人工智能算法在网络空间安全中的应用：技术与现状综述

陈捷[1,2]，武丹丹[2]，谢瑞云[2]
[1]西北工业大学网络空间安全学院，中国西安市，710000
[2]中国电子科技网络信息安全有限公司，中国成都市，610000

摘要：网络空间安全急需解决的3个技术问题是：网络攻击检测的及时性和准确性、安全态势的可信评估和预测以及安全防御策略优化的有效性。人工智能算法已成为网络安全应用增加安全机会和提高对抗能力的核心手段。近年来，人工智能技术的突破和应用为提高网络防御能力提供了先进的技术支持。本综述对2017至2022年间人工智能技术在网络空间安全领域的最新应用进行了全面回顾。参考文献来源于各种期刊和会议，其中52.68%的论文来自Elsevier、Springer和IEEE期刊，25%来自国际学术会议。本综述重点介绍了机器学习、深度学习和一些流行的优化算法在该领域的最新应用进展，对算法模型的特点、性能结果、数据集、以及潜在的优点和局限性进行了分析，强调了现存的挑战。本工作旨在为想进一步挖掘人工智能技术在网络空间安全领域应用的潜力、解决特定网络空间安全问题的研究人员提供技术指导，掌握当前技术和应用的发展趋势以及网络安全领域的热点问题。同时，本综述对当前面临的挑战提供了有效应对策略和方向。

关键词：人工智能；机器学习；深度学习；优化算法；混合算法；网络空间安全
https://doi.org/10.1631/FITEE.2200314