

简译版

## 2020 年人工智能的几个网空安全问题

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	How AI and Cybersecurity Will Intersect in 2020		
原文作者	埃丽卡·奇科夫斯基 ( Ericka Chickowski )	原文发布日期	2019 年 12 月 30 日
作者简介	埃丽卡·奇科夫斯基专门研究信息技术和业务创新。		
原文发布单位	Dark Reading		
原文出处	<a href="https://www.darkreading.com/application-security/how-ai-and-cybersecurity-will-intersect-in-2020/d/d-id/1336621?image_number=1">https://www.darkreading.com/application-security/how-ai-and-cybersecurity-will-intersect-in-2020/d/d-id/1336621?image_number=1</a>		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 <a href="https://bbs.antiy.cn">bbs.antiy.cn</a> 安天公益翻译板块		
免责声明	<ul style="list-style-type: none"> <li>本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。</li> <li>本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。</li> <li>译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。</li> <li>本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。</li> </ul>		

## 2020 年人工智能的几个网空安全问题

埃丽卡·奇科夫斯基

2019 年 12 月 30 日

了解人工智能 (AI) 使用的增加所带来的新风险和威胁。

### AI/机器学习 (ML) 数据投毒和破坏

安全行业需要密切关注攻击者的最新案例，这些案例旨在给业务应用程序中的 AI/ML 训练数据投毒，从而扰乱决策和其他运作。例如，想象一下，如果企业依赖 AI 来进行自动化供应链决策，会发生什么。一个被破坏的数据集可能导致严重的产品供应不足或供过于求。

Splunk 高级副总裁兼安全市场总经理宋海燕 (Haiyan Song) 说：“2020 年会出现这样一些对 AI/ML 不利的现象：它们通过篡改或者破坏输入的数据集，这样 AI/ML 算法就会出现错误，从而导致得出错误的结果。”

### 深度伪造 (Deepfake<sup>1</sup>) 音频将企业电子邮件泄密 (BEC) 攻击带入新领域

因攻击者冒充首席执行官 (CEO) 和其他高级管理人员，诱使负责银行账户的人，以完成交易或以其他方式完成交易的名义进行欺诈性转账，企业电子邮件泄密已经让企业损失了数十亿美元。现在，利用 AI 技术，攻击者将 BEC 攻击带入了一个新的领域：电话。今年，我们看到了关于该事件的首批报告之一：其中一名攻击者利用深度伪造音频在电话中冒充一家英国能源公司的首席执行官，以欺骗该公司的某人，将 24 万美元汇到一个虚假的银行账户。专家认为，到 2020 年将会出现越来越多的 BEC 攻击，它们利用 AI 技术去制作可以模仿 CEO 声音的深度伪造音频。

“尽管许多组织机构已经教会了员工如何识别潜在的网络钓鱼邮件，但他们还没有准备好让员工来识别利用深度伪造音频制作的‘他们’的声音，因为它们非常可信，而且实际上并没有很多有效的、主流的方法来检测它们，” Illumio 公司的首席技术官兼创始人 PJ 柯纳

<sup>1</sup> 译者注：Deepfake，是由“deep machine learning”（深度机器学习）和“fake photo”（假照片）组合而成，本质是一种深度学习模型在图像合成、替换领域的技术框架。

( PJ Kirner ) 说。 “虽然这类 ‘语音网钓’ 攻击并不新鲜，但 2020 年我们会看到更多的恶意行为者利用有影响力的声音实施攻击。 ”

## AI 驱动的恶意软件规避

深度伪造只是坏人利用 AI 进行攻击的一种方式。安全研究人员对于即将出现的由 AI 驱动的恶意软件规避技术感到焦虑不安。一些人认为，2020 年将会是他们发现首个使用 AI 模型来规避沙箱的恶意软件的年份。

Blue Hexagon 的首席技术官索米拉特·达斯 ( Saumitra Das ) 预测： “为规避沙箱分析，恶意软件不会带有某些明显 ‘特征’ 或者某个具体 ‘进程’ 。传统反恶意代码技术就是根据这些特点来设置规则，从而检测到恶意软件的。但借助 AI 技术，恶意软件就能准确分析、判断其运行环境是否在沙箱中。如果是在沙箱中，则会拒绝运行，进而逃避分析。 ”

## 生物识别技术的猫鼠游戏

当使用 AI 和生物识别技术对客户进行身份验证时，金融服务领域的防欺诈世界中将会上演一场猫捉老鼠的游戏。金融机构正在迅速开发利用人脸识别和 AI 的身份验证机制，以使用移动摄像头和身份 ID 来扫描、分析和确认在线身份。但坏人会使用 AI 制造利用深度伪造技术的假冒产品，试图欺骗这些系统，将这些技术踩在脚下。

Jumio 总裁罗伯特·普里格 ( Robert Prigge ) 表示： “到 2020 年，随着基于生物识别技术的认证解决方案得到广泛采用，我们将看到越来越多的深度伪造技术因欺诈而被武器化。 ”

## 差分隐私<sup>2</sup>发展迅速，助力分析数据防护

大数据、AI 和严格的隐私规定的结合，将会给企业带来麻烦，直到安全和隐私专业人士开始创新更好的方法，来保护客户分析方法；这些分析方法给 AI 起到了重要的作用。好消息是可以使用其他形式的 AI 来完成此项任务。

爱维士 ( Avast ) 人工智能部门主管拉贾希·古普塔 ( Rajarshi Gupta ) 表示： “在未来一年中，我们将看到 AI 算法的实际应用，包括差分隐私 ( 系统 ) 。这个系统将共享数据集中的模式描述，同时隐藏具体的某个人的具体信息。 ” 古普塔说，差分隐私将使公司 “像我们

<sup>2</sup> 译者注：差分隐私 ( Differential privacy ) 是基于数据失真的隐私保护技术，采用添加噪声的技术使敏感数据失真但同时保持某些数据或数据属性不变，要求保证处理后的数据仍然可以保持某些统计方面的性质，以便进行数据挖掘等操作。

今天一样从大数据洞察中获利”，但不会暴露客户和其他个人的“任何私人细节”。

## AI 可能面临的社会伦理以及公平正义问题

在 AI 社会伦理、公平正义以及后果等方面，还会面临一些深刻的问题。这些问题与安全领导有关，他们的任务是维护依赖人工智能操作的系统的完整性和可用性。

“2020 年，我们将会从 AI 在网空安全方面的应用中获得很多新的经验教训。最近有报道称，苹果卡（Apple Card）因男女性别的不同而提供不同的信用额度，这表明我们并不容易理解这些算法的工作原理，”博思艾伦咨询公司（Booz Allen Hamilton）网空安全战略主管、RSA 会议顾问委员会成员托德·因斯基普（Todd Inskeep）说。“当我们发现 AI 所做的事与我们所看到的并不同，或是其实 AI 并没有做什么的时候，我们似乎就要面临一些难以解决的问题了。”

## 安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，截止到 2019 年 9 月 30 日，安天的威胁检测引擎为全球超过六十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如 APT 组织）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问：

<http://www.antiy.com> (中文)

<http://www.antiy.net> (英文)

安天企业安全公司更多信息请访问：

<http://www.antiy.cn>

安天移动安全公司 (AVL TEAM) 更多信息请访问：

<http://www.avlsec.com>