ISSN: 2661-3719(Print); 2661-3727(Online)

人工智能技术在网络空间安全防御中的应用

郭海龙
广州市城市规划展览中心　广东广州　510000

摘　要：互联网的发展带来了前所未有的便利，但由于互联网的开放特性，使用互联网同时也面临着内外部的网络安全挑战。如何加强网络空间安全防御能力，有效保障互联网时代数字化转型变革中的网络安全，是目前面临的重大问题。而人工智能技术的发展，驱动了新型网络空间安全防御技术的诞生，依托人工智能技术，网络空间安全防御从传统的被动式安全响应到主动式安全防御进行转变。本文主要探讨人工智能技术在网络空间安全防御的应用。
关键词：人工智能；网络空间；网络安全防御

Application of artificial intelligence technology in cyber security defense

Hailong Guo
Guangzhou City Planning Exhibition Center Guangdong Guangzhou 510000

Abstract: The development of the internet has brought unprecedented convenience, but due to its open nature, the use of the internet also faces both internal and external network security challenges. Strengthening cybersecurity defense capabilities and effectively safeguarding network security during the digital transformation in the internet age is a significant challenge. The development of artificial intelligence technology has driven the emergence of new types of network cybersecurity defense techniques. Leveraging artificial intelligence, network cybersecurity defense is shifting from traditional passive security response to active security defense. This paper primarily explores the application of artificial intelligence technology in network cybersecurity defense.
Keywords: Artificial Intelligence; Cyberspace; Network Security Defense

随着全球化进程的不断加深，信息技术迅猛发展，国际形势急速变化，我国的网络空间安全面临着严峻挑战，网络空间安全问题已经严重影响国家安全。如何有效抵御外部网络攻击，如何快速发现内部网络安全隐患，已经成为当前网络安全技术发展过程中亟待解决的问题。从何处着手破局？合理运用人工智能技术可能是极为关键的一步。通过人工智能技术能模仿人类思维的技术特征，使得自主进行网络安全防御，自主进行系统维护等工作成为可能，人工智能技术的运用，对于推动网络防护技术的发展具有十分重要的意义。

一、人工智能技术

1.人工智能技术介绍

人工智能技术是当前信息科学的一个前沿技术，最近几年，人工智能技术成为了一个热门的研究方向，诸如ChatGPT等人工智能应用频繁地进入到我们的视野，给生产和生活带来质的变化。学术上来说，人工智能技术被划分为“强型”与“弱型”两类。“弱人工智能”指的是基于数理技术的机器学习算法，设计者需要预测出在实际使用中会遇到的多种情形，并利用电脑确定其可行性[1]，一旦超出了预设的范围，弱人工智能将无法应对。“强人工智能”有着更强的“思维能力”，它拥有像人类一样的思考能力，有一定的自主学习能力，即使面对超出预设程序范围的事情，也可以自主决策做出判断，并发出发出具体的操作指示。

2.在网络空间中运用人工智能技术的意义

网络空间的安全防御已经成为了一个不可忽视的工作，而做好安全防御，网络安全监控往往是其中最为关键的一环，及时“发现”危险是保障网络安全的基础。在如今信息爆炸、数据爆炸的时代，网络安全防御是为了提升网络系统的抗攻击能力，阻止虚假、有害信息在

网络空间传播，为缺乏网络安全防御能力的普通用户提供可靠的信息传输，确保数据安全。而随着信息技术的发展和普及，人们也渐渐意识到了网络防御效率和网络安全的重要性，并对其展开了更多的研究。尤其是当前，随着网络犯罪、网络攻击问题的日益严峻，为了保障使用者的信息安全，网络系统必须具有较高的应急反应能力和安全防御能力。将人工智能技术引入到网络空间安全防御领域，能够提高防御效率，有效减少信息系统遭受攻击而失效等事故，对提升信息系统的安全性，提升信息系统的整体性能有重要意义[2]。人工智能技术可以被运用到各类网络信息处理工作中，它不仅可以对未知的网络信息进行分析识别，还可以进行追踪和其他处理操作，从而保证网络系统的安全。

二、运用人工智能技术在网络空间进行安全防护的优越性

1.具有对不明确消息进行分析的能力

与其它类型的网络安全防御技术相比，人工智能技术可以高效地检测到未知的信息，并可以对模糊信息进行系统、全面、高效地处理，因此提升了整体安全防御效率和能力。在使用互联网的时候，使用者经常会受到一些不明病毒的攻击，如果不能准确地识别出这些病毒，就很难制定出有针对性的防治策略，无法防范病毒的攻击可能会给使用者带来了各种各样的损失。利用人工智能技术的模糊信息处理能力，可以对网络中的模糊信息展开一系列的、完整的识别，如果它存在着威胁特征，人工智能防御技术就可以在第一时间对它做出相应的反应，阻挡或截断其攻击行为，从而减轻所造成的危害，提高网络的安全程度[3]。

2.对非线性问题有较强的适应能力

目前国内网络有着很高的复杂度，网络中出现未知事件的几率较高，这就使得网内设备所面临的非线性影响大大增加。使用常规的安全防护技术，并不能对网络进行完全、有效的防护。如何能将人工智能技术有效地应用到网络空间的安全防御当中，可以在很大程度上增强计算机对非线性的处理和控制能力，进而可以对网络威胁展开有效的控制，防止设备受到网络上的各类攻击，从而进一步提升网络空间的安全防御能力，给用户提供更好的使用体验[4]。

3.具有良好的团队合作精神

伴随着信息技术的持续发展，信息技术基础设施的数目在不断地增多，网络的规模也在不断地增大，网络的结构也随之变得更加的复杂，这就对网络空间的安全防护工作提出了更高的要求。要提升整体网络的安全性，就必须加强各种系统间的高效连接，通过采用对应的分层管理方式，对各种攻击事件进行有效的控制，将其出现的几率保持在一个合理的区间。使用人工智能技术，可以强化不同的网络空间安全防御管理人员之间的合作，保证每个层级的安全管理者所采用的安全防御措施可以相互紧密地合作，从而逐渐地建立起一个完整的网络空间安全防御系统，为网络空间的安全提供一个更好的防护能力。

三、网络空间安全防御系统中人工智能技术的具体运用

1.人工神经网络技术

可信的神经网络通常是一系列简单的处理元所构成，具有很好的容错性和自主学习性，能够有效地进行分布式的数据存储。神经网络能适应多种特定的信息加工需求，并能达到知识自组织的目的。同时，神经网络的神经元运算相对独立，能够进行平行运算，且已有的软硬件均能够确保其运算效率。神经网络技术主要用于网络入侵检测，它能够发现并处理网络中存在的垃圾信息或恶意程序。将神经网络技术引入到网络监控的智能体决策算法中，能够明显地增强网络监控的有效性，并能避免监控过程中出现的许多错误现象。相比于常规的探测方法，神经网络技术在效率和准确度上有着显著的优势，甚至可以探测到新的蠕虫病毒。

2.智能防火墙技术

在网络安全防护中，最常见的一种防御设备就是防火墙，使用防火墙能够对网络中的安全隐患进行识别和控制，从而有效地保护“墙内”设备。一般来说，在传统的网络空间中，已经部署了各种各样的防火墙，但它们的部署使用并不能达到理想的防御效果，很难完全地、有效地抵抗安全风险。而人工智能防火墙技术则不一样，它具有显著的优点，可以对网络中的各类安全隐患问题进行统计和判断，高效地对潜在风险进行拦截，并将其解决，从而避免恶意攻击或可能出现的恶意攻击。与传统防火墙相比，智能防火墙技术对防御能力进行了改进和提升，它具有更为全面的功能，安全防护效果也更为明显。除此以外，它还可以对安全访问控制防御机制进行优化，从而保证网络的安全。

3.入侵检测技术

在网络空间的安全防护过程中，还必须要对入侵病毒或者其它的风险隐患展开监控，要清楚地认识到这些风险因子在进入到网络或者系统之后所造成的破坏力量，

在威胁出现之前就加以控制，以免给网络或者系统造成危害。尽管在传统的网络空间安全防御措施中，也包含了一些监控的方式和技术，但是这些方式都会产生一些缺陷或者是监控对象不明确的问题，为此，就必须运用人工智能技术来对这些问题进行改进，从而达到更可靠的监控和控制效果。使用人工智能的入侵检测技术，可以对所有的信息展开智能识别，找到其中是否存在着安全隐患，并利用有效的控制方法予以解决，从而确保网络空间的安全运行。目前，智能入侵检测技术已被大量应用在企业或行业组织的网络安全防御中，它可以有效地避免来自外界的多种侵入因子所造成的安全隐患。

4.垃圾邮件网络安全防御技术

在网络空间的安全防护中，运用人工智能技术也能够有效地防范垃圾信息。垃圾邮件给互联网造成了很多的麻烦和干扰，而且有些垃圾邮件还会将病毒或者其它的不良文件绑定到互联网上，如果没有能够及时地将它们处理掉，就有可能导致中毒。在这种情况下，如何对垃圾信息进行有效的识别与控制是非常关键的，必须要在网络安全防护中加以重视，而运用人工智能技术能够有效地解决垃圾信息问题。它能够实现对这些信息的完全拦截。垃圾邮件网络安全防御技术具有很高的应用价值。在互联网上，通过建立一套针对互联网上各种电子信息的防伪体系，从而为今后的垃圾邮件识别及拦截提供参考，使互联网上的电子信息不再被污染。

5.多智能体系统技术

多智能体系统是一类具有自主能力的分布式人工智能，它可以通过感知到周围的环境，并在响应中与周围的环境发生互动。目前，多智能体系统已经有了较为成熟的发展，因此它在网络空间的安全防护中的应用也日趋普遍。这一技术具有环境感知、规划的功能，在网络安全防护中，它主要被应用到对网络趋势的感知以及网络入侵检测等领域。目前，多智能体系统已经在各种网络空间安全演练中推广应用，比如DECIDE就是我国支持网络安全决策演习中的分布式环境。通过多智能体系统技术，我们可以实现对虚拟对手的模拟，进而实现和人类的真实性互动。agent平台JIAC以服务为核心，建立了一个网络安全仿真环境，在发生了网络入侵事件之后，可以完成对事件的评价，并找到相应的防护措施。agent技术的运用，能够有效地解决网络空间中存在的许多问题，进而提升网络空间的安全防护水平。

6.专家系统技术

作为一种发展比较早的人工智能技术，专家系统通常被用于构建知识库及推理机的工作中，它可以对一个领域中的知识展开推断，进而模仿人类专家的思维模式，对问题进行分析和解决，并给出专门的答案。但是，在进行专家系统推理的过程中，还需要建立一个比较完整的知识库，将其做为系统的操作依据。因为，人工智能专家系统只能在已有的知识中来实现其推理，因此，其推理行为不能超越已有知识的范围。目前，在网络空间安全防御中，专家系统的运用还有很大的发展余地，它是网络空间安全防御体系发展过程中的一个关键组成部分，它可以为网络空间安全防御的行动提供更为专门的知识支撑。通过专家系统，可以对入侵监控系统所检测到的信息展开推理，从而对网络系统在操作过程中，是否会出现安全隐患进行分析。最近几年，随着技术的发展，专家系统也得到了持续的升级，它能够将各种统计方法运用到对使用者进行分析，并构建出各个具有权限的使用者群体的行为描述模型，进而通过子系统对使用者的行为进行监测，对网络中的侵入行为进行辨识。

四、结束语

在信息化时代，网络空间的安全范围不断扩大。网络的安全性问题，不但关系到民众的日常生活，更关系到产业的发展与社会的安定。将人工智能技术引入到网络安全防御中已是大势所趋，是主动适应网络安全新形势、新要求的重要一步，是进一步提升网络空间安全性的关键。

参考文献：

[1]宋悦.人工智能技术在网络安全防御中的应用[J].科技风，2023（06）：65-67.

[2]郑汉军.人工智能技术在网络空间安全防御中的应用[J].网络安全技术与应用，2022（01）：100-101.

[3]于淏瑜.大数据时代人工智能技术在网络空间安全中的应用研究[J].无线互联科技，2021，18（24）：110-111.

[4]朱晨安.人工智能技术在网络空间安全防御中的应用分析[J].中国高新科技，2021（21）：149-150.