**人工智能在战争战略层面的应用**

**王军**

和许多技术一样，人工智能（AI）也有运用到军事上的潜力。但是我们还有多久才能看到可以改变游戏规则的人工智能应用出现在战场上呢?算法战争可能成为这场军事变革的主要推动者。人工智能是国防部在奥巴马的第二个任期内提出的“第三抵消战略”的核心，也是政府推动前沿技术发展的多项举措的重点。2018年6月，国防部成立了联合人工智能中心。此前，白宫于2018年五月成立了人工智能特别委员会，并于2019年2月11日发布了《维持美国人工智能领导力的行政命令》。国防部和情报界在人工智能上的投入也增加了。而对于在民用领域有类似参照的军事应用，如后勤、规划、分析和运输等，基于人工智能的数据分析早已在整个国防领域和情报界普及。这些应用与作战应用是分开的，也不同于作战应用。后者通常分为两类：一类主要产生作战层面的影响，另一类则还会产生战略层面的影响。人工智能在作战层面的应用可能会对为实现战术目标的一般军事力量的使用产生重大影响，进而影响常规威慑的可信度。而人工智能在战略层面的应用则可能对战争的规模和范围、战争升级和降级的政治决策产生重大影响，进而影响战略稳定和威慑力。

实现精准情报、监视与侦查（ISR）的系统：对军方来说，对象识别是人工智能的基本应用，因为它要对卫星和无人机收集的图像和信息进行筛选，以发现具有军事价值的东西，如导弹、部队和其他相关情报信息。国家地理空间情报局（NGA）率先将人工智能运用于军事和情报需求。但对象识别仅仅是个开始。情报、监视和侦查（ISR）是才是多域态势感知的关键。随着战场扩展到全球范围内的所有领域——海、陆、空、太空和网络，这种整体意识越来越重要。

让人工智能来管理并理解现代战争中海量的ISR数据是一件再适合不过的事情，这同样也是国防部“专家项目”（Project Maven，也被称为“算法战争跨部门小组”）的目标。据国防情报局军事行动支持科主任杰克-沙纳汉中将称，“专家项目”的目的是“为国防部的各个部门打开使用人工智能的大门”。

起初，“专家项目”的任务是帮助定位ISIS武装分子。然而它蕴含着巨大的潜力。多域战争涉及大量的异源数据流，只有在人工智能的帮助下它们才能被利用。与民用世界中传感器数量的快速增加一样，多域混合战场已经成为军事版的物联网，其中充满了评估战术、战略威胁和战略机遇的重要信息。拥有实时管理这些海量数据的能力可以带来巨大的优势，但如果不能从这些信息中汲取意义，则可能会导致灾难。

迅速处理来自多个平台的各种部门的海量信息的能力，可以转化为两个根本性的军事优势：速度优势和距离优势。移动速度比敌人快可以提高进攻的机动性，同时也让自己更难被击中。从更远的地方实施打击，不仅更加出其不意，也能最大限度地减少在敌方火力下的暴露。这些都是在海湾战争中首次出现的军事革命的核心原则。人工智能让实时分析战场态势成为了可能，并能在最大限度降低自身部队风险的同时实施快速和最优化的打击。国防科学委员会最近的一项研究表明，这种综合战斗管理、指挥、控制、通信和情报（BMC3I）的能力非常适合于发现和瞄准已部署的导弹发射台。因此，它们可能是对抗俄罗斯和中国的反介入和区域拒止（A2AD）战略的关键要素。这些战略旨在利用美国在欧洲和亚洲的陆上和海上资产的脆弱性。除了对目标进行地理定位外，有人工智能加持的BMC3I还可以帮助引导和协调多个平台之间的动能效应，从而有可能反制敌方当前的A2AD战略。从这个角度来看，人工智能在战术层面所累积的影响可能会成为战略层面的游戏规则改变者。

精确瞄准战略资产：有人工智能加持的ISR可以定位、跟踪和瞄准敌方的各类武器系统，这也就提高了打击航空母舰、机动导弹或核武器等战略资产的可能性。这种能力以及对其存在的感知，可能会打破长期以来关于威慑稳定性的假设，尤其是当有可能对敌报复性力量实施解除武装的打击时。能够“发现、确定并解决”敌方大部分战略资产的进攻性武器，加上能够摧毁剩余报复性力量的防御系统，可能会对基于相互脆弱性的威慑基本理念提出挑战。

有效导弹防御:有人工智能加持的目标定位和导航技术的进步，通过增强获取、跟踪和识别目标的能力，改善了各种战术和战略防御系统的前景，特别是弹道导弹防御系统。然而，强大的、新的进攻和防御能力的融合，重新引发了人们对那些可能影响战略稳定的突然袭击的担忧。

人工智能引导的网络：网络本来就是数字化的，自然就适合人工智能的应用，谷歌、Facebook等社交媒体巨头的代码中人工智能算法的核心地位就说明了这一点。海量的电子格式的数据的很适合人工智能发挥其优势。人工智能引导的计算机网络探测、映射和黑客攻击可以为机器学习提供有用的数据，包括发现网络漏洞、身份、档案、关系和其他可能对进攻和防御有价值的信息。中国将人工智能用于社会监控，这引起了人们对其在隐私和民主方面的影响的广泛关注，而俄罗斯的“影响行动”则表明社交媒体容易受到操纵。在进攻性方面，人工智能可以定位并针对特定节点或个人账户进行收集、破坏或造谣等行为。例如，针对国家指挥的基础设施和网络进行网络攻击可能会是灾难性的。在防御性方面，人工智能可以帮助探测到这种入侵，并在民用和军用操作系统中寻找具有破坏性的异常情况。人工智能将同时增强进攻和防御手段，且兼具积极和消极的战略效果。总而言之，人工智能在军事领域有很大的应用潜力，在作战和战略层面都是如此。而且随着美国和其他国家对这些技术的开发，人工智能可能会催生出新的重大作战和战略优势。