Creative Education Studies 创新教育研究, 2026, 14(5), 295-301
Published Online May 2026 in Hans. https://www.hanspub.org/journal/ces
https://doi.org/10.12677/ces.2026.145346

Hans汉斯

基于信息论的大学生网络空间安全素养培育

谢　茜

湖北大学网络空间安全学院，湖北　武汉

收稿日期：2026年4月1日；录用日期：2026年5月14日；发布日期：2026年5月25日

摘　要

随着数字化与网络化的深度融合发展，大学生网络空间安全素养已成为人才培养的重要内容。针对当前大学生网络空间安全素养存在“意识高于认知、认知高于行为”的结构性问题，本文引入信息论，以不确定性度量为理论基础，提出网络空间安全素养培育策略，并以《网络空间安全素养导论》课程为例进行实践验证。研究表明，该策略有助于提升学生的结构化认知与综合分析能力，促进安全素养由“知”向“行”的转化。

关键词

网络空间安全素养，信息论，不确定性，大学生

Cultivation of Cyberspace Security Literacy among College Students Based on Information Theory

Xi Xie

School of Cyber Science and Technology, Hubei University, Wuhan Hubei

Received: April 1, 2026; accepted: May 14, 2026; published: May 25, 2026

Abstract

With the deep integration and development of digitalization and networking, cyberspace security literacy among college students has become an important component of talent cultivation. However, a structural imbalance persists, where awareness exceeds cognition and cognition exceeds behavior. To address this issue, this paper introduces information theory and, based on uncertainty measurement, proposes strategies for cultivating cybersecurity literacy. These strategies are validated through practical application in the course Introduction to Cyberspace Security Literacy. The study

文章引用: 谢茜. 基于信息论的大学生网络空间安全素养培育[J]. 创新教育研究, 2026, 14(5): 295-301.
DOI: 10.12677/ces.2026.145346

shows that this approach helps enhance students' structured cognition and comprehensive analytical abilities, and promotes the transformation of security literacy from knowing to doing.

Keywords

Cyberspace Security Literacy, Information Theory, Uncertainty, College Students

1. 引言

网络空间已成为数字社会运行的重要基础环境，是支撑信息传播、社会治理与经济发展的关键载体。随着数字化进程的持续深化，网络空间安全的重要性日益凸显。据中国互联网络信息中心(CNNIC)发布的第 57 次《中国互联网络发展状况统计报告》[1]显示，截至 2025 年 12 月，我国网民规模达 11.25 亿人，互联网普及率突破 80%，网络已深度渗透至日常生活的方方面面。大学生作为网络空间的主要参与群体，其行为方式与安全认知水平对整体网络生态具有重要影响。因此，加强大学生网络空间安全素养培养，已成为高校人才培养体系中的重要内容。

大学生网络安全素养一般是指大学生安全、合法、高效利用网络资源的能力和认知水平[2]。近年来，大学生网络空间安全素养问题持续受到国内外学者的广泛关注[3] [4]。结合最新调查研究成果[5] [6]和高校学生的现实表现来看，当前大学生网络空间安全素养整体呈现出一定基础与明显不足并存的特征：一方面，多数大学生已具备较强的安全风险意识；另一方面，在知识体系构建、风险认知深化及安全行为落实等方面仍存在不足，表现为认知与行为之间的脱节。同时，不同专业背景学生在网络安全知识与能力方面存在显著差异。相关专业学生虽具备一定理论基础，但在实践转化与应用能力方面仍显不足；而非相关专业学生则普遍存在知识碎片化、体系性缺失的问题。

针对上述问题，亟需引入系统化理论框架，对网络安全认知、风险判断与行为决策之间的内在机制进行深入剖析。信息论作为研究信息不确定性及其传输规律的基础理论，为理解网络空间安全问题提供了统一的分析视角[7]。基于此，本文在梳理大学生网络空间安全素养现状及其问题成因的基础上，引入信息论相关理论，探讨其在大学生网络空间安全素养培育中的应用路径，以提升大学生网络空间安全素养水平，并以《网络空间安全素养导论》课程为例开展教学实践分析。

2. 网络空间安全素养现状分析

围绕大学生网络空间安全素养问题，本节从素养现状、教育现状及问题分析三个层面展开。

2.1. 大学生网络空间安全素养现状

近年来，随着网络环境复杂性的不断增强，大学生网络空间安全素养问题日益受到广泛关注。综合最新调研数据，当前大学生网络安全素养整体呈现出“意识高于认知、认知高于行为”的结构性特征，且该特征在不同专业背景学生之间表现出一定差异。

从总体情况来看，中国青年网校园通讯社[5] 2025 年对 4989 名大学生的调查显示，大学生对新兴网络安全风险的关注度较高，其中 91.52%的受访者认为人脸、指纹等生物信息泄露风险需要重点关注，87.31%的受访者对 AI 伪造技术诈骗表现出较高警惕性。然而，这种较高的风险意识并未有效转化为安全行为习

惯，例如38.46%的大学生从不更换账户密码，反映出认知与行为之间存在明显偏差。

从专业差异来看，网络空间安全及计算机类相关专业学生在安全知识与认知水平方面具有一定优势。《AI时代网络安全产业人才发展报告(2025)》[6]显示，在网络安全专业学生中，71.1%的学生表示对AI在网络安全领域的应用“非常了解”或“比较了解”，体现出其在前沿技术认知方面的优势。但与此同时，专业学生在知识向能力转化方面仍存在不足，实践能力与行为规范尚未完全形成。

综合来看，专业与非专业学生在网络空间安全素养方面既存在差异，也呈现出一定共性，其主要特征归纳如表1所示。

Table 1. Cyberspace security literacy among majors and non-majors
表1. 专业与非专业大学生网络空间安全素养现状

维度	专业学生	非专业学生
安全意识	较高，但对新兴风险认知更深	较高，但对风险原理理解不足
安全知识	系统完整，71.1%了解AI安全	碎片化，依赖媒体和自我摸索
安全技能	理论学习为主，实战能力不足	几乎空白，缺乏系统训练
安全行为	基础习惯有待改善	基础习惯普遍不佳

2.2. 网络空间安全教育现状

当前，高校网络空间安全教育已逐步引入多元理论视角，并从行为机理、能力结构与教学模式等方面开展探索。在行为机理层面，知识–态度–行为(Knowledge-Attitude-Practice, KAP)模型为解释、量化和分析大学生网络安全行为提供了理论框架。该理论认为个体的安全行为由安全认知和态度共同决定，认知需经过态度内化才能有效转化为行为，在网络空间安全教育领域应用广泛。例如，李媛媛等人将大学生网络安全教育、认知、态度、行为作为KAP分析框架中的研究变量构建了相关网络安全教育模型[7]。

在能力结构层面，由美国国家标准与技术研究院(NIST)发布的国家网络安全教育计划(National Initiative of Cybersecurity Education, NICE)从岗位需求出发，系统界定了各类职位的任务及所需“知识、技能、能力”，对网络安全教育与人才培养具有重要指导意义。例如，McGuan等人依托NICE框架，针对典型攻击场景提取对应的技术与非技术任务、知识、技能和能力，设计了一套情景化课程[8]。

在教学模式层面，成果导向教育(Outcomes-Based Education, OBE)理念强调以学习成果为导向，通过实践教学促进能力达成。蒲晓川和张远强基于OBE理念，将虚拟仿真教学融入《网络信息安全》课程[9]。此外，情境学习理论、建构主义学习理论等也在网络安全教育中得到广泛应用。

2.3. 网络空间安全素养问题分析

基于素养现状和教育现状，从知识结构、教育供给与认知转化三个维度展开问题分析。

(一) 知识结构维度

研究表明，无论是专业学生还是非专业学生，其网络安全知识均存在不同程度的结构性问题。专业学生虽具备一定理论基础，但其知识体系多以离散知识点为主，缺乏内在逻辑关联与结构化整合能力，难以在复杂情境中实现知识迁移与综合运用；非专业学生则普遍缺乏系统化网络安全教育，知识来源碎片化，难以形成完整认知框架，导致其对网络安全问题的理解停留在表层。

(二) 教育供给维度

当前高校网络安全教育整体仍以知识传授为主。尽管KAP、NICE及OBE等理论为教学设计提供了重要参考，但在实际教学过程中，多侧重于知识结构设计与能力要素划分，缺乏对安全思维能力进行系

统培养的教学模块与评价机制。同时，针对不同专业背景学生的差异化教学机制尚不完善，难以有效匹配不同群体的学习基础与认知需求。

(三) 认知转化维度

尽管大学生整体具备一定网络安全认知基础，但在实际网络环境中仍难以将相关认知有效转化为稳定行为模式。从现有教育实践来看，无论是 KAP 模型对行为路径的解释，还是 OBE 理念对能力达成的强调，均未能充分揭示个体在复杂信息环境中进行风险判断与行为决策的内在机制。

基于此，本文引入信息论作为分析工具，从信息不确定性及其传递机制出发，对相关信息过程进行量化分析，以刻画其内在作用关系。

3. 基于信息论的网络空间安全素养培育

面向大学生网络空间安全素养培育问题，本节从信息论理论基础及其在教育实践中的应用两个方面进行探讨。

3.1. 信息论相关理论基础

Claude E. Shannon 于 1948 年发表的经典论文《通信的数学理论》[10]标志着信息论的诞生，揭示了信息传输系统的基本规律。从信息的基本特点来看，一个事件的不确定性越大，其所蕴含的信息量越多；反之，不确定性越小，信息量越少。因此，对信息的度量需要建立刻画不确定性的数学模型。基于此，Shannon 在通信上定义信息是消除随机不确定性的东西，并引入信息熵以量化随机变量的不确定性。对于一个离散随机变量 X，其信息熵 H (X)定义为

$$H(x)=-\sum_{i=1}^{n} p(x_i)\log_2 p(x_i) \tag{1}$$

其中 $p(x_i)$ 是事件 x_i 发生的概率。信息熵反映信源输出的平均信息量，是衡量随机变量不确定性的基本指标。当概率分布越均匀时，系统不确定性越高，对应的信息熵也越大；反之，当分布越集中时，信息熵越小。为了描述信息的传输过程，Shannon 进一步提出了经典的通信系统模型，如图 1 所示。

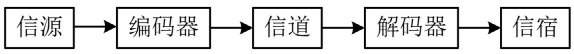

Figure 1. Unified communication system model
图 1. 统一通信系统模型

该模型将通信过程抽象为五个基本组成部分：信源、编码器、信道、解码器以及信宿。其基本过程为：信息从信源出发，经过编码、调制后进入可能受到噪声干扰的信道，最终通过解调、译码还原至信宿。整个通信过程本质上是不确定性逐步消除的过程：信源编码去除冗余，信道编码对抗干扰，译码环节则在噪声中还原原始信息。概而言之，信息论的核心思想是将“信息”抽象为可量化的实体，以概率模型刻画信源与信道口，用熵度量信息不确定性，为复杂系统问题提供了统一分析框架。

3.2. 信息论在网络空间安全素养培育中的应用

立足大学生网络空间安全素养培育需求，本小节从培育策略、课程实践与教学效果三个层面，探讨信息论在安全素养培育中的具体应用。

3.2.1. 培育策略

信息论为网络空间安全素养教育提供了“以不确定性为核心”的分析框架。据此，可从以下三个方面开展培育：

(一) 以信息不确定性为主线重构安全认知

引导学生理解“不确定性越大，信息量越大”的原理，进而理解网络攻击本质是增加系统不确定性，而防御措施旨在降低不确定性。例如，强密码与多因素认证能够降低账户被破解的不确定性，从而将安全行为与理论认知建立对应关系，促进系统化理解。

(二) 以通信系统模型为分析框架建立结构化思维

基于通信系统模型，将网络攻击与防御映射至不同环节：如身份冒充对应信源攻击，窃听与中间人攻击对应信道攻击；相应防御措施包括加密、认证与纠错机制等。该方法有助于形成系统化的攻防分析思维，增强对安全机制的整体把握。

(三) 设计基于信息度量的实践环节强化能力

依托信息论的可量化特征，设计实践任务，引导学生运用信息熵、信道容量等指标分析密码强度、异常流量及信息泄露问题，促进理论知识向实际应用与行为决策能力的转化。

3.2.2. 课程实践

为验证上述策略的可行性，选取《网络空间安全素养导论》课程开展教学实践。课程围绕知识、素养、能力三个维度设定培养目标：掌握网络安全核心概念与基本防护技能，强化网络安全意识与法律道德认知，培养批判性思维与持续学习能力。为实现上述目标，课程从以下三个方面开展教学实践。

(一) 理论认知引导

在讲授网络空间安全的基本构成和核心概念时，引入信息论对“信息”的定义，引导学生将信息由抽象概念转化为可量化实体，从而认识网络空间安全问题的本质在于对不确定性的识别、管理与调控，为后续学习奠定理论基础。

(二) 通信系统模型框架建立

在常见网络攻击类型及案例分析教学中，将攻击与防御过程映射至通信系统模型，引导学生识别攻击发生的关键环节，并分析防御机制如何通过编码与抗干扰手段降低噪声影响、实现纠错与校验，从而提升信息传输的可靠性与有效性，强化对攻防机理的结构化理解。

(三) 量化实践与信息度量应用

通过设计量化实验，将信息熵、信道容量等概念融入实践教学。例如，计算不同密码策略的信息熵以评估安全性，基于流量特征熵识别异常行为，以及通过隐蔽信道模拟分析信息泄露机制等。以密码信息熵计算实验为例，选取四组不同策略的密码样本(6 位纯数字、8 位小写字母、10 位大小写加数字、12 位全字符组合)，假设每个字符是独立且均匀随机选择的，引导学生计算每组密码的信息熵。设 N 为密码长度，L 为字符集合大小，则 $p(x_i)=1/\mathrm{L}^{\mathrm{N}}$ 。进而将其代入(1)中计算不同密码的信息熵值。通过比较熵值与理论破解时间，分析其安全性差异。该实验旨在帮助学生理解信息熵与密码强度的量化关系。

融入信息论的内容模块如表 2 所示。

Table 2. Selected teaching content from “Introduction to Cyberspace Security Literacy”
表 2. 《网络空间安全素养导论》部分教学内容

知识模块	教学内容	信息论融入点
网络空间安全概述	网络空间概念、发展历程、战略背景	通过信息不确定性引入安全认知
网络威胁与挑战	攻击类型、威胁源、案例分析	攻击映射至通信系统模型
信息与数据安全	数据保护、隐私与合规、备份与恢复	信息熵、信息量分析
安全实践与技能	密码管理、身份认证、安全配置	信息熵实践计算
案例分析与实践	网络安全事件分析、实践与演练	综合运用信息论分析攻击与防御

3.2.3. 教学效果分析

为探索信息论融入教学后的学生表现变化，本研究以某高校《网络空间安全素养导论》课程的课程报告(N = 193)与课堂问答记录为主要分析材料，采用内容分析法，对比未引入信息论教学的历史班级课程报告(N = 216)，从安全认知深度、技术分析能力及综合应用能力等维度进行比较分析。

综合分析发现，未引入信息论教学的课程报告主要呈现出以下特点：其一，在“网络空间安全认识”部分，多停留于概念性与宏观层面的描述，缺乏对安全问题本质的深入理解；其二，在法律法规部分，虽能较为完整地列举相关条文，但整体以复述为主，对其内在逻辑及实际应用理解不足；其三，在技术认知方面，能描述防火墙、加密等基本技术，但对其原理理解较为浅显，缺乏系统分析与综合运用能力。

相比之下，引入信息论教学后，学生课程报告在多方面呈现明显提升：一是在安全认知方面，部分学生能够从“信息不确定性”的视角分析安全问题，将网络攻击理解为对信息传输过程的不确定性干扰，体现出一定的理论抽象能力；二是在技术分析方面，能够结合信息熵、编码与传输等概念，对密码强度及数据保护问题进行更具逻辑性的阐释；三是在综合分析方面，学生更倾向于基于系统结构分析攻击路径与防御机制，而非简单罗列技术手段。

总体来看，教学效果由“描述性认知”逐步转向“解释性认知”与“结构化分析”，认知深度、理论应用能力及综合分析能力均有所提升，初步揭示了信息论在安全素养培育中的潜在价值。

4. 结论与展望

本文从信息论视角出发，围绕大学生网络空间安全素养培育问题，构建了以“不确定性度量”为核心的分析框架，并提出相应培育策略。通过课程实践与教学效果分析表明，引入信息论有助于为网络空间安全认知提供统一的理论支撑，强化学生对安全问题内在机理的理解，促进其形成更系统性与结构化的分析视角，从而为大学生网络空间安全素养培育提供新的理论依据与实践路径。

但本研究仍存在一定局限性：一方面，研究样本主要来源于单一高校且规模有限；另一方面，研究对象集中于特定课程学生群体，且教学效果评价主要基于课程报告文本分析。未来研究可进一步扩大样本范围并引入多校对比研究，构建多维度评价与长期跟踪机制，以更系统检验信息论在安全素养培育中的应用效果；同时拓展应用场景，将培育模式延伸至不同专业与课程类型，并探索与人工智能等技术融合，促进安全素养教育向智能化与个性化发展。

参考文献

[1] 中国互联网络信息中心. 第 57 次《中国互联网络发展状况统计报告》[EB/OL]. https://www.cnnic.org.cn/n4/2026/0304/c88-11549.html, 2026-02-05.

[2] 叶定剑. 当代大学生网络素养核心构成及教育路径探究[J]. 思想教育研究, 2017(1): 97-100.

[3] Leung, L. and Lee, P.S.N. (2012) Impact of Internet Literacy, Internet Addiction Symptoms, and Internet Activities on Academic Performance. *Social Science Computer Review*, **30**, 403-418. https://doi.org/10.1177/0894439311435217

[4] 阙凤仪. 大数据时代高校学生网络安全素养评价指标体系及应用研究[D]: [硕士学位论文]. 武汉: 武汉工程大学继续教育学院, 2022.

[5] 中国青年网校园通讯社. 大学生网络安全意识调查报告[EB/OL]. https://news.youth.cn/jsxw/202508/t20250822_16192155.htm, 2025-08-22.

[6] 工业和信息化部教育与考试中心, 安恒信息, 等. AI 时代网络安全产业人才发展报告(2025) [EB/OL]. https://cos.hrtools.club/6/58667/pdf/1759213357552a6a118e686a920be638773cb6afc9a82.pdf, 2025-09-16.

[7] 李媛媛, 袁玉林, 随力瑞. 基于 KAP 理论的大学生网络安全教育研究[J]. 中国安全科学学报, 2024, 34(5): 1-8.

[8] McGuan, C., Vijaya Raghavan, A., Mandapati, K.M., Yu, C., Ray, B.E., Jackson, D.K., *et al*. (2025) Bridging Cybersecurity Practice and Law: A Hands-On, Scenario-Based Curriculum Using the NICE Framework to Foster Skill Development. *Journal of Cybersecurity and Privacy*, **5**, Article No. 106. https://doi.org/10.3390/jcp5040106

[9] 蒲晓川, 张远强. 基于 OBE 理念的虚拟仿真教学创新改革——以“网络信息安全”课程为例[J]. 遵义师范学院学报, 2025, 27(1): 104-109.

[10] Shannon, C.E. (1948) A Mathematical Theory of Communication. *Bell System Technical Journal*, **27**, 379-423. https://doi.org/10.1002/j.1538-7305.1948.tb01338.x