AI 死亡启示录

人工智能2019-04-22

这是一个真实的故事。

今天 Reddit 机器学习板块最火的话题，莫过于一个“亡于 AI”的帖子，作者分享了发生在自己公司的一个故事：

在 A 公司有一支传统的 X 团队，他们使用本地 ERP 工具和传统编程语言进行高级分析，整个工作流程非常流畅，工具也非常有效，都是基于非常深入的业务和领域专业知识而设计的。

随后来了一支 Y 团队。这是一个全新的、充满雄心的数据科学团队，他们认为，X 团队的工具不够 fashion，完全可以用几个 R 脚本 + 一个定制的 ML 平台，直接干掉 X 团队现在使用的工具。

Y 团队的模型非常简单，甚至有点过于简单了。但看起来，明显比 X 团队使用的计量经济模型更加 “fashion”，加上 Y 团队顶着“机器学习”和 “数据科学”的 光环，因此领导层决定让 Y 团队对现有的相关分析平台进行大规模的改造。

但是，Y 团队并没有类似这种大规模转型的经验，而且他们还拒绝与 X 队合作。最终，作者预测这个项目的结局很可能是走向失败的，并会在整个财务和人员的角度，对整个公司造成严重伤害。

在当前环境下，数据科学社区带出来的风气，对 AI 的盲目崇拜，也是导致上述现象频发的原因。

今天新智元将 A 公司的惨痛教训详细还原，以警醒 AI 从业者。

X 团队：工具老派，专业知识够硬

A 公司已经存在几十年了，它不是其领域中最大的公司，但也备受尊敬。自 90 年代以来，风险分析和投资组合优化一直是 A 公司业务的核心，他们有一支由 30 名左右的分析师组成的大型团队，每天都在执行这些任务。

这些分析师使用由大型 ERP 公司（SAP、Teradata、Oracle、JD Edwards 等）或大型技术咨询公司（德勤、埃森哲、普华永道、凯捷等）与内部工程团队合作为他们实施的 ERP 解决方案。

使用的工具都是老一套的：在预置型服务器甚至大型机上运行经典的 RDBMS，使用 COBOL 编写的代码，Fortran 语言，ABAP 或 SPSS 之类的专有工具…… 你懂的。但模型和分析函数相当复杂，与已发表的学术论文相比，它们令人惊讶地处于前沿。

最重要的是，它们与公司的企业生态系统非常吻合，并且是基于多年深厚的领域知识磨练而成的。

他们拥有一支由几名工程师（从上述软件和咨询公司挖来的）和产品经理（从使用这些软件的经验丰富的分析师和管理人员中挖来，或从商业竞争对手挖来的）组成的技术团队来维护和运行该软件。

这些人的技术可能是老派的，但总的来说，他们非常非常了解这个领域和公司的整体架构。他们指导公司进行了几次大规模的升级和迁移，而且总是能按时交付，没有太多的开销。

虽然有几次他们出了 bug，但他们知道如何快速解决。事实上，在所处的行业利基市场中，他们以其专业知识而闻名，并与他们不得不打交道的各种供应商保持着非常好的关系。

有趣的是，尽管每天都要使用统计建模和优化算法进行处理，但参与其中的分析师、工程师或产品经理都没有自称为数据科学家或机器学习专家。这主要是一种文化传统：他们所获得的专业知识早于 2010 年左右开始的数据科学 / ML 的炒作，并且他们的大部分技能是使用专有的企业工具而不是当今流行的开源工具获得的。

他们中的一些人接受过正式的统计培训，但大多数人来自工程或领域背景，并在工作中学习了统计学。让我们称这支团队为 “X 团队”。

Y 团队：试图用 AI 解决所有数据问题

在 2010 年代中期左右，A 公司开始出现一些严重的令人焦虑的问题：尽管对于这样规模的一家公司来说它做得很好了，但整体经济和人口发展趋势正在缩小其客户群，一些所谓的破坏者开发出了一个新的应用程序和业务模式，开始严重侵蚀他们的收入。

必须采取适当的措施来安抚股东和投资者。A 公司已经有了一个不错的网站和一个相当时髦的应用程序，还有什么可以做的呢?领导层决定，现在是时候让人工智能（AI）和机器学习（ML）成为公司业务的核心部分了。

这时候，一位雄心勃勃的经理——没有科学或工程背景，只是几年前简短地玩过一个推荐系统——被选为创建数据科学团队的负责人，组建起一支 “Y 团队”。

Y 团队主要由内部员工组成，他们决心要成为数据科学家，并在加入团队之前完成了 Coursera 认证或 Galvanize 新兵训练营，此外还有一些刚获得博士或硕士学位的新人。他们不喜欢学术界，想要在工业界一展身手。而且他们都是非常聪明的人，会写很棒的博客文章，也会发表鼓舞人心的 TED 演讲，但总体而言，他们几乎没有任何实际的行业经验。

就像现在流行的那样，这个团队是数据科学组织的一部分，绕过 CIO 和任何技术或商业副总裁，直接向 CEO 和董事会汇报，因为 A 公司想在即将召开的股东大会上宣称这个团队是 “数据驱动” 和 “AI 驱动” 的。

在之前 3 到 4 年的时间里，Y 团队开发了一些 Python 和 R 脚本。他们的架构经验基本就是将 Flask 连接到 S3 bucket 或 Redshift tables，其中几位更有资源的人学习如何将他们的模型插入到 Tableau 或如何启动 Kuberneties pod。但他们并不担心：前面提到的经理(现在的团队主管)，是一个玩公司政治和自我推销的高手。

不管 Y 团队生产的可操作的成果有多少，或者他们部署到生产中的代码有多少，他总是支持他们，并确保他们有充足的资金。

事实上，他现在已经制定了一个宏伟的计划，即建立一个通用机器学习平台，用来解决公司的所有数据问题。

但是，真正的问题才刚开始。

冲突产生：互相看不对眼，拒绝沟通和合作

Y 团队中一些头脑清醒的成员，在搜索了他们的行业名称和 “数据科学” 这个词后，意识到贝叶斯模型是风险分析的主要解决方案，而且已经有一个漂亮的 R 语言工具包可以用，他们在 R-Bloggers.com 研究了相关的教程。

其中一位成员甚至在 Kaggle 数据竞赛平台上提交了一个 Bayesian 分类器内核(在排行榜上排名第 203 位)，并渴望将他的新发现的专业知识应用到实际问题中。

他们将这个想法提交给他们的主管，主管认为这是 ML 平台的一个完美用例。他们立即开始工作，完全没有费心去了解 A 公司是否有人已经在做风险分析。因为他们的组织是独立的，所以他们在获得资金之前并不需要和任何人核查这些问题。

尽管他们所做的本质上只是一个朴素贝叶斯分类器，但为了给董事会留下深刻印象，他们在项目名称中加上了 ML 这个术语。

然而，随着他们工作的进展，紧张的气氛开始凸显。

他们要求数据仓库和 CA 分析团队为他们构建 pipeline，最终这个项目的消息传到了 X 团队耳中。X 团队最初很兴奋：他们愿意竭诚与 Y 团队合作，并希望在自己熟悉的工具包中添加 ML。产品负责人和分析师也完全支持：他们看到了加入这个数据科学热潮的机会，而这时他们不停地听到的热词。

但由于傲慢和不安全感混合在一起的奇怪情绪，Y 团队拒绝与 X 团队合作，也拒绝与 X 团队分享任何长期目标，即使他们去了公司的其他部门就他们创建的新模型做演示和教程展示。

X 团队生气了：从他们对 Y 团队模型的观察来看，Y 团队的方法幼稚得无可救药，在生产中几乎没有扩大规模或可持续发展的可能性，而他们确切地知道如何帮助 Y 团队实现这一点。考虑到他们对 DevOps 和持续交付的熟悉程度，将模型部署到生产环境中需要几天的时间。

尽管他们自己的技术已经过时了，但 X 团队还是足够聪明，能够将其插入到现有的架构中。此外，该模型的输出并没有考虑公司的业务将如何使用它，或如何将它传递到下游系统，并且为了让模型被采用，产品所有者可能付出大量精力。

但是 Y 团队不听，他们的领导拒绝任何沟通的尝试，更不用说合作了。Y 团队表现出来的态度是：“我们是最先进的 ML 团队，你们是传统的服务器。我们不需要你的意见。“Y 团队似乎完全无视领域知识，或者更糟的是，他们认为所有这些领域知识只需要掌握一些业务指标的定义就够了。

X 团队感到沮丧，试图向领导层表达他们的担忧。但是，尽管他们掌握着 A 公司的业务流程中重要的一环，但他们只是一个几十人左右的团队，而且他们与最高管理层也隔了好几层，在这个拥有 1000 名员工的强大组织中，他们的声音不可能被管理层听到。

与此同时，Y 团队里这位势不可挡的主管正在做他最擅长的事情：玩弄公司政治。尽管他的团队实际交付的东西很少，但他已经说服董事会，所有的分析和优化任务现在都应该迁移到尚未交付的 ML 平台上。

由于大多数领导已经知道 X 团队和 Y 团队的目标存在重叠，他的观点不再是 Y 团队要有新的洞察力，而是他们将以更准确的基于云的 ML 工具取代基于统计学的工具。

尽管学术文献中没有支持朴素贝叶斯方法比 X 团队使用的计量经济学方法更好的观点，更不用说贝叶斯优化肯定会比生产中运行的 QP 求解器更好的怪异观点了。

等死，还是找死？

X 团队不知道，最初的贝叶斯风险分析项目现已发展成为一项价值数百万美元的重大改革计划，包括最终取代 X 团队支持的所有工具和功能，以及必要的云迁移，CIO 和几位业务副总裁均已就位。

由于 Y 团队没有工程技能，于是打算公司外部找一个没有人听说过的创业公司，把构建平台的任务外包给他们。另外，选外包公司要非常慎重，因为如果选择任何知名的外包公司，老板立马就会意识到 Y 团队不行，发现其实 X 团队比 Y 团队更适合这种规模的迁移。

Y 团队没有任何主流 ERP 部署的经验，更缺乏相关领域的知识，但他们的任务却是从根本上改变 A 公司现有核心业务的业务流程。他们的模型实际上比 X 团队要差，并且与实际情况真正需要的解决方案相比，他们的体系结构简单到令人绝望。

更打脸的是，通过贝叶斯分析、以及基于目前所有的证据都表明一个更让他们寒心的事实：Y 团队成功的可能性等于 0。

也许，该项目最好的是及时被终止，但仍然损失了超过 5000 万美元，领导层换血，数十人被解雇;最坏的结果无疑就是整个公司陷入困境。鉴于风险分析和投资组合优化对公司 A 的收入流的重要性，它可能不会破产，但会失去其大部分业务和员工。

古话说得好 “不上 ERP 等死，上了 ERP 找死”。错误实施 ERP 导致公司垮掉的大公司并不少见，例如 National Grid US，SuperValu 和 Target Canada。

结局

Reddit 发帖的作者认为，这次崩溃的核心驱动力确实来自于对数据科学家、机器学习模型以及 AI 的承诺的盲目信仰，以及在机器学习群体中非常普遍的炒作和自我推销的整体文化。

对机器学习 / 数据科学的过度关注需要为项目失败负责吗?

在 Reddit 的评论里，一些人认为这个锅技术不应该背!完全就是领导者的决策失误。因为在这个案例中，把机器学习、数据科学换成其他任何一种新兴的技术，最终的结局很可能是相同的。

作者也认为，不论机器学习也好、数据科学也好，只要能放在正确的场景中，确实可以正确的得偿所愿。将先进的机器学习技术、放在合适的场景中、并将成本控制在合理的范围内却拉低公司竞争能力的情况，没有理由发生。

此外，作者还认为，出现这种情况的原因既有公司决策问题，也有对 AI 的盲目崇拜问题，以下三点可能是公司引入 AI 之前应该警醒的教训：

认为数据科学团队应该独立运作。过度自治导致和公司业务、其他团队脱节。

由于对机器学习和数据科学的过度炒作，导致人们以为数据科学家是个全能型人才，啥都会。再有机器学习能力的加持，哇!简直没有什么问题是这位数据科学家不能解决的。

过度关注工具和基础知识而缺乏深度的经验。一个人可能了解 Python、R、Tensorflow、Shiny 等编程工具;有 Coursera 证书;写过点赞好几千的数据科学、机器学习文章，但根本对实际问题一无所知。如今的数据科学面试题基本都是：解释 p 值;解释弹性网络回归;如何在 sklearn 中使用模型… 拜托，任何会打字的人都能在 Stackoverflow 或 Cross-Validated 上查看这些问题的答案。实际上面试应该这样提问 :为什么投资组合优化使用 QP 而不是 LP?预测是如何影响客服水平的?推荐引擎如何决定什么时候该基于内容、何时使用协同过滤…

AI 有风险，引入需谨慎。