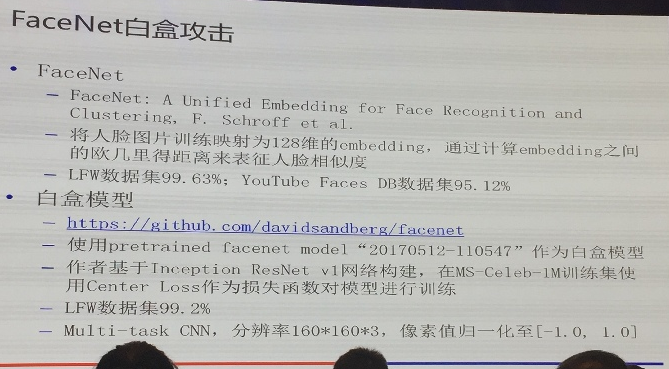
## 15. baiduAI模型与Paddle对抗工具

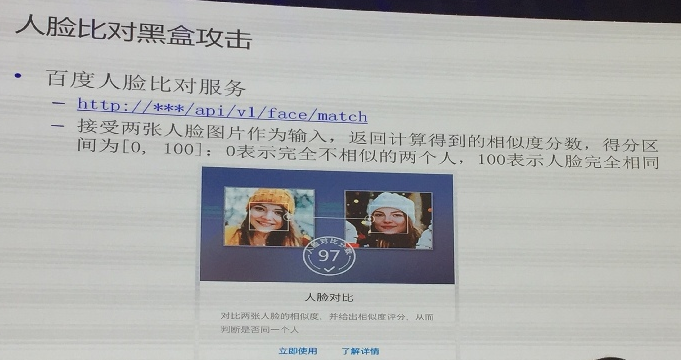
人工识别的熊喵小明星，黑盒攻击套路，和白盒生成方法（it is good）

github：；https://github.com/PaddlePaddle/models

人脸识别的制定生成攻击样本，又是人脸识别

BIM类的方法





## 16. 顶像--用户画像

数据采集的质量--风控体系保护数据质量

综合评估风险和业务画像 --是否是黄牛

深度画像的意义---风险与价值

## 17. 阿里ML安全--施亮 主机异常行为智能检测

迭代学习

拟合&误报

N-gream

又一次说到深度学习的好处和未来在迁移学习的

沙箱，溯源，计算，迁移学习，批量标注，情报，行为序列，NLP，Embedding,复杂网络

