浅析人工智能在网络安全防御中的应用

◆田　挺

（淄博职业学院 信息工程系　255314）

摘要：网络空间安全防御的主要目的是对大量的事态信息及时分析，并对不断变化的网络空间建设足够的安全防御。科技的发展促使人类的生活与网络空间息息相关，人工智能在各个领域蔓延开来。针对网络空间安全防御的人工智能技术，近年来得到了大量的科学关注，对其的研究和探索领域不断加深。本文简单叙述了网络安全防御和人工智能的基本特征，分析其应用优势，并例举出具体典型的应用实例，旨在为人工智能在该领域的发展提供有效对策，提升未来网络空间的整体安全性。

关键词：工智能；多 agent 系统；神经网络；网络空间安全防御

一、引言

计算机网络是信息时代的重要载体，在二十一世纪，全球飞速发展，计算机网络成为了与人类生活密不可分的重要组成部分。由于其具备了较高程度的网络共享性，使得个人以及公司网络安全性问题越发突出。智能化和自动化是网络安全防御的未来发展方向，人工智能技术的诞生到快速发展的过程表明了其具有的较高实用性和有效性，对其在网络空间安全防御中的研究成为了有效提高其安全防御能力的有效途径。

二、网络安全防御以及人工智能

1.网络空间

Cyberspace 即网络空间，它是一个无比巨大的虚拟画面，通过介质将所有东西相连接，其介质就是很多种信息技术的基础设施，包括了：互联网、通信网络、计算机系统以及嵌入式处理器和控制器。从另一个方向来说，即人工智能的 agent，Cyberspace 就是一个虚拟能量相互关系的一个空间。与一般人工智能相比，对环境的看法而言，其具有很多独特的特征，包含了感知、离散、复杂和对抗激烈等。在网络空间中，无时无刻不在发生力量之间的相互对抗，此刻需要智能防御、防火墙以及其他各种防御系统进行干预。

2.进攻性网络作战

进攻性网络作战指的是在 Cyberspace 中对攻击对象进行计算机网络攻击 (computer network attack， CNA) 和计算机网络刺探 (computer network exploitation， CNE) 的过程。CNA 和 CNE 的本质区别就是其方式的不同，前者属于一种恶意的网络攻击，后者属于情报收集。前者会造成计算机网络破坏、混乱，后者通过手段隐藏自己倾入对方计算机网络进行需求数据的收集。

3.网络防御

计算机网络防御 (computer network defense， CND) 是对计算机、网络以及各种信息的一种保护措施，它与计算机网络进攻组成对立统一的矛盾体，也可以进行非法计算机行动的监视以及对抗。我们经常使用的网络防御主要有防火墙、各种杀毒软件、网址的过滤，终端检测和响应等，实质性技术主要有主动诱骗、网络空间冲突规避技术以及被动信息保障等。

三、人工智能技术在网络空间安全防御应用的优势

人工智能随着人类科技的发展也在进行不断的革新与转变，由于其具有人类大脑，甚至优于人类大脑的储存和识别能力而被运用于现代的各个领域。在计算机网络空间安全防御领域，人工智能主要有以下几个优势特征：

1.模糊处理信息

人工智能具有超强的网络安全防御管理能力，它可以对人类和其他方式未知的问题进行及时处理和防御，最高程度保障计算机网络的安全性。网络空间所具有的开放性特点成为了保障网络安全的难点。信息数据的快速更新，成为了进行网络空间安全防御的最大阻碍。人工智能可以进行复杂问题的简单化，对流动性超强的信息资源进行具体分析并判断。通过结合实时网络情况，进行网络信息传播的输入与输出，保障网络空间的秩序和环境安全。因此，人工智能在网络空间安全防御的领域具有显著的优势。

2.节约资源

除了人工智能网络安全防御，其他的网络安全防御技术基本对资源的耗用都是巨大的，例如空间资源和时间资源。并且所进行的防御成效不大，造成了高耗用低质量的现象。人工智能所具有的独特优势能够在减小资源输出的基础上还能够提高网络安全防御能力，是推动网络技术发展的有效力量来源。

3.较强非线性处理能力

我国的网络空间构成复杂多变，网络空间安全防御的工作也会经常受到不可控因素的影响，造成防御工作效率低下，并且其他的网络空间防御技术智能化程度较低，非线性的处理能力不够。而人工智能的安全防御是一种结合多种学科的新兴技术，通过大量实践与充足理论支撑的产物，非线性处理能力是非常强大的，对网络空间安全防御工作的提升具有较大帮助。

四、人工智能在网络空间安全防御中的具体应用

1.神经网络

神经网络就像人类神经突触一样，是由大量的微处理单元所组成的一个庞大的神经网络。它与人类大脑能力相似，具有对信息进行分类的容错能力，学习能力，适应能力，其每一个处理单元是相对独立但整体联系的。对问题的处理可以多个同时进行，有很强的执行能力，通常需要软件和其他硬件的相互配合。神经网络能有效帮助网络空间防御进行学习和分类，对问题提供对应事件提供对应解决方案。

当前，在网络入侵检测领域。神经网络已经得到了良好的发展以及实行，比如 DDos 检测、计算机蠕虫、垃圾邮件、僵尸等检测以及分类和调查。有一些神经网络需要通过硬件或者某些图形的处理器进行工作，其具有非常快速的处理能力，在网络安全领域得以大量的运用。神经网络在大量运用的过程中也得到了一定程度的研究，例如第三代神经网络的产生又如 FPGAS (field programmable gate arrays，现场可编程门阵列) 的应用。

2.多 agent 系统

Agent 在人工智能领域运用广泛，它可以看作一个自动执行实体，需要借助传感器和效应器协助工作。多 agent 系统的快速发展，在网络空间防御领域也得到运用，因为它具有感知能力以及较强的规划能力，能有效实现势态感知、入侵检测以及人工防御。美国国土安全部门对互联网结构进行测量，Archipelago 以及 DIMES 是典型的项目，在全球的网络空间中部署很多 agent 来实现连续测量，这一项目极大程度提高了美国互联网感知力。

3.专家系统

专家系统相对其他系统而言，是一种出现时间较早，发展也较为成熟的一种人工智能技术。它主要由知识库和推理机构两部分组成，知识库主要就是对一个领域或者问题专家建议和应对过程的收集，并模拟一个人类专家进行一个决策的过程。专家系统的能力高低主要取决于内部知识库的质量，通过专家系统在网络空间防御中能够起到有效决策的制定以及自动化的开发。所以，网络空间安全防御中专家系统是很重要的。

五、结束语

人工智能技术在网络安全防御领域的研究虽然处于初始的研究阶段，它的运用和发展也备受争议，但是人工智能在人类社会不同领域的开花也预示着在网络安全领域也能够起到可以推测到的贡献性力量。我国在该领域的发展还需要更多研究工作者的关注和探究。

参考文献：

[1]刘喆.人工智能技术在网络空间安全防御中的应用[J].科学家，2017.

[2]李剑.人工智能技术在网络空间安全防御中的应用分析[J].数码世界，2018.

作者简介：田挺，男，民族：汉，职称：讲师，研究方向：网络管理、网络工程。