人工智能技术在网络空间安全防御中的应用

王 浩

北京结慧科技有限公司 北京市 100043

摘 要：怎样才可以从根本上解决好各种网络信息的有效形式产生的网络攻击，这想必是对我们所设立的网络安全系统的必然考验，现如今的人工智能技术仍然采用最传统的方案，因此效率并不是很高，随着时代的飞速发展，网络空间安全防御也渐渐的进入群众的眼中，并且也获得了很多收获。近些年的网络空间安全综合了大量的新方案取得实际化的效果，此篇文章适分析各个领域方案的应用措施，从而达到经济收益最大化，促进网络安全工程的发展。

关键词：人工智能；网络空间；网络防御；实践运用

Application of artificial intelligence technology in Cyberspace Security Defense

Hao Wang

Beijing Jiehui Technology Co., Ltd. Beijing 100043

Abstract: How can we fundamentally solve the network attacks caused by various effective forms of network information? This must be an inevitable test of the network security system we have set up. Today’ s artificial intelligence technology still adopts the most traditional scheme, so the efficiency is not very high. With the rapid development of the times, cyberspace security defense has gradually entered the eyes of the masses, and has also obtained a lot of gains. In recent years, a large number of new schemes have been integrated in Cyberspace Security to achieve practical results. This article is suitable for analyzing the application measures of schemes in various fields, so as to maximize economic benefits and promote the development of network security engineering.

Keywords: Artificial intelligence; Cyberspace; Network defense; Practical application

前言

现如今时代的不断进步，对于网络的探索也逐渐深奥了许多，每一个网络系统都是独立的，他们都有属于自身的特点。想要将网络安全整体提高的效率得到提高，那么这不单是对每一个工作人员的考验，还是对每一个工作人员对网络空间安全技术的考验。想要更好的提升网络安全防御技术就应该选择最优质的方案去提升网络安全水平，因此我们应该将人工智能和网络安全相结合，人工智能是近几年人们研究出的新型技术，这种技术不仅仅可以大幅度提升工作的效率，还可以提高准确度，我们必须想到一个两全其美的办法让人工智能技术在网络安全中得以体现。

1 网络空间安全防御相关概念

想要让整个网络空间安全工程中更好的融合人工智能，将整个工作更直观的展现在大众眼光中，那么就需要我们对整个工程的具体含义进行详细的阐述。

1.1 网络空间

网络原指用一个巨大的虚拟画面，把所有东西连接起来，也可以作为动词使用。在计算机领域中，网络就是用物理链路将各个孤立的工作站或主机相连在一起，组成数据链路，从而达到资源共享和通信的目的。

凡将地理位置不同，并具有独立功能的多个计算机系统通过通信设备和线路而连接起来，且以功能完善的网络软件 (网络协议、信息交换方式及网络操作系统等) 实现网络资源共享的系统，可称为计算机网络空间。

1.2 进攻性网络作战

所谓进攻性网络作战就是一种黑客行为，它通过破坏对方的计算机网络和系统，刺探机密信息达到自身的政治目的。现如今时代飞速发展，各国的相互联系也由网络而相联系，而现如今出现了一些破坏网络安全的系统，这种系统具有十分强大的侵略性，一旦设定好目标对象，那么第一时间就会让其系统瘫痪，这就是当代的一种战争形式。

1.3 网络防御

网络安全防御是一种网络安全技术，指致力于解决诸如如何有效进行介入控制，以及如何保证数据传输的安全性的技术手段，主要包括物理安全分析技术，网络结构安全分析技术，系统安全分析技术，管理安全分析技术，及其它的安全服务和安全机制策略。

1.4 网络态势感知

态势感知是一种基于环境的、动态、整体地洞悉安全风险的能力，是以安全大数据为基础，从全局视角提升对安全威胁的发现识别、理解分析、响应处置能力的一种方式，最终是为了更好的方便决策与行动。

2 我国对人工智能的探讨

从二十一世纪开始以来我们国家档案界的知识分子和处理档案管理几位学识渊博的教授们开始利用人工智能技术和网络安全相结合的技术去顶替人的大脑来思考问题，这样做可以最大程度的减少工作的难度和提升工作效率，如今国家在人工智能的探索主要涉及下类的几个层面 :

2.1 人工智能的不同看法

由于随着人工智能的开展和网络安全的结合给每一位学者们都带来了崭新的困难和问题。有的教授觉得应

该在人工智能的帮助下更进一步的提升网络安全的安全性能，为人民创造更有利的新价值 可是在现如今最根本的模式下想去转换成新的智能化的学识还是需要一定的时间。有一部分的教授觉得系统的，反复的，工作进展效率的下降会直接导致人工智能的进展效率变低，可是在影响下的同时人工智能的确可以把档案的总体化，自动探究，加强系统工作等进一步的去提升它的价值。

2.2 怎样开展人工智能和网络安全相结合

在人工智能通过网络安全的系统活动的选择和探究中，在国家的网络信息储存室的修建过程中把人工智能技术利用在档案的总结，档案自动归类，档案危险警示，档案建立系统的工作中产生的效果很成功。其他的教授觉得采用新型人工智能手段去把网络安全管理系统变得更加完善，选择新的接入途径，进行储存网络信息管理档案的应用和把每一个档案进行重新排序，从而进一步的把人们的各类要求逐个完成。怎样让自己对人工智能有个正确的认知是我们现如今存在的大问题，一部分教授觉得把帮助人们学习和思考方面的效果放大，这样不仅仅有利于人们的科技进步，还可以提升学习的效率和利用率，在当今社会时代的发展速度下要利用最基础的档案将总体全部改变，包括档案的检测，档案的利用和每一份档案应具有的作用都应该发生新的改变。从整体上观察，无论是世界上任何一个国家在对人工智能的理解和把它应用在各个领域上的各有各的办法。国外主要把人工智能技术放在主要的工作上去观察运用在现实从而产生的效果，在档案室的文档里网络安全信息储存平台所造成的影响显而易见。在我国主要通过把人工智能利用在档案管理活动上，利用它所带来的一定的创新性，还有不同的可能性进行深层分析，目前我国这项技术还处于在最基础的时期，可是我们每一个人心里面都清楚想要以最快速度把传统的管理模式改进成一个新型模式是一个长久的过程，需要我们一点一点的去结合人工智能去进行改进，更替，这样做才可以更加进行久远的开展工作。

2.3 人工智能的弊端

根本上来说人工智能的存在也是为了促进人们的生活，所谓的理论知识也就是片面的，我们应该应用于实际，不单单是在技术上，还应该在总体的知识储备上开展新的学习。这样的相辅相成就会解决一大部分难题，我们就从人工智能和网络安全相结合来说，这个技术的首要方向就是应该确定自己的目标，认清什么是重点的，什么是次要的。利用专业技术是我们实现人工智能和网络安全相融合的前提，如果强行的融合和探究，那么所造成的结果只会和预期的效果相反。在我们把我们所学习的技术应用到实际中，那么完成我们的任务便是我们的根本目的，面对现如今时代进步的飞快，市场需求种类复杂，我们需要的就是我们每一位技术人员的潜心研究和努力。我们在利用根本的 PS 技术和分析图像的技术上可以对我们的文档进行新的总结和区分，这样大大的提升了运行效率也，让这一过程变得更加简单化，利用了选取信息的操作让整体看起来更加简单化，这样也就优化了整个检测速度。现如今，人工智能技术在部分地区无法开展是我们所面临的重点问题。在研究中我们发现，这项技术的成不成功和上升空间并不是主要特点，尤其现如今该专业技术的专业知识的学生的缺少和有些人们滥竽充数造成不同的迷惑性。我们的人工智能技术需要的是那些在社会上具有较大影响力的企业做支撑，并且只有资质潜力的教授级别的人物才可以把这项技术发挥的淋漓尽致。所以需要的是我们的专业人员应该具有谦虚，耐心的性格去教育那些晚辈，应该取长补短合理的开展这项工作，努力的培养新生代，不让这项技术流失。多方向共同协助，团结起来才是这个专业领域的出发点。现如今在我国的各个地区网络安全管理中心都和最具有专业性的人工智能技术的组织成立的新的平台，这样对我们共同探索学识，把两个专业领域相融合提供了更大的帮助 [1]。

3 网络安全的加密技术

如今，网络已经普及到了千家万户，对于计算机安全也得到了高度重视，网络数据加密技术就是其中之一，由于加密算法涉及广泛，在强度方面也大不相同，现有的两种加密系统分为共享钥匙加密（对称钥匙加密）和非共享加密两种形式。

3.1 对称密钥加密

共享钥匙加密可以理解为私人共享要是加密，利用相同的钥匙进行对对称加密的解密。为此，对于数据和信息的收集者和发送者而言都应有一把同样的钥匙，在私人共享加密钥匙的系统中，相对于有一定权威的加密算法，是一种使用密钥匙的快算法（DES）。此加密算法是由国际商业机器公司（IBM）开发出来的，利用 64 比特钥匙和相应数据针对算法进行解密与加密。对于 DES(一种使用密码钥匙的快速算法) 进行多样化的操作模式，平时普遍使用的两种操作模式：分组密码的最基本操作模式简称（ECB）和 加拿大广播网络（CBC）：电子密码本模型又可称为电子密码本型其原理是：将明文按分组密码的分组规模分成若干个分组，并将明文分组按照一定的顺序编号，每一个明文分组直接作为分组密码算法（ECB）的输入。对于相同种的密码钥匙而言，在其控制下加密的到相应的密文组。所以很容易遭到“在破译密码时，逐一尝试用户自定义词典中的可能密码（单词或短语）的攻击方式简称字典攻击。出现解密错误或时其他问题时单纯影响目前的加密算法，并不能产生大范围的影响。对于西班牙（ES）语而言，它在加密技术的发展中起到了重要的作用 [2]。现如今，对于网络的安全更加严格，各加密技术专业人员对于安全性也进行了严格的分析，在细节方面缺少一定细致，随着一种使用密钥的快速算法开发出来，推动了快速算法的发展其功能在算法方面更加全面。

3.2 信息安全

随着网络行业的逐步发展，信息安全逐步进入大众视野，对于这方面的研究也在不断进行，对于信息安全而言从根本上讲是对重要的数据进行防护和加密，保护重要资料和数据不被泄露。从计算机问世到如今，互联网一直处于飞速发展阶段，如今计算机从局域网发展到可以连接千家万户的网络，对于计算机的使用也逐步大众化，信息安全技术是当今信息化时代的重要保障，随着网络遍布全球各地，这使得对于网络信息安全的概念

逐步加深，对于数据安全来讲加密性和整合程度，完整性都是数据安全的相关概念，而对于使用者来说身份识别，各项授权和访问权限隐私问题等等。

4 发展趋势与展望

4.1 网络安全和人工智能的发展前景

现如今网络发展速度在日益变快，各种维持网络安全的防火墙也在逐渐更替。因此想要更好的维护整个网络的安全进行，就需要我们每一个工作人员的共同努力，提升整个工程的运行速度和工程开展技术，这样才可以才众多网络发达的领域里崭露头角。现阶段部分网络安全管理技术已经和人工智能相结合，呈现的效果处于两极分化的状态，部分的人工智能在工作的时候，时常会出现卡顿，不按照系统指令的问题，这些问题会大大降低整个工作的完成度和工作效率，这也就让人工智能在人们心中地位大打折扣 [3]。

人工智能的进步速度为文件整治的方向指明了新的道路。由于时代的发展人工智能在当今社会的利用也越来越广泛了起来，每一位员工利用自身对网络安全的技术还是研究整体的管理方面的新方案都可以让自身的技能熟能生巧。在档案管理的层面里选择采用人工智能来让该工作有新的进步和推进时，需要时刻关注着应该采用最有利的方法，做到取其精华，去其糟粕，这样才可以最快捷的利用人工智能所带来的方便。

现如今人工智能在当今社会发展的速度已经达到了家喻户晓的程度，而随着人工智能发展的推进下，也成为了网络安全发展和进步的新问题，我们应该积极的去发掘新的解决方案去主动的找寻新的方向去解决问题 [4]。此篇文章利用各个地区网络安全档案管理和人工智能的进展速度，来辨析人工智能对网络安全的影响，最后去选择新的方案去解决问题和采用新办法去开展新的创新。

4.2 网络安全和人工智能的展望和作用

随着人工智能和网络安全档案管理技术的相结合也会逐渐的推进网络安全的更替进步。随着人工智能在人们的日常生活中逐渐的被应用的越来越多，可是本应该适应人工智能的安全系统的确还是存在一种最根本的失控状态，不能准确的锁定，细致的引进当今工程的进展。最基础的信息的成分需要在人工智能的影响下重新进行总结，基础的信息定义怎样改变才可以和人工智能彻底的融合，系统的档案区分办法还有总体定义怎样才可以在现如今的社会上发展各方面相互促进融合全是现在应该主动去面对的困难。现如今人工智能在现实生活的应用需要新的改变和进步。在利用我们现在手里面有的资料来看，人工智能在不知不觉的时候已经充斥着我们的生活了，无论是家庭还是社会都已经离不开人工智能的应用了，所以我们我们也可以猜测，在以后的日子里面人工智能所给我们带来的改变一定会让我们的网络安全受到一定的影响 [5]。要是网络安全管理部门可以重点认识到人工智能给人们带来的优劣，我们就可以通过该方法引发的心理作用让每一个人都参与到人工智能建设中来。人工智能在我们日常工作中无时无刻的都在帮助我们去提升自己的能力。在今后的日子里是人工智能发展的关键时机，因此网络安全也受到了人工智能影响，在受到影响的同时我们的技术人员就应该随机应变的去学习一些专业知识，还需要具有独特的眼光和清晰的对这个技术的认知。所以在现如今社会中我们的每一个技术人员都应该思考自己在自己所在的领域是否具有一席之地，我们应该怎样利用自己的专业知识去促进人工智能的发展和进步，我们与什么样的技术组织携手才可以更有利的帮助自己实力得到加强，这样做才可以防止自己随着时代的更替发展而导致自身的步伐跟不上从而被社会淘汰。

5 结束语

想要从根本上让整个网络领域和人工智能充分融合，那么就需要我们的工作人员具有很强的专业知识能力，网络领域的变化是飞快的，死板的知识并不能让整个工作做的更好，而需要的是灵活多变的探究，这样才可以让整个工作做到经济收益最大化。即使人工智能在人们的眼中呼声并不是很大，但是我们可以承认的是，通过人工智能和网络安全的结合已经让我们得到了更加便利的生活，因此我们应该竭力的去探究新的方案，取其精华去其糟粕，使人工智能和网络安全的防御系统更好的结合。

参考文献：

[1] 张云春。朱艳萍、姚绍文、林英。易超 . 面向人工智能的网络空间安全教学改革 [J]. 计算机教育，2020（10）：125-129.

[2] 李志勇 . 大数据时代人工智能在计算机网络技术中的应用研究 [J]. 网络安全技术与应用、2020（45）：103- 104.

[3] 张路、王威扬 . 人工智能技术在网络空间安全防御中的运用分析 [J]. 天津科技、2020（47）：61-62.

[4] 任小成 . 基于大数据时代人工智能在计算机网络技术中的应用分析 [J]. 中国战略新兴产业 ,2018(42)：201-204.

[5] 柏苗，万丽 . 基于大数据时代探索人工智能在计算机网络安全技术中的应用 [J]. 中国新通信 ,2018(36)：11-31.

作者简介：王浩 1989 年 10 月 02 日，男，汉，河北，本科 开发工程师，现主要从事的工作或研究的方向：计算机视觉与隐私计算，