

# 大数据与人工智能时代背景下的网络安全课程体系研究

董理君, 刘超, 张锋, 姚宏

(中国地质大学(武汉)计算机学院, 湖北 武汉 430078)

**摘要:** 大数据和人工智能技术的发展,对传统的网络安全教学带来了冲击。一方面,很多网络攻击技术本身就利用了大数据和人工智能原理;另一方面,人工智能与大数据本身也存在安全问题。然而,当前的网络安全课程体系尚未将这些内容整合成一个有机整体。通过分析当前网络安全课程授课在宏观、微观和过程控制上的部分缺陷,提出融合大数据与人工智能思想的网络安全课程体系,包括基于人工智能与大数据的“全网安全”课程构建、人工智能与大数据安全知识融合、面向新时期的网络安全知识图谱搭建共3个方面,以建立面向大数据与人工智能背景的网络安全课程体系,弥补当前网络安全教学中缺失的相关内容,改进教学效果。通过人工智能和大数据角度对网络安全教学提供有参考价值的新方法,力求促进信息安全、人工智能、大数据等相关专业知识的融合。

**关键词:** 大数据;人工智能;网络安全

**DOI:** 10.11907/rjdk.231545

**中图分类号:** G642

**文献标识码:** A

**开放科学(资源服务)标识码(OSID):**

**文章编号:** 1672-7800(2024)008-0037-06



## Exploration of Network Security Curriculum System in the Context of Big Data and Artificial Intelligence Era

DONG Lijun, LIU Chao, ZHANG Feng, YAO Hong

(School of Computer Science, China University of Geosciences, Wuhan 430078, China)

**Abstract:** The development of big data and artificial intelligence techniques has brought an impact on traditional network security teaching. On the one hand, many cyber-attacks themselves use the principles of big data and artificial intelligence. On the other hand, artificial intelligence and big data themselves also have security problems. However, the current network security curriculum system has not yet integrated these contents into an organic whole. This paper analyzes some deficiencies in the macro, micro and process control of the current network security course teaching, and proposes a network security course system that integrates big data and artificial intelligence. By through the "full network security" based on artificial intelligence and big data course construction, the knowledge integration of artificial intelligence & big data security, and the construction of network security knowledge graphs, this study establishes a network security course system for big data and artificial intelligence backgrounds, and makes up for the content in the current network security teaching, to improve the teaching effect. This paper provides a new method of the network security teaching from the perspective of artificial intelligence and big data, and strives to promote the integration of information security, artificial intelligence, and big data-related professional knowledge.

**Key Words:** big data; artificial intelligence; network security

### 0 引言

人工智能、大数据对传统的网络安全课程知识结构带

来了巨大冲击<sup>[1]</sup>。大数据和人工智能技术在给人们的生活、出行、工作和学习带来极大便利的同时,也在数据隐私保护、网络攻击与防御等方面带来了新的网络安全隐患。一方面,人工智能和大数据技术使得网络安全攻击手段更

收稿日期:2023-05-25

扫描二维码阅读全文:

基金项目:中国地质大学(武汉)教学研究项目(2019A43,2019A41)

**作者简介:** 董理君(1978-),男,博士,CCF会员,中国地质大学(武汉)计算机学院副教授,研究方向为网络安全与智能计算;刘超(1978-),男,中国地质大学(武汉)计算机学院副教授,研究方向为大数据与系统安全;张锋(1974-),男,博士,中国地质大学(武汉)计算机学院副教授,研究方向为系统安全与大数据分析;姚宏(1976-),男,博士,中国地质大学(武汉)计算机学院教授,研究方向为网络安全与知识工程。



加复杂和隐蔽,如APT攻击(可持续性威胁)本身自带智能特征,可以通过长期潜伏,结合社会工程学原理,用数据挖掘的方式动态发现用户行为漏洞,从而进行“个性化”攻击<sup>[2]</sup>。另一方面,人工智能和大数据技术也为网络安全提供了新的解决方案,如基于深度学习的入侵检测、网络攻击预测<sup>[3]</sup>、基于大数据分析的信息内容安全判定<sup>[4]</sup>等。然而,传统的网络安全课程尚未完全将以上内容结合成一个有机整体<sup>[5]</sup>。

对于人工智能与大数据背景下的网络安全知识传授、学习,在课程体系建设方面尚有一些亟待解决的问题。首先,需要解决基于人工智能与大数据的多个网络安全课程共性挖掘问题<sup>[6-8]</sup>。要实现符合国家网络安全战略下专业发展需求的“全网安全”课程体系,必须挖掘网络安全、恶意代码攻防技术、操作系统安全等传统经典课程中基于人工智能与大数据的共性知识结构,以求与网络安全态势感知的态势提取、态势理解、态势预测相呼应,而当前的课程体系尚缺乏这一融合机制<sup>[8-10]</sup>。其次,要解决多种知识融合的网络安全教学过程控制问题。人工智能与大数据中的许多技术本身就具有知识组织、知识学习的特点,这与网络安全教学知识的传授可以很好地结合<sup>[11-13]</sup>,而当前的网络安全教学尚未足够重视这一特点。

本文通过分析当前形势下网络安全教学所存在的技术缺陷,提出融合大数据与人工智能思想的网络安全课程体系(Network Security Curriculum Integrating Big Data and Artificial Intelligence Ideas)——BANS课程体系,力图基于人工智能与大数据技术特点,涵盖传统的网络安全防护<sup>[14]</sup>、恶意代码攻防技术<sup>[15]</sup>、操作系统安全<sup>[16]</sup>等课程内容,构建一套切实可行的网络课程设置方案。

## 1 当前网络安全教学中存在的技术缺陷

在大数据和人工智能时代背景下,之所以存在多个网络安全课程的共性挖掘问题和多种知识融合的教学过程控制问题,主要因为当前的课程体系存在以下缺陷:

(1)从宏观体系来看,当前课程构架偏重于传统的网络安全防护技术,缺乏对恶意代码攻防技术与操作系统安全技术在人工智能和大数据环境下的统一整合,缺乏一条能够将网络防护、恶意代码攻防、操作系统安全技术进行有机关联,并与人工智能、大数据技术紧密耦合的知识结构,即在总体上缺乏一个“全网安全态势感知”的课程体系。

(2)从微观内容来看,课程内容分布存在缺失的问题,难以适应人工智能、大数据带来的安全挑战。人工智能与大数据技术在为网络安全保障提供更先进技术的同时,也为攻击者提供了更加智能的入侵手段,且人工智能、大数据技术本身也存在安全缺陷,当前的课程体系缺乏对这一方面的有力体现。

(3)当前的授课方式仍属于基于教材章节进行知识组织的线性过程,而没有认识到网络安全知识的学习是一个与人工智能、大数据紧耦合的非线性过程。在整个教学过程中,缺乏能对整体知识内容进行梳理、融合的方法和工具,教学效果不佳。其实质是授课过程中缺乏一个网络安全知识图谱,忽略了网络安全教学本身也是一个知识工程实施过程<sup>[12-13]</sup>。

## 2 BANS课程体系构建指导原则

BANS课程体系构建的总体指导原则如下:

(1)课程体系应涵盖网络安全防护、恶意代码攻防与操作系统安全等知识内容,形成基于人工智能与大数据的“全网安全”课程架构,符合国家的“全天候全方位感知网络安全态势”整体战略。

(2)设置并实施面向网络安全的人工智能安全与大数据安全知识内容,弥补当前网络安全课程中的内容缺失,以信息安全法律法规为导向,在课程体系中设置必要的人工智能与大数据知识环节,帮助学生树立正确的网络安全观<sup>[17]</sup>。

(3)以课程实践的形式带动学生搭建一套网络安全知识图谱,并形成一套相对完整的网络安全数据集,使学生对网络安全体系全貌有一个总体认识,并通过图谱搭建过程提高自身的动手实践能力,尤其是运用人工智能与大数据基本技术的能力。

## 3 BANS课程体系设计方案

如图1所示,BANS课程体系在总体框架上由3门传统的网络安全课程(侧重网络架构安全的网络安全防护、侧重网络行为安全的恶意代码攻防,侧重网络节点安全的操作系统安全)知识单元共同构成,探索人工智能与大数据环境下的“全网安全”课程模式、知识内容和总体网络安全课程知识图谱。

### 3.1 人工智能与大数据环境下的“全网安全”课程内容设计

在传统的课程设置中,网络安全防护、恶意代码攻防与操作系统安全3方面内容是作为相对独立的知识单元实现的。该方式虽然具有知识量大、技术内容丰富的优势,但缺乏有机整合,不能体现“全网安全”的知识需求。究其原因是传统的网络安全课程重在传授安全防护技术本身的原理,而缺乏将3种安全技术知识有效关联起来的知识框架。在人工智能与大数据形势下,这一问题尤为突出:任何安全技术都不可能孤立存在,只有相互融合才能实现全网模式的智能安全 and 数据安全。因此,应将安全防护、恶意代码攻防、操作系统安全进行统一规划,形成一个有机的“全网安全”课程整体。

本文采用的设计方案是:以人工智能和大数据技术为

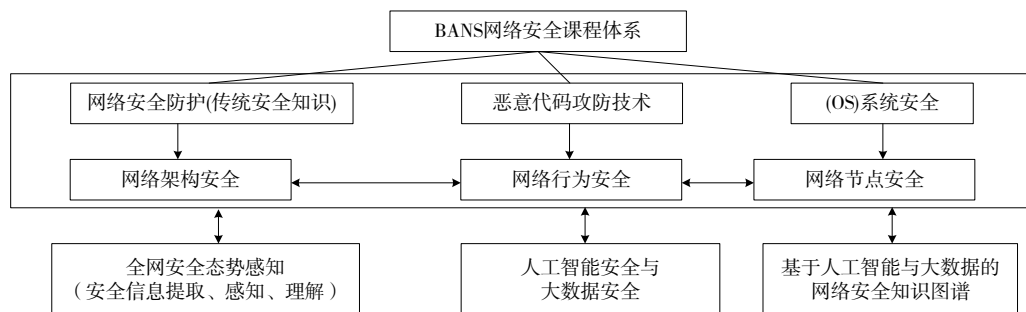


Fig. 1 BANS curriculum framework

图1 BANS课程体系框架

纽带,以“全网安全态势感知”为载体,以经典网络安全技术为基础,挖掘其与恶意代码攻防、操作系统安全之间的共性,形成有机的、具有人工智能与大数据特色的“全网安全”综合课程体系。以“全网安全态势感知”中的态势提取、态势理解、态势预测等智能数据分析技术为线索,以人工智能和大数据在信息安全中的应用为场景,形成一个贯穿网络安全课程体系的内容链条。

### 3.2 网络空间中人工智能安全与大数据安全知识内容设计

传统的网络安全课程中不包含人工智能安全与大数据安全,一方面是因为人工智能与大数据安全问题近几年才受到重视,传统课程尚未纳入;另一方面是人工智能与大数据本身已发展成为各自独立的专业体系,包含丰富的内容,其安全问题并不是传统网络安全课程能够完全覆盖的。然而,在当前的形势下,网络空间中无时无刻不包含着人工智能与大数据相关因素,网络安全的知识内容无法回避人工智能安全与大数据安全问题。

因此,BANS采用的设计方案是:结合网络安全课程自身知识内容的特点,设置面向网络空间安全的人工智能安全与大数据安全相关知识内容:以信息安全法律法规为导向,以网络防护、恶意代码攻防、操作系统安全中的核心技术为示例,在课程体系中设置必要的知识环节,涵盖人工智能安全与大数据安全技术。

### 3.3 基于人工智能与大数据视角的网络安全课程知识图谱设计

目前网络安全课程教学主要采用课堂讲解、课下实验的线性方式。该方式对于非信息安全专业的网络安全通识课程而言基本适合,但对于人工智能与大数据形势下的信息安全专业教学尚不够完善。首先,按照人工智能的定义,学习的过程本身是一个智能化的知识采集过程;其次,网络安全的知识点丰富多样,本身具有一定的大数据特性;最后,这些知识与特性实际上作为一个整体构成了一个网络安全知识图谱。而按照人工智能的思想,人脑的思维本身就属于“图谱思维”。换言之,网络安全的知识掌握本身就是一个在教学过程中搭建知识图谱的过程。因此,不仅要从网络安全课程的角度看待人工智能与大数据,而且需要从人工智能与大数据角度看待网络安全教学过程的高层次思想。实施这一教学目标的关键在于构建基于

人工智能与大数据视角的网络安全课程知识图谱。

本文采用的设计方案是:以3门经典网络空间安全课程(网络安全、恶意代码攻防与操作系统安全)的具体知识点为对象,实时跟进网络安全态势感知与知识工程的知识体系变化;以人工智能和大数据技术为工具,以课程内的小型工程立项为载体,引导学生在学习过程中逐步建立网络安全知识图谱。在网络安全课程知识图谱构建的整个过程中,采用递归反馈式教学方式:网络安全知识图谱构建过程既是学生实践锻炼的过程,又为后续教学提供了有价值的知识库,从而形成良性循环。

## 4 BANS课程体系内容

BANS课程体系内容如图2所示。

全网安全态势感知部分按照态势提取、理解、预测设置如下课程内容:①基于传统网络安全课程中的安全审计技术(安全协议日志分析、防火墙日志分析),引入人工智能和大数据中的数据采集技术,形成态势提取部分知识单元;②基于人工智能和大数据的数据分析技术,设置黑客攻击行为理解、恶意代码行为理解知识内容,并利用机器学习技术进行串联,形成态势理解部分知识单元;③将网络安全、操作系统安全中的入侵防范、安全控制、行为预测等内容利用智能决策技术和大数据挖掘技术进行串联,形成态势预测部分知识单元。

人工智能安全与大数据安全部分设置如下课程内容:①依据新《中华人民共和国网络安全法》,讲述为维护网络空间主权和国家安全、社会公共利益,保护公民合法权益的一系列法律保障措施,使学生树立正确的网络安全观;②以网络安全和恶意代码攻防技术中的入侵检测、恶意代码分析为例,解读人工智能与大数据在网络攻击中的风险原理,并依据信息安全法律法规提供总体的解决方案和防范措施,使学生了解并掌握人工智能与大数据安全在网络传输及网络行为安全方面的基础知识;③以系统安全中的安全控制为例,解读反向数据挖掘带来的隐私泄露和防护措施失效问题,从“全网安全态势感知”的角度给予防范措施,使学生掌握人工智能与大数据安全在网络节点安全方面的基础知识。

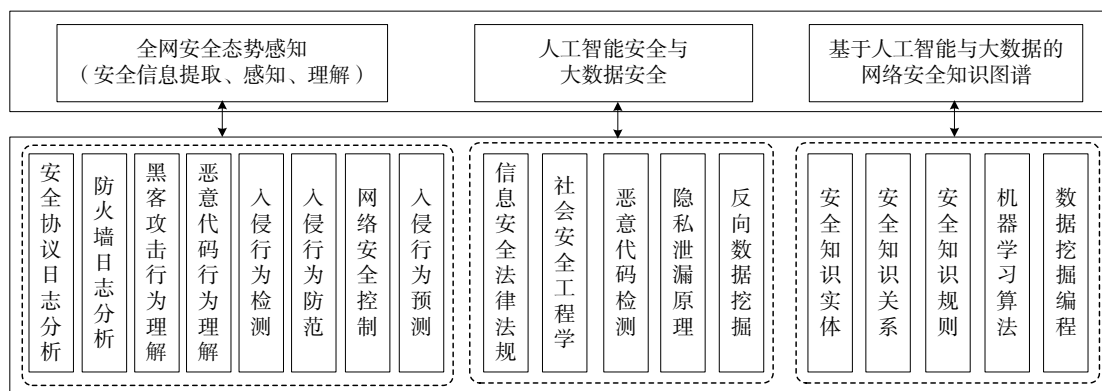


Fig. 2 Content of the BANS curriculum system

图2 BANS课程体系内容

基于人工智能与大数据的网络安全知识图谱部分设置如下课程内容:①在讲解网络安全、恶意代码攻防技术与操作系统安全课程内容的同时,实时整理知识点内容,并结合公开发布的《网络安全百科全书》《信息安全知识词典》等开源数据集,按照从易到难、由少到多的方式构建网络安全知识数据集;采用现有的人工智能和大数据技术工具包,引导学生通过实验的方式逐步完善数据集;②采用多种实现技术(如网络爬虫技术、文档解析技术,并结合精准的人工标注技术),从数据集中抽取知识实体、关系、规则,并以此为载体,促进学生在实践过程中掌握Python编程、机器学习算法等在网络安全图谱构建中的应用;③为将知识图谱构建与教师的教学、学生的学习活动紧密结合在一起,在网络安全课程体系内以实验课和课下作业的形式,结合学生兴趣成立若干个工程小组,分配不同任务,按照虚拟工程项目的方式,使学生深入理解人工智能与大数据背景下的网络安全知识构成。

## 5 教学实践及成果

课程组将BANS课程体系运用到实际教学中,本节介绍两个典型的BANS课程实践案例,并简要概述BANS课程效果。

### 5.1 小型案例:基于智能优化组合的动态访问控制模拟实验

该教学案例为BANS课程体系中的实践课程《网络与系统安全实验》的实验内容:以网络安全为背景,要求以数学建模的形式,利用人工智能和大数据相关技术进行求解。

案例背景:访问控制列表(Access Control List, ACL)实际上是网络空间中的行为准则。将ACL简化为一个二分图 $G=\{U, P, E\}$ ,其中 $U$ 可视为用户集合, $P$ 可视为权限集合,所有规则只能存在于 $U$ 和 $P$ 之间,构成边集 $E$ 。在传统的机制(如防火墙)中,判断某一行为是否符合规则是通过遍历ACL列表逐一进行的,即从头到尾逐个对比已知的“用户,权限”事实与ACL中存放的“用户,权限”,分析是否合法。

问题提出:在开放式的大数据环境下,传统的遍历模式会产生过重的计算负担,且无法根据已有知识预估新行为的安全性。

实践要求:利用机器学习和数据挖掘技术,把开放式环境下大规模ACL中的所有用户、权限都转换为向量,利用向量计算实现高效的访问控制。课程提供一个规模达到18万个具有“用户—权限”规则模式的防火墙数据集。

案例综述:实验以网络安全访问控制为背景,力求解决开放式大数据环境下的动态访问控制问题;采用表示学习的思想,利用机器学习和数据挖掘技术,以智能优化求解的方式提供解决方案。该实验综合了网络安全、机器学习、大数据分析等技术内容,有效体现了BANS课程体系中的多维度网络安全知识融合思想。

### 5.2 综合案例:基于百科词典的网络安全知识图谱构建实验

该教学案例为BANS课程体系中的一个亮点:既不作为单独的实验课内容,又不作为单独的课堂作业,而是以课外扩展形式开展的一项综合实践活动。因此,本案例按照课题背景、数据准备、技术方案、图谱展示等模块进行组织,模拟一个工程化的项目过程。

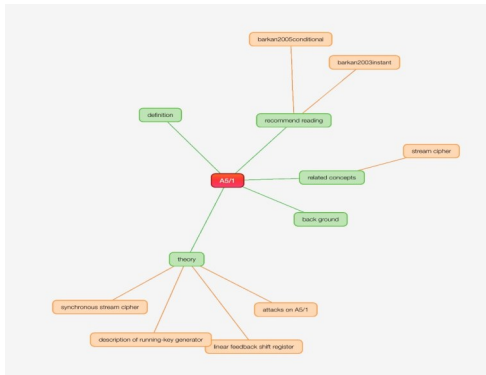
案例背景:根据前述内容可知,在BANS课程体系中,网络安全知识不仅包括经典的网络与系统安全技术,而且包括社会安全、法律法规等安全管理内容,且不同知识点之间存在着大量关系,从而构成了一个天然的语义网络——面向网络安全知识图谱。网络安全知识图谱打破了传统基于线性模式的网络安全知识组织方式,转变成以多维的关联模式进行呈现,更有利于学生全方位地掌握网络安全知识。

数据准备:本案例中采用的用于构建网络安全知识图谱的数据实例为信息安全经典著作《Encyclopedia of Cryptography and Security(2nd edition)》,该书是有关密码学及其网络安全应用的百科全书,由460篇文章组成,包括大量密码学与网络安全的专有名词、表格、社会应用及其对应的关联关系。

技术方案:从数据源中抽取用于构建网络安全知识

图谱的实体和关系。实体抽取内容包括:基于专有名词的实体抽取、基于图片描述的实体抽取、基于公式信息的实体抽取、基于表格信息的实体抽取。对于关系抽取,由于百科全书中每一章都包含不同副标题及超链接,全书的网页版有 LaTeX 源码可以访问,所以可根据超链接和 LaTeX 源码,运用 Python 爬虫技术、机器学习算法等进行关系提取,根据实体、关系即可构建知识图谱。

图谱展示:将构建的知识图谱用免费的图数据库工具 Neo4j 进行存储,图 3 为学生在完成图谱时的两个截图,以上信息可以基于数据库的查询语句进行查询。



(a) Partial display of the graph (entities and relationships of the A51 algorithm)  
(a) 图谱局部展示(A51算法的实体和关系)



(b) Global display of the atlas  
(b) 图谱全局展示

Fig. 3 BANS network security knowledge graph example display  
图 3 BANS 网络安全知识图谱实例展示

案例综述:该案例通过知识图谱构建这一实践途径,以可视化技术以及相关的属性描述构建不同实体之间的结构关系与发展进程。使用知识图谱组织的网络安全知识结构清晰,一方面使学生了解、掌握对应的人工智能和大数据技术知识,另一方面帮助学生更有效地梳理网络安全知识要点,同时有利于教师对自身知识内容和结构的不断优化。

5.3 课程教学效果

实践结果表明,BANS 课程体系及其教学方法在中国地质大学(武汉)计算机学院信息安全专业、智能科学与技术专业的本科生授课中取得了良好的教学效果。该课程

体系前期的组成课程《网络安全》、《操作系统原理及安全》及其对应的实验课程《网络安全实验》、《操作系统原理及安全课程设计》,以及 BANS 课程体系正式完成后的整合课程《网络与系统安全》、《网络与系统安全实验》和与之对应的融合机器学习与大数据分析在网络安全中应用的《数学建模》课程,连续 5 年在教学质量评价中得到优秀。具体评教成绩如表 1 所示。

Table 1 Teaching quality evaluation scores for five consecutive years  
表 1 连续 5 年教学质量评价得分

| 年份   | 课程            | 教学质量评价得分 |
|------|---------------|----------|
| 2018 | 网络安全          | 92.87    |
|      | 网络安全实验        | 92.37    |
|      | 操作系统原理及安全     | 92.94    |
|      | 操作系统原理及安全课程设计 | 90.06    |
| 2019 | 网络安全          | 92.84    |
|      | 网络安全实验        | 92.67    |
|      | 操作系统原理及安全     | 92.89    |
|      | 操作系统原理及安全课程设计 | 92.93    |
| 2020 | 网络安全          | 93.18    |
|      | 网络安全实验        | 93.29    |
|      | 操作系统原理及安全     | 93.48    |
|      | 操作系统原理及安全课程设计 | 93.10    |
| 2021 | 网络与系统安全       | 93.18    |
|      | 网络与系统安全实验     | 92.61    |
|      | 数学建模          | 93.40    |
| 2022 | 网络与系统安全       | 93.46    |
|      | 网络与系统安全实验     | 93.17    |
|      | 数学建模          | 93.50    |

此外,教学团队还获得以下教学成果:《计算机病毒实验教程》获得湖北省网络空间安全优秀教材奖(2021 年);ACM 国际大学生程序设计竞赛金奖、银奖各 1 次;全国软件和信息技术专业人才大赛全国总决赛程序设计一等奖 1 次;校级优秀本科毕业论文指导教师、优秀班主任等荣誉称号。所取得的成绩都与 BANS 课程实践教学密不可分,BANS 课程体系面向新时期下网络安全教学的需求,围绕培养学生动手能力和建立清晰的知识结构为中心,有效提高了教学质量。

6 结语

BANS 课程体系将传统的网络安全课程建设与当前迅速发展的人工智能及大数据技术联系起来,构建人工智能与大数据形势下的网络安全课程体系。BANS 的创新之处在于:①以人工智能和大数据技术为纽带,将传统的网络安全防护、恶意代码攻防和操作系统安全课程整合到“全网安全态势感知”的知识框架中;②从知识工程的角度审视网络安全课程教授过程,率先提出以知识图谱的形式刻画网络安全课程体系的知识全貌。

对 BANS 课程体系建设的研究和实践有利于构建具有“全网安全态势感知”特性的知识体系,这实际上与习近平总书记“4.19 讲话”及《中华人民共和国网络安全法》中所

强调的“全天候全方位感知网络安全态势”整体战略一致;有利于学生直观、深刻地理解网络安全课程体系全貌,并帮助其树立正确的网络安全观。此外,我国高等院校逐渐设立了网络空间安全、人工智能和大数据专业,三者的理论技术互相交叉融合已成为大趋势,探索BANS课程体系的构建将有助于解决这些新兴专业之间的知识融合问题。

#### 参考文献:

- [1] ZHAO Z W. Discussion on network and information security in big data era [J]. Computer Science and Artificial Intelligence, 2022(1):29-31.  
赵占旺. 大数据时代网络与信息安全探讨[J]. 计算机科学与人工智能, 2022(1):29-31.
- [2] FU Y, LI H C, WU X P, et al. Detecting APT attacks: a survey from the perspective of big data analysis [J]. Journal on Communications, 2015, 36(11): 1-14.  
付钰, 李洪成, 吴晓平, 等. 基于大数据分析的 APT 攻击检测研究综述[J]. 通信学报, 2015, 36(11): 1-14.
- [3] LI J Y, ZHAO B, LI X, et al. Network traffic anomaly prediction method based on deep learning [J]. Computer Engineering and Applications, 2020, 56(6): 39-50.  
黎佳玥, 赵波, 李想, 等. 基于深度学习的网络流量异常预测方法[J]. 计算机工程与应用, 2020, 56(6): 39-50.
- [4] HASAN M K, ALKHALIFAH A, ISLAM S, et al. Blockchain technology on smart grid, energy trading, and big data: security issues, challenges, and recommendations [J]. Wireless Communications and Mobile Computing, 2022(9):1-26.
- [5] LUO M, ZOU J L, WANG R N, et al. Multi-level teaching reform of network security course [J]. Computer Education, 2022(1):102-105.  
罗敏, 邹菁琳, 王若男, 等. 多层次的网络安全课程教学改革[J]. 计算机教育, 2022(1):102-105.
- [6] YUAN C M, SUN N, YANG Q Y. Exploration on the course construction of cyberspace security combined with artificial intelligence technology [J]. Advances in Social Sciences, 2022, 11(9):3926-3932.  
苑春苗, 孙娜, 杨清永. 结合人工智能技术的网络空间安全专业课程建设探索[J]. 社会科学前沿, 2022, 11(9):3926-3932.
- [7] PENG Z F, XING G Q, CHEN X Y. An overview of application and technology of artificial intelligence in cybersecurity [J]. Journal of Information Security Research, 2022, 8(2): 110-116.  
彭祯方, 邢国强, 陈兴跃. 人工智能在网络安全领域的应用及技术综述[J]. 信息安全研究, 2022, 8(2): 110-116.
- [8] LU H Q. Data network security strategy in the context of big data [J]. Big Data and Artificial Intelligence, 2023, 3(4): 27-29.  
陆海琴. 大数据背景下数据网络安全策略[J]. 大数据与人工智能, 2023, 3(4): 27-29.
- [9] ZHOU Q, HU Y. "Adversarial learning" teaching method and its application in computer network security course [J]. Computer Education, 2023 (4):58-63.  
周庆, 胡月. “对抗式学习”教学法及其在计算机网络安全课程中的应用[J]. 计算机教育, 2023(4):58-63.
- [10] SUN W F, JIA M H, QIN Z Q. A study on the co-teaching program of cyber security professional course coherence [J]. Computer Education, 2019(12):51-54.  
孙伟峰, 贾茗涵, 覃振权. 网络安全专业课程贯通的联合教学方案研究[J]. 计算机教育, 2019(12):51-54.
- [11] YAN Z. A study on multidimensional flexible teaching and learning process under knowledge modeling and assisted training system [J]. Computer Education, 2021(8):189-193.  
严志. 知识建模和辅助训练系统下的多维柔性教学过程研究[J]. 计算机教育, 2021(8):189-193.
- [12] JI S, PAN S, CAMBRIA E, et al. A survey on knowledge graphs: representation, acquisition, and applications [J]. IEEE Transactions on Neural Networks and Learning Systems, 2021, 33(2): 494-514.
- [13] DING Z Y, LIU K, LIU B, et al. Survey of cyber security knowledge graph [J]. Journal of Huazhong University of Science and Technology (Nature Science Edition), 2021, 49(7): 79-91.  
丁兆云, 刘凯, 刘斌, 等. 网络安全知识图谱研究综述[J]. 华中科技大学学报(自然科学版), 2021, 49(7): 79-91.
- [14] ALDAAJEH S, SALEOUS H, ALRABAE S, et al. The role of national cybersecurity strategies on the improvement of cybersecurity education [J]. Computers & Security, 2022, 119:102754.
- [15] ZHOU X C, GONG J H, LI Y Q, et al. Research progress of malicious code detection technology based on deep learning [J]. Modern Computer, 2019 (15): 42-46.  
周显春, 龚家浩, 李芸倩, 等. 基于深度学习的恶意代码检测技术研究进展[J]. 现代计算机, 2019 (15): 42-46.
- [16] SHEN Q N, QING S H. Exploration of a new teaching mode of "operating system security" - application and practice of byu teaching network [J]. Modern Educational Technology, 2010 (S1): 32-33.  
沈晴霓, 卿斯汉. “操作系统安全”新型教学模式的探索——北大教学网的应用与实践[J]. 现代教育技术, 2010 (S1): 32-33.
- [17] DENG R Y, YU M L, DING Y, et al. Safeguarding cyberspace security with the legal system to build a strong cyber nation - Interpretation of the Cybersecurity Law and the National Cyberspace Security Strategy [J]. E-Government, 2017 (2): 2-35.  
邓若伊, 余梦琨, 丁艺, 等. 以法制保障网络空间安全构筑网络强国——《网络安全法》和《国家网络空间安全战略》解读[J]. 电子政务, 2017 (2): 2-35.

(责任编辑:黄健)