简译版

理解人工智能与网空安全的关系

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	Understanding the Relationship Between AI and Cybersecurity		
原文作者	David Strom	原文发布日期	2018 年 3 月 22 日
作者简介	David Strom 是一位安全顾问，为众多创业公司和成熟的技术企业提供建议。https://securityintelligence.com/author/david-strom/		
原文发布单位	SecurityIntelligence		
原文出处	https://securityintelligence.com/understanding-the-relationship-between-ai-and-cybersecurity/		
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 bbs.antiy.cn 安天公益翻译板块		
免责声明	• 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。 • 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。 • 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。 • 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空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。		

理解人工智能与网空安全的关系

David Strom

2018 年 3 月 22 日

在谈及人工智能（AI）和网空安全的未来关系时，很多人想到的第一件事就是《终结者》系列电影中虚构的人工智能程序天网（Skynet）。但也有安全专家认为，必须从更广泛的角度来理解人工智能，了解它如何影响网空安全，以及 IT 部门如何使用 AI 来规划未来的安全技术采购。（译者注：在《终结者》系列电影中，天网是人类于 20 世纪后期创造的以计算机为基础的人工智能防御系统，最初是研究用于军事的发展。天网在控制了所有美军的武器装备后不久获得自我意识，认定人类是它存在的威胁。于是倒戈对抗其创造者，采用大规模杀伤性武器[甚至核暴]来灭绝全人类，即“审判日”正式来临。）

以色列电信创新实验室首席技术官杜杜·米姆兰（Dudu Mimran）在 2018 年经济合作与发展组织（OECD）论坛的演讲和随后的博客中讨论了人工智能和网空安全之间的关系。我在米姆兰的办公室（以色列贝尔谢巴）采访了他，后来又通过电子邮件对他进行采访。

AI 和网空安全的短期和长期预测

米姆兰说：“虽然人工智能驱动的网空攻击的威胁越来越有可能，但我并不太担心机器在短期和中期内能够获得自我意识并伤害人类。我们的生活越来越依赖技术，远在我们开发出具有自我意识的机器之前，这一点将会被攻击者利用。尽管如此，如今即使没有复杂的人工智能，攻击者的大多数目标也可以实现，这就是为什么我们没有看到这种新的攻击浪潮。”

他在 OECD 演讲中提到了四个时间范围：

1) 短期的超级个性化，算法将会比我们更了解我们自己。

2) 中期的干扰，基于各种针对性的自动化工作。

3) 长期无处不在的自动化机器，如无人驾驶汽车。

4) 长期的情况，例如恶意的天网式场景。

将 AI 应用于恶意软件溯源

AI 技术最重要的应用之一是恶意软件溯源。根据米姆兰的说法，如果你了解你的攻击者“并且实时做出反应，那么你反击真实攻击者的机会将会更高。”

然而，他在 OECD 演讲中指出，溯源“因缺乏商业可行性而投资不足”。这是一个众所周知的问题，因为研究人员必须检查大量的变量，包括恶意软件的书面非编码语言，使用的文化或政治引语，以及哪些代码片段模仿现有的恶意软件结构等等。

米姆兰提出了决策者可以改善溯源的两种方法。第一种方法是支持和建立一个联合的全球情报网络，该网络包括商业和政府研究人员，可以跟踪不同地区的威胁。第二个方法是资助正在进行的研究，以帮助改善溯源，同时保护数据隐私。

“溯源是一个分布式的问题，跨越不同的技术堆栈、系统和组织，这些中央实体可以帮助编织这样的线索。”米姆兰说。他对此持乐观态度——尤其是对那些专注于这些合作创意、与欧洲最大的银行合作共享威胁情报的新型安全创业公司。

在 AI 时代保护数据隐私

数据隐私是一个重要的考虑因素。米姆兰去年写道：“大量个人数据分布在不同供应商的中央系统中，这会增加数据的泄露风险，为攻击者创造以不可思议的方式滥用这些数据的机会。”

隐私问题的一个解决方案是某种形式的基于区块链的创新。米姆兰提到了最近获得资助的 ForgeRock 等公司。“这些公司面临的挑战是与世界其他地区的整合，”他说，“身份主要嵌入到在线服务和产品中，创建一个外部中立实体为所有服务提供相同的流畅体验，这是一项重大挑战。”

去伪存真

这些技术也适用于其他网空防御战术。米姆兰说：“我们确实看到了人工智能在安全运营中心（SOC）用作自动化工具的初始努力，但这些只是初步的。”

但是，保持谨慎是非常重要的——特别是当供应商试图超卖（oversell，超出供应力地过多出售）他们的工具并声称这些工是基于 AI 的时候。CSO Online 强调了区分具有基于规

则的检测引擎的产品和利用真正 AI 的产品的重要性，因为“许多拥有数百条规则的供应商认为他们已经完成某种近似版本的 AI”，实际上仅仅验证现有的恶意软件特征不构成 AI，而仅仅是一种模式匹配。

米姆兰还提到了日益增长的物联网（IoT）僵尸网络威胁。“物联网僵尸网络的问题触及了许多松散的方面，而且没有银弹来解决这些问题。解决僵尸网络问题的最佳方法是主机之间进行合作，以及通信或服务提供商将僵尸机器的流量提供给执法部门。”他说。

远离天网式的未来

人工智能的兴起当然会使威胁情况进一步复杂化，但认识到威胁情报共享、恶意软件溯源和数据隐私的重要性的企业可以领先旨在利用技术实现恶意目的的犯罪分子一步。正确理解 AI 并进行相应投资的安全团队能够在威胁源创造"天网"之前掌握众多网空安全优势。

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，安天依托下一代威胁检测引擎、主动防御内核等自主先进技术、“赛博超脑”支撑平台和专家团队，为用户提供端点防护、流量监测、快速处置、深度分析等产品，以及安全管理、威胁情报、态势感知和靶场演练等解决方案。

安天为国家主管部门、军队、保密、部委行业等高安全需求部门，提供高级威胁和新兴威胁解决方案和能力体系，产品与服务保障了“载人航天”、“探月工程”、“空间站对接”、“大飞机首飞”等重大国防军工任务。安天也是全球重要的基础安全供应链上的核心节点，全球近百家著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴，安天的检测引擎为全球近十万台网络设备和网络安全设备、超过十亿部智能设备提供安全防护。其中移动检测引擎是全球首个获得 AV-TEST 年度奖项的中国产品。

安天技术实力得到行业管理机构、客户和伙伴的认可，安天已连续五届蝉联国家级安全应急支撑单位资质，亦是中国国家信息安全漏洞库六家首批一级支撑单位之一。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，提供了先发预警和全面应急支撑。安天针对震网、毒曲、火焰、沙虫、方程式、白象等 APT 组织或 APT 行动，进行了深度的解析，对捍卫国家主权、安全和发展利益形成了有利的支撑。

在 2016 年 4 月 19 日由习近平总书记召开的网络安全和信息化工作座谈会上，安天创始人、首席技术架构师作为网络安全领域的发言代表，向习总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了位于哈尔滨科技创新城的安天公司，对安天负责人说，“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*