CONNECTEDFUTURES
Executive Insights by Cisco

# 人工智能与安全：一场军备之战

## 人工智能有望成为网络战的关键武器，但无法在短期内取代人类安全团队。

2018年6月 Kevin Delaney

网络攻击。它们冷酷无情，比以往任何时候都更聪明，并造成巨额经济损失– 至少有一半以上的事故造成了50万美元的损失，思科（Cisco）报道。

这些威胁不仅日益增多，而且高度自动化，复杂的攻击可以自行探测、调整、隐藏和复制。这使得IT和安全团队难以应付复杂和庞大的数据量，而传统的防御策略可能无法处理这些数据。

“过去的几年中发生了大量的网络攻击，我们并非没有得到信息，” Barly Endpoint Security 的首席科学家 Ryan Berg 说，“而是除非恰好有人看到，否则人们无法处理这么多信息，从而导致警报疲劳，我们无异于大海捞针。”

在未来，对抗机器的最好防御将是其他机器。

“我们早已预见未来的机器之战，”信息安全论坛的执行董事 Steve Durbin 表示，“人工智能恶意软件攻击人工智能防御软件。但我认为这一情况会很快改变。事物变化的速度总让我们感到惊讶。

> 我们早已预见未来的机器之战 – 人工智能恶意软件攻击人工智能防御软件。
>
> – Steve Durbin，信息安全论坛

但这并不意味着人类安全团队会很快消失。

企业领导者需要正确的技术、战略和人才，进行机器对战的军备之战。这是一场只会愈演愈烈的战争，因为像机器学习这样的新兴技术及其更先进的同类人工智能扮演着越来越重要的角色––无论是攻击者还是防御者。

### 蜂拥而至的变异信息

“机器学习让我们深入到检测内容的本质。” 思科威胁情报研究团队 Talos 的 Luci Lagrimas 说，我们每天帮助用户拦阻197亿次威胁。

CONNECTEDFUTURES
Executive Insights by Cisco

# 人工智能与安全：一场军备之战

## 人工智能有望成为网络战的关键武器，但无法在短期内取代人类安全团队。

2018年6月 Kevin Delaney

例如，恶意软件和僵尸网络能够实现“变异”，这意味着安全团队面对的敌人是不断复制和改变的有时甚至毫无休止。

“攻击者每天都会生成成千上万份恶意软件，”思科 Talos 的 Matt Watchinsky 解释道。“因此，每个人都可能收到一份独一无二的恶意软件。本质上是相同的一份恶意软件，但经某种方式的修改，它变成了独一的一份。”

但是防御者，也变得越来越智能。

“这是一个不断变化的世界，威胁正在成倍增加。” Radware 公司的 Erwin Kim 说，“当然防御系统的自我学习能力也在不断加强。我们说的是在不到10秒的时间内处理一个当天的变异体，或者新的攻击，如果正好有文件可以阻止它，那么就不需要人工处理了。”

但值得注意的是，这些技术带来的影响才刚刚开始，而安全方面的真正变化还需时日。

“我并不认为人工智能或机器学习已发挥全部的潜力。” Durbin 说，“话虽如此，但它确实有令人期待的潜力，比如安全事件检测、识别和传播风险信息，当然还有态势感知这个陈年话题。”

所有企业在这场战斗中都将面临巨大的威胁，而将这种潜力转化为防御力量变得越来越重要。

“我们每天要解析成千上万个事件，都需要我们采取保护措施。” Watchinski 说，“我的机构有300人，而我们真正鉴定为高危事件的90%到95%都无需人工实际处理。这些都是自动分类的。”

### 人为因素

随着安全系统越来越多地采用机器处理，那么人类又扮演了怎样的角色?

Watchinski 团队的300名专家没有被取代的风险，其他安全员工也是如此。

“电脑依然相对笨拙，” Berg 强调说，“它需要人们将上下文输入电脑，让电脑去理解事件的起因。这一点在长时间内是不会改变的。”

Sven Krasser 是 Crowdstrike 的首席科学家，他称人工智能和机器学习是“力量倍增器”。“这是一个工具，可以让我们举起更大、更重的数据集。”他说，“去做一些超越人类认知的事情。”

他很快补充说：“似乎人们将人工智能误解为独立的分析仪，但事实并非如此。”

但各种人为的网络犯罪却可以分析。

Watchinski 说：“你在安全领域所对抗的是另一个人类，他只需方寸之地就能掀翻整个世界。机器要做到这一点仍然十分困难。”

他们也知道越来越强大的机器可以为他们的邪恶行径所用。

Durbin 说：“好人与坏人所能获得的资源都是一样的。”

因此，最好的策略是对人力资源进行正确的投资——用技术加以增强。这包括提升内部人才，增加机器学习，或者依赖外部供应商。在大多数情况下，综合利用这些方式才是制胜之道。

CONNECTEDFUTURES
Executive Insights by Cisco

# 人工智能与安全：一场军备之战

## 人工智能有望成为网络战的关键武器，但无法在短期内取代人类安全团队。

2018年6月 Kevin Delaney

Durbin：“这是一个很好的例子，说明我们可以将技术与人机界面结合在一起，将这两种元素结合起来，而不是由一种取代另一种。今后我们仍将面对技术短缺的情况，所以这只有好处。”

### 人工智能时代的人才缺口

虽然机器并不急于取代人类，但它们正在迫使人们重新定义保持安全和竞争力所需的技能。

考虑到 IT 领域的人才短缺，尤其是围绕机器学习这样的新兴技术，领导者必须确保他们的团队能够继续提高技能，这不仅仅是为了拓展他们的能力，更是为了吸引人才。

在思科对各大洲不同行业的600名 IT 和商业决策者进行的调查中，61%的人支持对现有团队进行技术技能再培训。（然而，他们最愿意雇佣的技术技能是人工智能/机器学习，占65%）。

“你必须不断训练，不断提高技能，” Durbin 说，“它还涉及透明度和这种公开雇佣合同，双方都明白自己的目标是什么。如果我们为你提供机器学习的相关知识，在技术上提高你的技能，你能给我们提供什么？”

“你要在机构内计划建立这种肌肉记忆。” Berg 补充说。

“如果你想拥有这种能力，就要能够自己打造，因为人才真的非常短缺。这不是一蹴而就的事情，但它要成为你公司 DNA 的一部分。”

安全不只是防御，还要融入公司的增长战略，而 CIO 和 CISO 要在最高管理层和董事会中拥有发言权。毕竟，在安全威胁带来的不确定性因素的笼罩下，创新无法蓬勃发展。

“【安全】是肌肉记忆的潜在竞争优势，” Durbin 说。“因为安全逐渐融入企业战略，成为我们进入市场的方式以及我们保护资产的方式。”这可以产生竞争优势。(阅读 Durbin 的专栏 数据和美元：首席财务官在网络安全中的角色。)

### 拙劣的演员和和唾手可得的目标

好消息是，许多网络罪犯尚未利用人工智能，但其部分原因是仍有太多的疏忽，让他们不费吹灰之力便可达成目标。例如，有不合规安全条例的机构(为什么当许多员工不假思索地点击可疑附件时，黑客还要投资于先进的技术？)

当然，这很快会改变。特别是当国家支持的网络罪犯还在不断提高他们的技能。

Durbin 说:“我认为这恰好是防守方可以抢得先机的时机，主要是因为我们所谈论的复杂程度超出了大多数网络罪犯的范围。如果你碰巧是一个民族国家或者你有一个特别庞大的网络犯罪团伙并且有大量的资源，那么你当然会沿着这条路走下去。”

无论如何，聪明的领导人都会做好最坏的打算。

“自满是很容易的，” Krasser 警告说，“但我们需要继续前进，改进技术。机器学习从未像现在这样成功。开始很容易，但它需要投资，而投资需要的不仅仅是团队中的几位数据科学家。它必须成为你战略的一部分。”

CONNECTEDFUTURES
Executive Insights by Cisco

# 人工智能与安全：一场军备之战

## 人工智能有望成为网络战的关键武器，但无法在短期内取代人类安全团队。

2018年6月 Kevin Delaney

做好最坏的准备意味着下一波攻击会彻底淘汰当前的技术，包括区块链，从机器学习到真正人工智能的进化，以及被 Watchinski 称为“密码噩梦”的量子计算。

“我们在量子计算领域还有很长的路要走。” Durbin 补充道，“但所谓的长路很可能不会超过5到6年。它有可能改变游戏规则，因为量子计算将打破加密技术，这是毫无疑问的。”

银行业等高价值目标的行业已经在研究量子防御以抵御量子攻击。

“我们谁都不知道量子计算会在何时出现，”德宾补充说，“很可能某个国家正在破解加密技术，收集信息。”

与此同时，安全和商界领袖正面临严峻的威胁，这只会让情况变得更糟。他们必须确保自己的团队拥有合适的人才和技术，继续脚踏实地——为明天的威胁做准备，并抵御今天的紧急状况。

“这是创新者的两难境地，” Krasser 总结道。“当人们对 LED 趋之若鹜时，即便你制造了一台最好的电视，也不过是无用功。同理，你要知道趋势所向，而非当前的状况。”

### 标签

Steve Durbin、机器学习、网络攻击、网络战

### 话题

风险管理与安全、人工智能与自动化、网络安全