doi:10.1631/FITEE.1800573

题目：网络安全遇上人工智能：综述

概要：网络安全与人工智能技术有着广泛的交叉。一方面，可以将人工智能技术（如深度学习）引入网络安全领域，构建智能模型，实现恶意代码检测、入侵检测和威胁情报感知等。另一方面，人工智能模型面临针对样本、学习过程和决策等的各种威胁。因此，人工智能模型需要网络安全防护技术来对抗各类攻击，实现隐私保护机器学习以及安全的联合深度学习等。本文对人工智能与网络安全交叉研究进行综述，首先总结现有利用人工智能技术对抗网络攻击的研究工作，包括采用传统机器学习技术和深度学习技术在对抗网络攻击方面的应用和效果。然后总结和分析人工智能会遭受的对抗攻击，对现有针对对抗攻击的防御方式进行归类，分析各自特点。最后，从构建加密神经网络和实现安全联合深度学习两个方面阐述现有工作中构建安全人工智能系统的方案。

关键词：网络安全；人工智能；攻击监测；防御技术