DOI:10.13718/j.cnki.jsjy.2023.01.012

美国中小学生网络安全素养教育的实践策略与保障机制

王正青,程 涛
(西南大学 教育学部,重庆 400715)

摘要:中小学生网络安全素养教育旨在确保学生获得网络安全基本知识,养成网络安全自护能力。作为教育信息化发展的前沿国家,美国基于中小学校网络安全事件频发的现实背景,统筹部署中小学生网络安全素养教育实践策略,包括:营造网络安全文化氛围,以增强学生网络安全意识;设置网络安全素养教育课程,以筑牢网络安全知识根基;开展网络安全主题竞赛,以构建网络风险防御能力;推出网络安全营地活动,以增进网络安全认知体验。美国依托政策规范、师资培训、经验交流、资金支持等手段,保障中小学生网络安全素养教育有效开展。借鉴美国培育中小学生网络安全素养经验,我国可从推进网络安全素养教育制度建设、统筹调配网络安全素养教育资源、加大教师网络安全教育素养培养力度、倡导社会行业组织支持参与等几个方面着手,完善中小学生网络安全素养教育体系架构。

关键词:美国;中小学生;核心素养;网络安全素养;网络安全课程

中图分类号:G571.2 **文献标识码**:A **文章编号**:2095-8129(2023)01-0100-08

作者简介:王正青,教育学博士,西南大学教育学部教授,博士生导师;程涛,西南大学教育学部博士研究生。

一、问题提出

新冠疫情背景下,在线教育规模大幅扩大,随之共生的网络安全问题引发世界各国高度关注。网络安全是确保信息技术基础设施及网络通讯系统和系统上所存储、处理或传输的数据与信息不受安全威胁[1]。然而,广大中小学生心理不成熟的特点及落后的网络安全意识,难以匹配当前日益增加的教育信息化发展诉求,致使中小学成为网络安全事件的高发区。2020年5月,共青团中央维护青少年权益部和中国互联网络信息中心联合发布的《2019年全国未成年人互联网使用情况研究报告》显示,2019年,我国未成年网民规模为1.75亿,其中19.8%的未成年网民遭遇过账号密码被盗,15.4%和11.4%的未成年网民分别遭遇过电脑/手机中病毒和网络诈骗,6.4%的未成年人经历了个人信息泄露危机[2]。

2020年8月,教育部等六部门发布《关于联合开展未成年人网络环境专项治理行动的通知》,要求通过专题教育、课堂教学、班团队会等形式,加强中小学生网络素养和网络安全自我保护教育及宣传引导,提升中小学生的上网技能、信息甄别和安全防护能力等网络素养。网络安全素养教育有益于强化学生网络安全素养建设,提升网络安全意识和防御能力,推动构建和谐清朗的网络空间环境。基于此,本文以教育信息化发展的前沿国家美国为研究对象,在厘清美国培养中小学生网络安全素养的现实背景基础上,分析美国中小学生网络安全素养教育的实践策略与保障机制,以期对提升我国中小学生网络安全素养、强化中小学生网络安全意识与行动自觉性有所助益。

二、美国培育中小学生网络安全素养的现实背景

“互联网＋”时代的到来加快了教育信息化的发展步伐，其在助力教学便捷化和学习泛在化的同时，也因网络空间的虚拟性、超时空性和无中心性等特征，造成美国中小学出现了一系列网络安全问题，发生了不少网络安全事件。所谓“网络安全事件”，是指实际或潜在威胁互联网系统及其所持有的信息，亦或对安全策略和安全程序等构成威胁的系列事件和违规行为，包括未经授权的访问、披露、修改或销毁[3]，继而对机构运作和人员体系产生不利影响。有研究发现，教育行业最容易成为网络不法分子的攻击目标，教育领域总体网络安全在全美 17 个行业中排名倒数第一。2016 年至 2019 年，中小学网络安全事件更是波及全美各州，尤其以德克萨斯州、纽约州、伊利诺伊州、加利福尼亚州和佛罗里达州为典型代表，分别共计发生 117 起、88 起、60 起、45 起和 26 起中小学网络安全事件。2019 年，美国 44 个州公开报告了 348 起中小学网络安全事件，这一数字是 2018 年的近 3 倍[4]。

美国中小学频发的网络安全事件大致包括三类。(1)数据泄露事件。这是 2019 年美国中小学网络安全事件中最常见的类型，占比达到 60％。学生数据信息泄露类型主要为两类，一类是学生学业记录如考试评估分数和特殊教育记录等信息被泄露，另一类是学生个人身份信息记录如社会保险账号等被泄露。教育数据一旦泄露很容易被非法查看、复制、传输和利用。自 2005 年以来，美国中小学和高等教育机构发生数据泄露事件高达 788 起，导致超过 1 487 万份数据被泄露[5]。美国相关统计显示，2019 年 7 月 1 日至 2020 年 5 月 5 日，共发生中小学生数据泄露事件 13 起，影响全美 146 个学区[6]。(2)勒索软件事件。此类网络安全事件占比为 18％。勒索软件通过发布具有恶意链接的电子邮件和黑客网址引诱网络用户点击浏览，继而锁定用户系统或加密计算机上的文件信息，并在恢复系统或文件之前要求用户支付“赎金”，以达到劫持计算机系统进行勒索的目的[7]。勒索软件往往会破坏教育机构的正常运作，并使机构内部重要文件信息的机密性、完整性和安全性面临风险。美国纽约州、俄亥俄州、阿拉巴马州、亚利桑那州、新泽西州多所中小学校都曾因勒索软件事件而被迫停学或关闭学校。(3)网络钓鱼或网络诈骗事件。2019 年，美国虽然只有 8％的学校网络安全事件被归类为网络钓鱼或网络欺诈，但其却是引发数据泄露和软件勒索事件的常见手段。网络钓鱼是指通过诱导用户访问虚假网站，欺诈网络用户泄露信用卡密码和银行账户等敏感信息。美国肯塔基州曾因此类事件而损失了大约 370 万美元。网络钓鱼是指目前为止，美国中小学领域发生的最为严重的网络诈骗事件。此外，德克萨斯州、俄勒冈州、北卡罗来纳州和弗吉尼亚州也曾因网络钓鱼事件而损失 60 万美元至 290 万美元不等[8]。

此起彼伏的网络安全事件让美国认识到实施网络安全素养教育已经迫在眉睫。美国以规避中小学网络安全事件为导向，以提升中小学生网络安全素养为宗旨，全面实施网络安全素养教育战略。一是强化学生网络安全意识建设，使其获得网络安全基本常识，能够甄别网络不良信息和潜在安全风险。二是提升中小学生网络安全自护技能。包括下载安装权威软件，并对其进行定期杀毒检查和密码更新设置，对黑客攻击、教育数据泄漏、网络暴力、网络钓鱼与欺诈、恶意链接和网络病毒等多类网络威胁及时采取相应的安全防范和应对措施，从而降低人为因素造成的网络安全事件发生概率。三是推动网络安全专业人才培育实践，填补网络安全职业空缺。相关统计显示，截至 2018 年 11 月，美国有 30 多万个网络安全职位空缺；到 2022 年，美国网络安全专业人才缺口预计将上升至 180 万人[9]。巨大的网络安全职位空缺，促使美国将目光投向学校网络安全专业人才培养。美国基于网络安全素养教育需要，致力于促发中小学生网络安全职业意识萌芽，刺激中小学生在大学阶段主动选择信息技术和网络安全专业，最终构建起网络安全专业人才贯通培养模式，平衡网络安全专门人才匮乏与美国社会网络安全职业岗位需求激增的矛盾。

三、美国培育中小学生网络安全素养的实践策略

美国以中小学网络安全课程开发为引领，以多类型网络安全实践活动为手段，积极推进网络安全素养教育实施，以强化学生信息隐私保护观念，增强网络诈骗防护意识，提高自护本领。

（一）营造网络安全文化氛围，增强学生网络安全意识

美国培育中小学生网络安全素养从树立网络安全危机意识和防护观念着手。美国联邦调查局（Federal Bureau of investigation，FBI）除积极开展学校网络安全事件调查外，还针对网络安全威胁和学生数据隐私等问题，向各州学区和教育组织发出预警通知，以强化学校师生的网络安全危机意识。2004 年，美国国土安全部（Department of Homeland Security，DHS）下属的国家网络安全部（National Cyber Security Division）和国家网络安全联盟（National Cyber Security Alliance）共同发起行动倡议，确定将每年 10 月定为美国的“国家网络安全意识月”（National Cyber Security Awareness Month，NCSAM）[10]。自此，美国各级中小学围绕“国家网络安全意识月”主题，倡议积极开展信息共享、隐私保护、入侵检测、密码设置等网络安全领域宣传教育活动，帮助学校师生及社会大众了解在线安全、网络欺凌、网络礼仪等常识，增强学生网络安全思想观念，确保其了解网络安全事件发生前后的具体行动策略和应急响应程序，能够有效识别、正确处理和及时化解网络风险。此外，学校也倡导家长共同参与网络安全意识建设行动，通过指导和监管孩子网络行为，为其把好网络安全关。

（二）设置网络安全素养教育课程，筑牢网络安全知识根基

学校网络安全课程是实施网络安全素养教育的基本载体，美国在循序渐进理念下实现了各学段课程的贯通融合。一是秉承循序渐进理念，逐级推进学校网络安全课程构建与实施。美国德克萨斯州赫斯特-尤利斯-贝德福德独立学区（Hurst-Euless-Bedford Independent School District）在 2018 年首次为七年级学生开设网络安全课程，旨在引入网络安全基本概念，包括网络、编码、密码学、硬软件、数字公民身份、网络安全、网络道德与法律等。八年级学生的网络安全课程在其基础上进行了扩展，升至九年级时，则会就网络安全课程掌握程度进行评估。以密码学课程为例，七年级学生主要学习密码学的基本原理、目的和作用等内容。八年级学生将学习密码学的运用历史和不同密码的具体使用方法。九年级学生不仅需要创设自己的网络密码，还需通过参加网络安全竞赛，证明其对密码学概念的掌握程度[11]。

二是注重大中小学网络安全课程的贯通融合。美国威斯康星州以网络安全专业人才建设为根本，强调网络安全素养教育建设应囊括从中小学到研究生阶段的全流程专业课程与学位设置，继而为学生开辟一条进入网络安全领域的职业通道[12]。弗吉尼亚州于 2017 年秋季在九至十二年级专门设置了 8 门全新的网络安全课程，学习主题包括网络安全基础、网络安全软件操作和系统技术、网络安全软件高级操作、网络安全系统建设等。对网络安全感兴趣的学生，可以选择两门及以上网络安全必修课程进行集中学习，以便为大学网络安全专业选择以及未来从事网络安全职业筑牢根基[13]。

（三）开展网络安全主题竞赛，构建网络风险防御能力

网络安全主题竞赛是美国推动中小学生网络安全素养培育的重要举措。美国中小学生参与的网络安全比赛主要分为两种类型，一类侧重于强化中小学生网络安全意识，另一类聚焦中小学生网络安全维护实践操作技能。美国推出的“全国中小学网络安全意识海报大赛”（National K-12 Cybersecurity Awareness Poster Contest）即为第一种类型。大赛以促进中小学生网络安全素养提升为目标，以互联网或移动设备的安全使用为主题，针对不同年级学生提出不同设计主题建议。如小学和初中阶段的设计主题包括：哪些信息可安全地发布在社交媒体、哪些应该保密、如何对待网络陌生人、如何处理网络欺凌和设置安全密码等。大赛会从小学、初中、高中三个年级组中选出优胜者，排名前四的优秀作品将被制作成网络安全宣传海报，并分发至全国各地[14]。

在提升中小学生网络安全技能方面，美国专门为高中女学生设置了“女生网络安全领航比赛”(Girls Go-Cyber Start)，要求学生充当网络保护代理，以深入研究加密和数字取证等内容。参与者不需要信息技术或网络安全方面的专业知识或经验，只要具备电脑操作能力和问题解决热情皆可报名参赛。相关统计显示，2018年，美国共计6 550名高中女生参加Girls Go-Cyber Start资格赛，2 200支队伍进入挑战赛，17个州的62所高中因为学生的优良比赛成绩而获得财政奖励。有研究表明，仅36%的学生在参与Girls Go-Cyber Start之前考虑过攻读计算机科学与技术或信息安全专业，但在参赛后，该数字已经上升至70%[15]。此外，美国针对初高中学生还推出了“网络爱国者竞赛”(Cyber Patriot)。2019年，美国共计6 750支队伍报名参赛，教师通常作为教练负责学生招募和团队注册，挑战内容是发现和修复虚拟操作系统中的网络安全漏洞[16]。

总体而言，美国网络安全主题竞赛在深化中小学生网络安全意识、激发学生网络安全研究兴趣方面，发挥了极大作用。

(四)推出网络安全营地活动，增进网络安全认知体验

除上述实践外，美国还开展了多种类型的网络安全营地活动，以满足中小学生网络安全实践体验诉求，增进和丰富学生对于网络安全的现实理解与切身感知。2014年，在美国国家安全局(National Security Agency，NSA)、国家科学基金会(National Science Foundation，NSF)和国家情报局长办公室(Office of the Director of National Intelligence，ODNI)的支持下，美国正式启动了“未来网络安全新星”(Gen Cyber)夏令营项目，旨在通过提供适龄的特色网络安全活动，教授网络安全原则和概念、在线安全和道德规范等内容，增进中小学师生暑期网络安全认知体验。同年，美国空军协会(Air Force Association，AFA)推出了“网络安全营地”(Cyber Camp)计划，其主要针对刚接触网络安全领域或具有一定网络安全知识、希望获得更多相关知识的中学生。网络安全营地计划将为学校和教育机构订购一套包括教学模块、教师指南、学生手册、演示软件和竞赛软件等在内的学习包，以实现网络安全技能传授[17]。2016年，弗吉尼亚州网络安全营地在8个学区开展了共计70小时的暑期培训，包括提供基本编程技能指导，帮助高中生探寻网络安全领域职业机会，鼓励其获得网络安全相关证书[18]。

四、美国培育中小学生网络安全素养的保障机制

美国通过网络安全素养教育政策规范、资金支持、构建网络安全素养教育学术交流平台、优化网络安全素养教育师资队伍等举措，推动美国中小学生网络安全素养教育有效落地。

(一)政策规范：强化中小学生网络安全素养教育顶层设计

美国颁布了系列网络安全素养教育政策和法规，这些政策和法规在强调中小学生网络安全素养教育价值的基础上，也为学校制定网络安全素养教育体系架构提供科学指导。早在2000年，美国国会就颁布了《儿童互联网保护法》(*Children's Internet Protection Act*，CIPA)，要求学校、家长及社会等各方协调解决儿童在互联网上接触淫秽或有害内容的问题。2020年，美国国家教育统计中心(National Center for Education Statistics，NCES)出台的《网络安全论坛指南：保护你的数据》(*Forum Guide to Cybersecurity: Safeguarding Your Data*)，系统概述了全美中小学网络安全现状，以进一步凸显中小学培育学生网络安全素养的迫切性。

除此之外，美国还从壮大网络安全人才队伍规模的视角，彰显中小学网络安全素养教育的时代价值。2017年，美国颁发的《网络安全人才框架》(*Cybersecurity Workforce Framework*)明晰了网络安全领域从业人员所需的知识、技能和能力，为学校和教育机构组织开展中小学生网络安全素养教育与培训提供了文本参考[19]。2019年，美国发布《联邦网络安全研究与发展战略计划》(*Federal Cybersecurity Research and Development Strategic Plan*)，明确指出目前美国网络安全人员不仅在数量上同时也在质量上供需矛盾加剧，而实施网络

安全素养教育是突破这一困境的重要途径，应支持中小学阶段网络安全课程的创新研发，引入网络安全技术主题教育[20]。弗吉尼亚州教育局也发布了《弗吉尼亚州21世纪职业道路——网络安全》(*Virginia's 21st Century Career Pathway: Cybersecurity*)，文件阐述了关于培养大量网络安全专业人才的构想，在肯定中小学网络安全素养教育助力网络安全专业人才建设的重要作用基础上，提出应以中小学网络安全素养教育为切入点，帮助美国小学、初中和高中学生做好未来投身网络安全职业的准备。

(二)师资培训：提升中小学教师网络安全素养

师资能力保障是中小学生网络安全素养培育题中应有之义。美国为此做了两个方面的工作。一是通过网络安全师资培训课程，促进中小学教师专业发展，科学指导其推进网络安全素养教育教学实践。美国联邦教育部、国家综合网络教育研究中心(National Integrated Cyber Education Research Center，NICERC)、学生隐私政策办公室(Student Privacy Policy Office，SPPO)、隐私保护技术支持中心(Privacy Technical Assistance Center，PTAC)和美国国土安全部等推出的“网络安全教育培训支持计划”(Cybersecurity Education Training Assistance Program，CETAP)，致力于提供网络安全师资培训资源，提升中小学教师网络安全素养，并通过教学工具指导，协助教师有效开展网络安全课堂教学[21]。二是依托网络安全领域模范教师的引领作用，潜移默化地提升网络安全素养教育师资队伍的网络安全素养。2019年5月，美国联邦政府专门设置了“网络安全教育总统奖”(Presidential Cybersecurity Education Award)。该奖由美国教育部部长颁发给中小学网络安全素养教育领域杰出工作者，以表彰其在提高学生网络安全意识、增进学生网络防御知识、提升学生网络安全技能以及培养美国未来网络安全专业人才方面作出的突出贡献。2022年，美国教育部部长米格尔·卡多纳(Miguel Cardona)即对来自俄亥俄州的本杰明·多尔蒂(Benjamin Dougherty)和加利福尼亚州的罗伯特·艾伦·斯图布尔菲尔德(Robert Allen Stubblefield)两位获奖者进行了颁奖[22]。

(三)经验交流：构筑中小学生网络安全素养教育学术共同体

美国教师联合会(American Federation of Teachers)主席兰迪·温加滕(Randi Weingarten)指出，21世纪，网络攻击将会成为学校所面临的真正的安全威胁[23]。为此，美国通过网络安全素养教育学术会议，构建中小学生网络安全素养教育共同体，共商共建网络安全素养教育机制。美国国家标准与技术研究所(National Institute of Standards and Technology，NIST)支持的“国家网络安全教育倡议下的K12网络安全教育会议”(National Initiative for Cybersecurity Education K12 Cybersecurity Education Conference)是美国推进中小学生网络安全素养教育的重要交流平台。2018年12月，会议在美国德克萨斯州圣安东尼奥市举办，吸引了美国各州学区行政人员、中小学教育工作者和课程专家等众多代表参与。会议深入探讨了网络安全素养教育体系的构建与实施以及网络安全职业意识的培养与强化等主题。此外，美国网络安全专业人才发展组织(Cyber.org)也会在每年夏天针对中小学网络安全素养教育工作者举办为期3天的“网络教育发展论坛”(Cyber Education Discovery Forum)，致力于讨论网络安全素养教育教学策略设计，畅通中小学教育工作者网络安全教学的经验交流渠道[24]。

(四)资金支持：保障中小学生网络安全素养教育有效落实

美国通过资金支持，确保中小学生网络安全素养教育有效落地。美国国家科学基金会(NSF)与联邦教育部、州教育厅以及地方教育机构合作，为基础教育、高等教育和职业教育阶段的网络安全素养教育计划提供经费支持。一是聚焦强化网络安全意识。美国联邦政府拨付110万美元助力国家“网络安全意识月”计划运行，倡导美国中小学和高校管理者、教师、学生以及中小型企业，通过加强网络安全素养教育和培训、举办网络安全学术会议等举措，协同推进全美网络安全意识计划(National Cybersecurity Awareness Program)[25]。二是推

动网络安全素养教育资源开发。2012年，国家科学基金会提供20万美元支持推进“网络安全教育、课程和专业人才开发”（Cyber Security Education，Curriculum，and Workforce Development）项目，其专注于联邦和各州学区开发网络安全模块化课程，推动美国高中生和大学生网络安全夏令营和网络职业规划等活动实施，扩大美国网络安全人才库[11]。三是助力开展网络安全竞赛。2011年，美国国家安全局向“马里兰州网络挑战赛”（Maryland Cyber Challenge）中获胜的高中生和大学生颁发8.4万美元奖学金，鼓励其积极攻读科学、技术、工程和数学学位。2017年，密歇根州出资50万美元赞助支持本州开展初高中网络安全竞赛，以提升学生计算机专业技能[26]。

五、美国实践对我国中小学生网络安全素养教育的启示

美国基于中小学校网络安全事件频发的现实困境，积极落实中小学生网络安全素养教育实践。其中小学生网络安全素养教育策略与保障机制，对我国推动落实中小学生网络安全素养教育具有重要参考价值。

（一）推进网络安全素养教育制度建设，完善中小学生网络安全素养教育体系

2020年10月，教育部印发《大中小学国家安全教育指导纲要》，强调践行“没有网络安全就没有国家安全，没有信息化就没有现代化”的基本理念，推进中小学数据安全传输、网络信息加密、防范网络诈骗等方面的意识教育。尽管我国已初步确立网络安全教育工作要点，但已有政策文本对中小学生的网络安全素养界定模糊，对中小学网络安全素养教育缺乏系统规划，对中小学何时以及如何开展网络安全素养教育等问题缺乏规范陈述。因此，我国中小学生网络安全素养教育体系有待进一步深化。

聚焦美国中小学生网络安全素养培育经验可以发现，美国颁发的系列政策文本正式明确了中小学开展网络安全素养教育的基本价值，并尝试指导构建中小学网络安全素养教育体系。作为高校网络安全专业人才培养的起始阶段，中小学的网络安全素养教育对加速美国高校网络安全学科发展步伐，推动网络安全专业人才培育实践，填补网络安全职业空缺发挥了重要作用。有鉴于此，首先，我国也应从强化中小学网络安全素养教育制度设计着手，重视中小学网络安全素养教育在推进高校网络安全学科建设和专业人才培养中的奠基性作用。其次，完善我国网络安全素养教育体系架构，使我国学校网络安全素养教育适当向前延伸，确保我国中小学网络安全素养教育逐步制度化、规范化和系统化，最终构建起囊括各个教育阶段的全流程学校网络安全素养教育体系。

（二）统筹调配网络安全素养教育资源，创建中小学生网络安全素养教育机制

目前，我国70%左右的未成年人在学校网络教育课程中学习过网络安全防范和自我保护以及文明上网等知识内容，但仅有55.6%和50.5%的未成年人学习过网络操作技能和网络法律知识[2]。美国在培育中小学生网络安全素养的过程中，既基于社会网络安全文化和学校网络安全课程深化学生理论认知，也通过网络安全比赛和营地活动项目锻炼学生的网络操作技能。借鉴美国中小学生网络安全素养教育行动举措，我国的中小学生网络安全素养教育应致力于做好三个方面的工作。一是做好网络安全素养教育统筹部署与资源协调工作，坚持以中小学生身心发展规律和认知特点为基本考量，创新设计中小学生网络安全课程，并实现不同年级之间网络安全素养教育课程的有效衔接。二是秉持活动设计和竞赛参与理念，将中小学生网络安全素养教育与各类实践活动相结合，推动开展网络安全竞赛和体验项目，实现寓学于乐、知行结合，确保学生能够正确处理好物质世界、精神世界和虚拟世界三者之间的关系，具备网络信息获取、鉴别、利用、处理和安全防护能力[27]。三是在网络安全实践体验中，正确引导中小学生对于网络安全学科专业和职业岗位的理解、认识与兴趣，丰富网络安全素养教育活动的内涵和价值。

（三）加大教师网络安全教育素养培育力度，确保中小学生网络安全素养教育有效实施

美国K-12网络安全资源中心（K-12 Cybersecurity Resource Center）首席执行官道格·莱文（Doug Levin）指出：“今天学校面临的

数字威胁比以往任何时候都大，就像我们知道正确的饮食和锻炼可以带来更健康的生活一样，我们也需制定基本的网络安全措施，如部署反恶意软件和反网络钓鱼技术，实施多重认证，以及提供用户培训，这些都可以产生很大影响。”[28]教师是网络空间的使用者和网络安全素养教育的实施者，因此应高度重视教师的网络安全教育素养建设。一是加大网络安全教育师资培训力度，及时更新中小学教师关于网络安全素养教育方面的知识储备和教学技能，增强中小学教师对网络安全素养教育的认同感和责任感。二是为中小学教师开展网络安全素养教育教学提供相应的材料支持和教学方法指导，推动教师网络安全教学水平提升。三是充分挖掘中小学网络安全素养教育领域的优秀师资，倡导其发挥模范带头作用，以点带面，逐步推进我国中小学生网络安全素养教育教学实践落地[29]。四是定期开展网络安全素养教育研讨会，帮助教师梳理学校网络安全教学中的共性难题，构建经验交流与问题解决平台。

（四）倡导社会行业组织支持参与，共创中小学生网络空间安全和谐氛围

美国社会组织机构通过资金支持、协同管理和舆论营造等手段，主动参与推进中小学生网络安全素养教育实践。借鉴美国中小学生网络安全素养教育行动经验，第一，我国应充分激发社会行业组织的主动参与意识，使其树立合作共赢理念，积极协助学校营造安全和谐的网络空间环境，为推动我国实现网络强国和教育强国献策献力；第二，形成多元化网络安全素养教育投入格局，引导、督促行业机构和公益组织加大对中小学生网络安全素养教育的投入与资助力度，构建起政府、社会和学校相互补充、相互促进的网络安全素养教育资金投入模式；第三，鼓励社会多元力量发挥自身特色与行业优势，围绕中小学生网络安全素养教育的核心要义、重点工作和战略部署，开展多视角、多途径、多领域战略合作，助力我国中小学生网络安全素养教育工作顺利和有效实施。

参考文献：

[1] 祝智庭，彭红超．创新发展技术赋能的智慧教育——访我国智慧教育开拓者祝智庭教授[J]．教师教育学报，2021(4)：21-29.

[2] 共青团中央维护青少年权益部，中国互联网络信息中心．2019年全国未成年人互联网使用情况研究报告[EB/OL]．(2020-05-13)[2022-11-29]．http://www.cnnic.cn/n4/2022/0401/c116-1117.html.

[3] 王正青．大数据时代美国学生数据隐私保护立法与治理体系[J]．比较教育研究，2016(11)：28-33.

[4] National Forum on Education Statistics. Forum guide to cybersecurity: safeguarding your data[EB/OL]. (2020-10-21)[2022-11-29]. https://nces.ed.gov/pubs2020/NFES2020137.pdf.

[5] REMS TA Center. Cybersecurity considerations for k-12 schools and school districts[EB/OL]. (2017)[2022-11-29]. https://rems.ed.gov/docs/Cybersecurity_K-12_Fact_Sheet_508C.PDF.

[6] United States Government Accountability Office. Recent K-12 data breaches show that students are vulnerable to harm[EB/OL]. (2020-09)[2022-11-29]. https://www.gao.gov/assets/gao-20-644.pdf.

[7] HERNANZEZ S. Cyber security in state and local educational agencies[EB/OL]. (2019-07-23)[2022-11-29]. https://nces.ed.gov/forum/pdf/S2019_Cybersecurity.pdf.

[8] The K-12 C Cybersecurity Resource Center. The state of k12 cybersecurity[EB/OL]. (2020-03)[2022-11-29]. https://k12cybersecure.com/wp-content/uploads/2020/03/K12Cybersecurity2019YearinReview.pdf.

[9] EdWeek Research Center. The state of cybersecurity education in k12 Schools[EB/OL]. (2020-06-23)[2022-11-29]. https://cyber.org/news/state-cybersecurity-education-k-12-schools.

[10] National Cyber Security Alliance. 16th Annual National Cybersecurity Awareness Month begins today[EB/OL]. (2019-11-17)[2022-11-29]. https://staysafeonline.org/press-release/16th-annual-national-cybersecurity-awareness-month-begins-today/.

[11] ELLEDGE K. 3 steps for teaching cybersecurity in the classroom[EB/OL]. (2020-07-28)[2022-11-29]. https://cyber.org/news/3-steps-teaching-cybersecurity-classroom.

[12] State of Wisconsin Department of Administration. State of Wisconsin strategic IT plan 2022-2024[EB/OL]. (2021)[2022-11-29]. https://det.wi.gov/Documents/StrategicITPlan2022.pdf.

[13] Virginia Department of Education. New cybersecurity career pathway courses offered beginning fall 2017[EB/OL]. (2017)[2022-11-29]. https://www.doe.virginia.gov/instruction/career_technical/cybersecurity/cyber-courses-2017.pdf.

[14] Alaska Department of Education and Early Development. Cybersecurity awareness kids safe online[EB/OL]. (2017)[2022-11-29]. https://www.cisecurity.org/wp-content/uploads/2017/07/2018-Contest-Guide.pdf? x60581.

[15] CyberStart America. The cyberstart America program is our most advanced[EB/OL]. (2018)[2022-11-29]. https://www.cyberstartamerica.org/history/.

[16] Boston Tech Mom. Learning cybersecurity: competitions and workshops forteens[EB/OL]. (2020-11-14)[2022-11-29]. https://cyber.org/news/learning-cybersecurity-

competitions-and-workshops-teens.

[17] Virginia Department of Education. Virginia's 21st century career pathway cybersecurity[EB/OL]. (2016)[2022-11-29]. https://www.doe.virginia.gov/administrators/superintendents_memos/2016/040-16a.pdf.

[18] Virginia Department of Education. Virginia cybercamp 2016[EB/OL]. (2016)[2022-11-29]. https://www.doe.virginia.gov/instruction/career_technical/cybersecurity/cybercamp-report.pdf.

[19] National Institute of Standards and Technology. National initiative for cybersecurity education(NICE)cybersecurity workforce framework[EB/OL]. (2020-11-13)[2022-11-29]. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.

[20] Cyber Security and Information Assurance Interagency Working Group. Federal cybersecurity research and development strategic plan[EB/OL]. (2019-12)[2022-11-29]. https://www.nitrd.gov/pubs/Federal-Cybersecurity-RD-Strategic-Plan-2019.pdf.

[21] National Initiative for Cybersecurity Careers and Studies. Cybersecurity in the classroom[EB/OL]. (2019)[2022-11-29]. https://niccs.cisa.gov/formal-education/integrating-cybersecurity-classroom#wcm-survey-target-id.

[22] U.S. Department of Education. Education Department announces Ohio and California teachers as 2022 presidential cybersecurity education awardees[EB/OL]. (2022-11-17)[2022-11-29]. https://www.ed.gov/news/press-releases/education-department-announces-ohio-and-california-teachers-2022-presidential-cybersecurity-education-awardees.

[23] U.S. Senate Committee Homeland Security and Governmental Affairs. Peters,Scott introduce bipartisan legislation to protect k-12 school systems from cyber-attacks[EB/OL]. (2019-11-26)[2022-11-29]. https://www.hsgac.senate.gov/media/minority-media/peters-scott-introduce-bipartisan-legislation-to-protect-k-12-school-systems-from-cyber-attacks.

[24] National Science Foundation. Cyber security education,curriculum,and workforce development[EB/OL]. (2012-07-02)[2022-11-29]. https://www.nsf.gov/awardsearch/showAward?AWD_ID=1204904.

[25] Office of Procurement Operations Grants Division. National cybersecurity awareness program[EB/OL]. (2014-07-24)[2022-11-29]. https://www.federalgrants.com/National-Cybersecurity-Awareness-Program-47280.html.

[26] Michigan Department of Education. Michigan Department of Education memo[EB/OL]. (2017-09-14)[2022-11-29]. https://www.michigan.gov/documents/mde/Cybersecurity_Grant_600569_7.pdf.

[27] 王正青,唐晓玲. 信息技术与教学深度融合的动力逻辑与推进路径研究[J]. 电化教育研究,2017(1):94-100.

[28] LEVIN D. K-12 cybersecurity lessons learned from 'constant barrage ofattacks'[EB/OL]. (2019-03-19)[2022-11-29]. https://www.edweek.org/technology/k-12-cybersecurity-lessons-learned-from-constant-barrage-of-attacks/2019/03.

[29] 沈小碚,樊晓燕. 智慧教育背景下教师专业发展面临的挑战与机遇[J]. 教师教育学报,2020(1):33-39.

The Practice Strategy and Guarantee Mechanism of Cultivating Primary and Secondary Students' Cyber Security Literacy in the US

WANG Zhengqing,CHENG Tao

(*Faculty of Education,Southwest University,Chongqing* 400715,*China*)

Abstract:Cyber security literacy education for primary and secondary students aims to ensure that students acquire basic knowledge of cyber security and equip themselves with cyber security self-protection ability. As the leading country of educational informatization development,the United States formulates practical strategies for cyber security literacy education for primary and secondary students against the realistic background of frequent cyber security incidents,including creating cyber security culture atmosphere to consolidate students' cyber security awareness,setting up cyber security courses to build a solid foundation of cyber security knowledge,carrying out cyber security competitions to build cyber risk defense capability,and launching cyber security camps to enrich cyber protection experience. Ameirica guarantees cyber security literacy education for primary and secondary school students through policy speicifications,teacher training,experience exchange and financial support. Learning from the experience of the United States in cultivating the cyber security literacy of primary and secondary school students,China can improve the cyber security literacy education system of primary and secondary school students by promoting the construction of cyber security education regime,coordinating the deployment of education resources,increasing the training of teachers' information literacy,and advocating the support of social organizations.

Key words:the United States of America;primary and secondary students;key competencies;cybersecurity literacy;cyber security curriculum

责任编辑　邓香蓉