

数字智能:面向未来的核心能力新要素*

——基于《2020 儿童在线安全指数》的数据分析与建议

祝智庭¹, 徐欢云², 胡小勇²

(1.华东师范大学 开放教育学院, 上海 200062;

2.华南师范大学 教育信息技术学院, 广东 广州 510631)

[摘 要]“网络大疫情”安全风波使得人类对发展“数字智能”空前重视。文章首先阐述数字智能的概念、标准框架与关键特征。接着,利用“儿童在线安全指数”(COSI)国际评估项目数据,以在线安全指数排名前十的国家为研究分析样本,揭示各国在儿童在线安全方面的现状与关键问题,确定我国儿童在线安全的相对风险与防护薄弱之处。研究结果表明:数字智能、数字技术使用自控力、网络风险可作为儿童在线安全指数的三个关键性预测维度;社会基础设施、家校指导与教育是制约儿童在线安全水平的两个重要薄弱领域,各国在指导与教育、社会性基础设施投入上严重欠缺。儿童的数字智能素养在屏幕时间管理、网络欺凌管理、隐私管理、数字公民身份等方面表现较好,在网络安全管理、数字同理心、数字足迹管理和批判性思维上属于薄弱环节。最后,从顶层设计、环境支撑、教研引领、效果评估等方面,提出了我国数字智能教育发展的策略性建议。

[关键词] 数字智能; 在线安全; 新冠疫情; 核心素养; 网络欺凌

[中图分类号] G434

[文献标志码] A

[作者简介] 祝智庭(1949—),男,浙江衢州人。教授,主要从事教育信息化系统架构与技术标准、信息化促进教学变革与创新、技术使能的智慧教育、面向信息化的教师能力发展、技术文化等方面的研究。E-mail:ztzhu@dec.ecnu.edu.cn。胡小勇为通讯作者,E-mail:huxiaoy@senu.edu.cn。

一、网络疫情大爆发引发数字智能新关注

“互联网+”浪潮,刺激了数字原住民群体数量的持续增长,“数字智能”正成为人们有效建设和参与数字智能社会的新需求。《2018 年度全球移动互联网市场报告》^[1]显示:2018 年年底,全球互联网用户达到 43 亿人,约占全球人口 57%,全球超过一半人口已连接互联网。《第 45 次中国互联网络发展状况统计报告 2020》^[2]显示:截至 2020 年 3 月,我国网民数量为 9.04 亿,手机网民有 8.97 亿。其中,10 岁以下网民占 3.9%,10~19 岁网民占 19.3%,20~29 岁网民占 21.5%,且人均

每周上网时长为 30.8 小时。然而,人类在赢来数字技术发展“红利”之时,“网络大疫情”风波悄然来临。2018 年数字智能研究报告显示^[3]:在 29 个国家及地区的 8~12 岁被调查者中,有 56%经历网络欺凌、数字游戏成瘾、在线色情行为,全球有 2.6 亿儿童可能陷入网络风险,且在预估 2020 年的 7.2 亿 8~12 岁网民中,3.9 亿儿童将卷入网络风险。相比 ICT 发达国家,ICT 新兴国家儿童遭遇网络风险的可能性高达 1.3 倍。

有研究表明,数字智能与儿童在线风险行为休戚相关。数字智能提高到平均分 100 分时,共享个人数据及信息风险降低 17%,线上意外交流聚会风险下降

基金项目:国家社会科学基金教育学一般课题“面向‘互联网+’的教师教研形态转型与变革研究”(课题编号:BCA180094);广东省教师教育在线开放课程“人工智能教育应用”(项目编号:8A006412)

* 本文系根据祝智庭教授 2020 年 4 月 30 日所作报告内容整理而成,胡小勇教授团队梳理和充实了内容。

6%,在线色情干扰和在线暴力内容风险分别下降 12% 和 24%,网络欺凌和网络游戏成瘾分别下降 40% 和 5%^[4]。鉴于此,在国际经济论坛(又称达沃斯论坛)的框架内组建了一个国际研究机构“数字智能研究院”(DQ Institute),2018 年首发的重量级研究报告《智胜网络大疫情:2020 年,数字智能为每个孩子赋能》(Outsmart the Cyber-Pandemic: Empower Every Child with Digital Intelligence by 2020)提出“以数字智能作为抵御网络大疫情的疫苗,给每个孩子赋能,使他们到 2020 年拥有数字智能”的号召,并发起“DQEveryChild”全球性运动,通过帮助发展世界各地儿童的数字智能,实现儿童网络风险最小化和发展机会最大化,拥有在数字化世界人人成功的平等机会。本文通过阐明数字智能作为未来人才核心能力新要素的内涵,引介国际数字智能全球标准框架及其数字智能教育实施现状,并提出未来数字智能教育发展趋势与策略建议,推动未来国内研究者从更多不同视角来探索数字智能教育的理论与实践。

二、数字智能:面向未来的核心素养新要素

数字智能是与智商、情商一脉相承的新一代人类智能发展形态,最初是由朴圭贤博士(Park, Y.)研究团队在 2016 年世界经济论坛发表的学术文章中正式提出并受到广泛关注。2018 年,世界经济论坛发布《忘掉智商吧,未来数字智能更重要》报告,在“数字世界之六大行动”中明确提出“培养数字公民的‘数字智能’(Digital Intelligence,简称 DI)成为世界各国教育的紧迫使命”。随后,经济合作与发展组织(OECD)、IEEE 标准协会、数字智商研究院(DQ Institute)与世界经济论坛联合成立“数字智能联盟”(CDI),推动数字智能概念及数字智能教育行动走向世界,其研究成果“数字智能全球通用框架”被世界各国政府、学校教育者、技术公司和服务提供商采用。

(一)数字智能的兴起:从 IQ 到 DQ^[5]

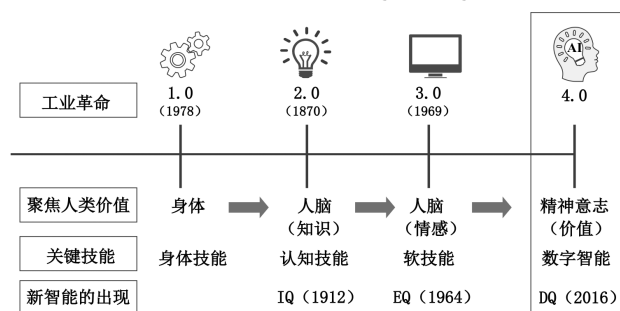


图 1 IQ、EQ、DQ 的演化发展示意图

伴随着每一次工业革命产生的经济及社会系统结构性变革,人类的关注焦点随之转移。第一次工业革命和第二次工业革命实现了以高效率规模化生产为目标的机械化进程,人的核心能力体现为身体技能,并日益强调知识和技能的人脑价值优势,用于测量知识和认知技能的智商(智能商值, Intelligence Quotient, 简称 IQ)诞生,使得学校教育系统致力于培养知识工作者。第三次工业革命,电子化设备和互联网改变了人类的交互、工作和生活方式,人的核心能力由知识转向情感管理和关系构建,强调同理心、自我感知、关系管理等软技能的“情商”(情感智能商值, Emotional Intelligence Quotient, 简称 EQ)诞生。第四次工业革命促发了人工智能部分替代人类脑力劳动的新变革,使得 4 年内全球超过 7500 万个工作岗位变得无足轻重,同时带来 133 万个新兴工作岗位的发展新机遇,迎来自动化和数字创新的“数商”(数字智能商值, Digital Intelligence Quotient, 简称 DQ)新时代。数字智能作为融合身体性技能、认知性技能、情感性技能,体现智慧和普适价值观的新一代核心能力要素,使个体成为具有终身学习能力的技术价值主导者和创造者。

(二)数字智能的内涵阐述

1. 数字智能的八大维度

维度 层级	数字身份	数字使用	数字安全	数字安防	数字情感智能	数字通讯	数字素养	数字权利
数字公民身份	数字公民	平衡使用技术	行为网络风险管理	个人网络安全管理	数字同理心	数字足迹管理	媒体和信息素养	隐私管理
数字创造力	数字创作者	健康使用技术	内容网络风险管理	公共网络安全管理	自我意识管理	在线交流与合作	内容创建和计算素养	知识产权管理
数字竞争力	数字变革者	数字参与	商业和社区网络风险管理	组织网络安全管理	关系管理	公共和大众传播	数据和 AI 素养	参与权管理

图 2 数字智能(DQ)的 24 项能力^[5]

宏观层面,数字智能由八个维度构成,具体包括^[5](如图2所示):其一,数字身份(Digital Identity),创建并保持健康的线上线下身份一致性,分为数字公民、数字共同创作者、数字变革者。如:管理在线声誉,认识自我在线角色及长短期在线状态影响。其二,数字使用(Digital Use),平衡、健康和文明地使用技术,对自身行为负责。个体可自我掌控并平衡切换在线和离线状态。其三,数字安全(Digital Safety),个体安全和有道德地使用技术,理解、缓和及管理网络风险,理性应对网络行为风险管理、网络内容风险管理、网络商业和社区风险管理;运用技术恰当管理网络欺凌、伪装、暴力等在线风险,避免或缓解网络暴力和在线色情行为风险。其四,数字安防(Digital Security),探测和管理数据、设备、网络系统免受网络威胁,通过个人网络安全管理、组织网络安全管理,检测黑客攻击、诈骗和恶意软件,并使用合适安全技术工具保护数据。其五,数字情感智能(Digital Emotional Intelligence),认识、引导和表达个体内外部数字交互过程中的情感状态,包括数字同理心、自我意识管理、关系管理,即个体运用同理心与在线其他人建立良好关系。其六,数字通讯(Digital Communication),运用数字技术与他人交流和协作,分为数字足迹管理、在线交流与合作、公共与大众传播。其七,数字素养(Digital Literacy),寻找、阅读、评价、分析、创造、适应和分享信息与技术媒介,包括媒体和信息素养、内容创建和计算素养、数据和AI素养。其八,数字权利(Digital Rights),使用技术理解和维护正当权益,包括隐私管理、知识产权管理、参与权管理等。

2. 数字智能的三大层次

微观层面,数字智能具有层次性,由二十四项具体内容构成三大层次。

数字公民身份是数字智能发展的第一层级,个体以一种安全、负责和道德的方式使用数字技术。作为一套基本数字生活技能,象征数字时代对基本人权的保障,政府、社会及学校需为个体免费平等地提供获得该层级数字智能的教育机会,包括数字公民、平衡使用技术、网络行为风险管理、网络个人安全管理、数字同理心、数字足迹管理、媒体和信息素养、隐私管理等八个方面。如创建和管理在线身份以塑造数字形象;管控屏幕和数字媒体设备使用时间,以平衡处理多任务及线上线下生活;运用技术、社会认知和决策,来防范和管理网络欺凌;使用安全策略和保护工具应对个人数据和设备的黑客攻击、诈骗和恶意软件入侵;在同步或异步互动中理解并表达对他人的需求

的关注与同理心;积极管理平台间共享和标记的个人或他人信息,树立良好数字声誉;批判性组织、分析和评价媒体及信息;谨慎保护线上个人及他人隐私信息等。

数字创造力是数字智能发展的第二层级,涵盖更高级的数字技能素养和未来准备就绪能力,包括成为数字共同创作者、健康使用技术、网络内容风险管理、网络安全管理、自我意识和管理、在线交流与合作、内容创建和计算素养、知识产权管理等8个方面,是个体充分融入数字生态系统的象征,标志个体通过创造新知识和技术将创意转化为产品,创造经济和社会价值。如利用技术发展高层次思维和共创知识服务;以积极、健康方式使用技术;妥善处理网上不良内容信息,积极建设健康、开放和支持型的在线社区;预测并处理数字环境中的数据、设备和系统威胁;认识数字化生存发展价值体系;有效利用技术开展远程交流及协作;创新性生产信息、知识及媒体技术,促进终身学习和自身技能发展;使用和创建内容过程中正确处理知识产权等。

数字竞争力是数字智能发展的第三层级,标志个体具备解决全球危机的潜在能力,并作为数字经济的成员,在推动创业和刺激经济增长方面发挥有效作用。具体包括个体成为数字变革者、文明使用技术、网络商业和社区风险管理、网络组织安全管理、关系管理、公共和大众传播、数据和AI素养、参与权管理等8个方面。如评估和利用数字红利,参与地方、国家及全球性人类福祉事务;抵御和处理在线商业或社区网络风险;实施组织网络安全防御和改善组织网络安全系统;有效管理在线社交关系;与在线参与者广泛高效开展社会性会话;利用数据生成、分析并呈现有意义信息,开发、使用人工智能技术来优化学习工作绩效;正确理解和行使个人数据保护、言论自由等在线参与权等。

(三)数字智能的特征分析

1. 彰显包容性和通用性的发展理念

在概念及内容上,数字智能有一套通用语言、系统结构和分类法,其通用标准框架融合全球25个区域及国际性组织发布的领先技能框架,数字素养、数字技能、21世纪技能框架等众多关键技能被映射到DQ框架,体现兼容并蓄,博采众长。如欧洲公民数字能力框架、美国ISTE学生标准、荷兰国际计算机与信息素养研究、欧盟EntreeComp创业能力框架、英国《互联世界的教育:为儿童和年轻人适应数字生活的框架》、世界经济合作组织的《成人能力国际评估项

目》、联合国教科文组织《全球媒体和信息素养评估框架:国家就绪准备和能力》等。同时,数字智能全球标准框架被世界各国广泛接受。DQ 框架的协同创建者涉及数字智能研究院(DQ Institute)、电气和电子工程师标准协会(IEEE SA)、世界经济论坛(WEF)和世界经济合作与发展组织(OECD)等多个国际性组织,清晰高效的定位角色推动数字智能标准框架推广应用以及持续更新。

2. 以培养未来人才核心能力为方向标

数字智能的八个核心维度聚焦学习者获取相应的知识、技能和形成价值观,关照应对网络风险危机与困境、在线行为的责任担当、创造数字经济的新价值等三种未来人才发展核心能力,蕴含可持续、适应力、创新的发展理念,为保障人类安全、社会经济增长和实现幸福发展奠定坚实基础(如图 3 所示)。此外,数字智能将“教育 2030 框架”(the OECD Education 2030 Framework)中的创造新价值、排危解难和担当责任等关键变革性能力,以及《2018 年度未来职业报告》中适应 2022 年的未来人才竞争力框架相关联,形成三者能力间的映射关系,充分反映不同层级的数字智能对提升变革性能力和未来职业发展技能的影响及差异化目标需求,成为通达人类幸福的奠基石。

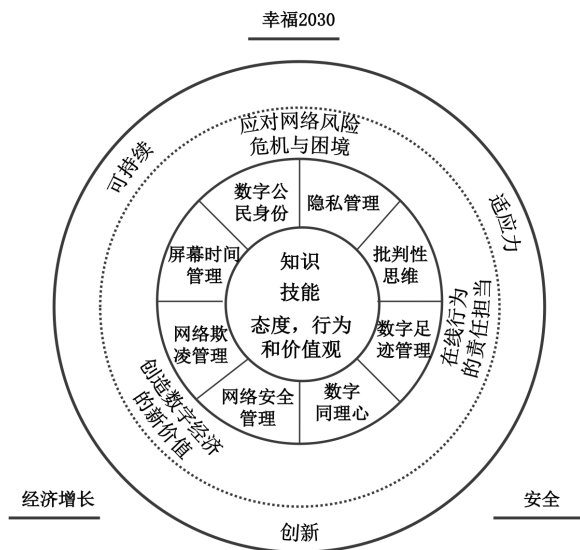


图 3 DQ 框架与未来学习 2030 框架关系图^⑥

三、数字智能教育的国际评估及实践案例

#DQEveryChild 作为一项帮助 8~12 岁儿童发展数字智能的全球战略性行动,致力于研究帮助儿童提高数字适应力的解决方案,世界 80 多个国家参与其中。“儿童在线安全指数”(COSI)是结合数字智能框架监测世界各国儿童数字智能和在线安全水平的大型

国际评估项目,本文以此为例介绍国际儿童数字智能评估及数字智能教育发展趋势。

(一)数字智能教育的国际评估项目:国际儿童在线安全指数

国际儿童在线安全指数由三大指导性结构、六大支柱、二十四项内容构成(如图 4 所示),是数字智能通用框架在 8~12 岁儿童群体的具体实践应用。三大指导性结构包括:(1)智慧使用,包括网络风险和技术使用自控力,涵盖网络欺凌、滥用技术、危险内容、风险联系、网络威胁、名誉风险、超长时间使用屏幕、社交及电子游戏活动、移动技术应用普及等九项内容。(2)赋能,包括数字技能、指导与教育,涵盖数字技能、家庭引导和学校在线安全教育等具体内容。(3)基础设施,包括社会性基础设施和数字网络世界的连通性,涵盖在线安全法律框架、网络安全基础架构、社会行业参与、互联网访问可及性与连接速度等内容。

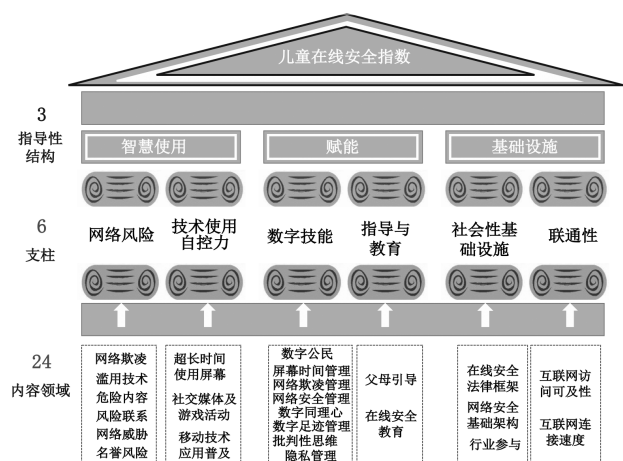


图 4 儿童在线安全指数评估框架^⑦

(二)数字智能及在线安全的国际评估项目: COSI 2020 年国际儿童在线安全指数调查,基于 2017—2019 年接受 #DQ EveryChild 组织邀请的 30 个国家,共计 145426 名儿童为研究对象,以儿童在线安全指数为测评工具(如图 4 所示),系统了解世界儿童在线安全及数字公民身份实况。

为探索有效推进数字智能教育的实施策略,本文根据 DQ 研究院网站的实时更新测评数据,从 30 个被调查国家中选取儿童在线安全指数排名前 10 的国家数据为分析样本(见表 1)。

表 1 涵盖西班牙、澳大利亚、新加坡、韩国、意大利和日本六个发达国家,以及马来西亚、土耳其、印度、中国四个发展中国家,覆盖面较为合理,通过比较网络风险、数字技术使用自控力、数字技能、指导与教育、社会基础设施、连通性等 6 个核心领域,综合分析

国际儿童数字智能发展及在线安全的优势及问题。

表1 国际儿童在线安全指数总体比较一览表

比较维度 国际排名		网络 风险	数字技 术使用 自控力	数字 技能	指导与 教育	社会基 础设施	连通 性
1	西班牙	3	5	18	4	8	7
2	澳大利亚	11	11	6	15	3	4
3	马来西亚	10	13	2	7	7	15
4	新加坡	12	6	7	11	19	1
5	韩国	6	3	4	25	6	2
6	意大利	5	19	11	13	4	11
7	日本	1	1	5	26	9	13
8	土耳其	25	8	9	12	13	9
9	印度	2	4	1	2	11	28
10	中国	13	10	8	24	21	8

1. 网络风险

国家排名与所在国家儿童遭遇网络风险呈反比,即排名越靠前,儿童网络风险程度越低。数据分析显示:发达国家儿童面临的网络风险相对更低,日本、西班牙、韩国、意大利在儿童网络风险防控上表现优异。此外,印度在儿童网络风险防控绩效上表现突出。从具体指标看,其一,发达国家在网络风险的六项子指标表现水平总体优于发展中国家。日本和西班牙在网络欺凌、技术的无序使用、危险内容、风险联系、网络威胁、名誉风险等方面处于领先水平,表现为儿童网络风险防控能力强、安全状态好。土耳其和中国的儿童的网络风险程度较高。其二,各国在六项子指标上表现差异较大,解决儿童在线安全的具体途径应各有侧重。如澳大利亚儿童需重点防控网络欺凌和危险内容;韩国需优先防控网络钓鱼和黑客攻击等网络威胁;意大利可重点提升儿童的危险内容和风险联系防控能力;中国在网络欺凌、技术无序使用、网络威胁和名誉风险等方面均位于世界平均水平底端,均需作为优先管理事项。

2. 数字技术使用自控力

国家排名与所在国家儿童数字技术使用自控力成正比,即排名越靠前,儿童数字技术使用自控能力表现越好。相比发展中国家,发达国家儿童的数字技术使用自控性更高,如日本、韩国、西班牙、新加坡等国儿童的数字技术使用自控力较强(另外,这种情况还包括发展中国家印度),土耳其、中国、马来西亚等国儿童表现一般。从具体指标看,其一,发达国家儿童的屏幕使用时间超长现象更为明显。意大利、新加坡、澳大利亚等国每周屏幕使用时间超过40小时的儿童

比例更高,需重视调节干预儿童屏幕使用时间。其二,发展中国家儿童的高频社交媒体及数字游戏活动成瘾现象更为严重。意大利和中国需要重点关注儿童在高频社交媒体使用及数字游戏的干预支持服务。其三,发达国家儿童的移动技术拥有率与依赖性更高,如意大利、西班牙、澳大利亚等国需采用智能设备应用管控干预服务来保障儿童在线安全。

3. 数字智能

国家排名与所在国家儿童数字智能成正比,即排名越靠前,儿童的数字智能越高。整体来看,发展中国家儿童的数字智能居中等偏上水平,印度和马来西亚两国儿童的数字智能水平位居领先地位,中国和土耳其居中等偏上水平。发达国家儿童的数字智能居整体水平前列,韩国、日本、新加坡三国表现优异,西班牙表现在中等偏下水平。从具体指标看,其一,发展中国家儿童构建和管理数字公民身份表现更优异。印度、中国、马来西亚等国儿童在保持线上线下身份一致性、数字媒体技术与知识、在线自我效能感等方面优势明显。其二,发达国家儿童的网络欺凌管理技能整体优于发展中国家。中国和土耳其等发展中国家需帮助儿童提高网络欺凌风险的处理技能。其三,发展中国家儿童的网络安全管理技能整体强于发达国家,马来西亚、印度、中国儿童居于前三位。其四,发展中国家的儿童数字同理心表现整体优于发达国家。日本、西班牙和中国需引导儿童形成数字同理心态度和行为。其五,各国儿童的数字足迹管理和批判性思维技能均需改善提升。西班牙儿童数字足迹管理技能远低于世界平均水平,西班牙和土耳其等国儿童批判性思维技能远低于世界平均水平,韩国、日本、中国等国儿童的数字足迹管理和批判性思维技能均处于世界平均水平左右。其六,发展中国家的儿童隐私管理技能整体优于发达国家,意大利、土耳其、韩国需提升儿童在线个人信息及知识共享等技能。

4. 指导与教育

国家排名与所在国家儿童获得在线安全指导教育支持力度呈正比,即排名越靠前,儿童获得父母数字媒体使用引导和学校提供的在线安全教育服务越多。各国具有一定层次性差异,整体表现不尽人意,印度、西班牙和马来西亚在儿童在线数字化安全指导上的投入和绩效相对较好,新加坡、土耳其、意大利和澳大利亚处于世界平均水平左右,韩国、日本和中国远远低于世界平均水平,说明各国都需重视并加强家校协同,增强父母对儿童数字媒体使用的积极指导,提高学校为儿童提供在线安全教育的学习支持服务。

5. 社会性基础设施

国家排名与所在国家儿童获得在线安全保障的社会性基础设施支持力度成正比,即排名越靠前,儿童在国家立法维权、网络安全基础架构及社会各行业参与度上获得支持服务越多。发达国家整体水平位居世界前列,且差异程度不大;发展中国家整体处于世界平均水平,中国需注重改善社会基础设施。从具体指标看,各国的网络安全基础架构相对最好;国家儿童在线安全的立法维权框架亟待改善;发达国家在儿童在线安全的社会行业参与度高于发展中国家。其中,新加坡、土耳其、中国、日本、韩国等均需重视并加强对儿童在线安全的立法维权行动。西班牙、新加坡、澳大利亚、日本和韩国在儿童在线安全的网络基础架构上体现优势,印度、中国、意大利等国均需注重设计并实施促进网络安全基础建设的整体架构及行动方案。日本、澳大利亚、韩国、意大利等发达国家的社会行业在促进儿童在线安全及数字智能上的投入绩效出色,新加坡、西班牙、中国、印度等国需提升行业参与积极性。

6. 连通性

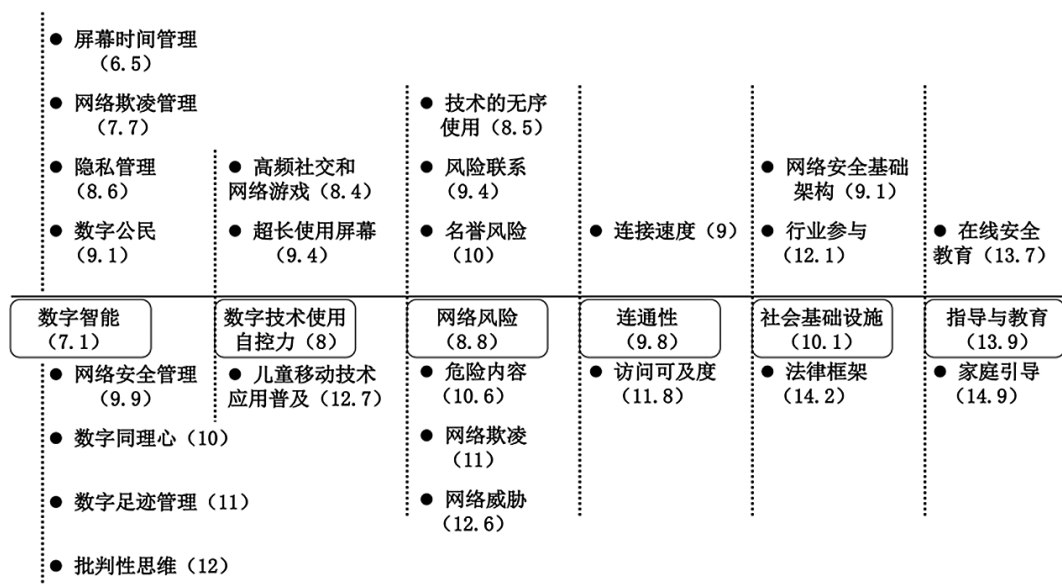
国家排名与所在国家儿童获得在线连通性服务支持力度成正比,即排名越靠前,儿童在获得互联网优质访问服务和快捷访问速度上的支持越好。发达国家整体水平位居世界前列,但存在一定差异,新加坡、韩国、澳大利亚等国居于世界领先水平,意大利和日本居于世界平均水平前列。发展中国家表现相对落后且差异明显,印度亟须将连通性作为提高儿童在线安全指数的优先建设事项。具体来看,发达国家的互联

网优质在线访问服务居于世界前列,印度、土耳其、马来西亚和中国需着重优化儿童的互联网在线连接访问支持服务。同时,各国在互联网上传及下载速度方面表现较好,发达国家总体优于发展中国家。印度、马来西亚、日本等仍需在互联网连接速度上改善提升。

(三) 研究结果分析

结合整体及局部性表现,对国际儿童数字智能和在线安全现状进行归因分析,总结在线安全指数中六大核心维度的发展走向,分析各项内容指标的重要层级,综合预测数字智能教育发展趋势。其中,网络风险、数字技术使用自控力、数字智能、指导与教育、社会基础设施、连通性六个核心维度的整体概况以及内容指标的局部表现,均采用相应平均排名高低来评估(如图5所示)。排名靠前的维度及内容指标发展越好,对在线安全防控效果的预测力更强;反之,属于儿童安全防控的薄弱环节,需列为优先重点改进事项。

由图5可知,在线安全指数的六大维度中,发展程度由高到低依次为数字智能、数字技术使用自控力、网络风险、连通性、社会基础设施、指导与教育。其中,儿童的数字智能、数字技术使用自控力、抗网络风险可作为在线安全指数的三个关键预测维度。社会基础设施、指导与教育是制约儿童在线安全水平的两个重要薄弱领域,世界各国在指导与教育、社会性基础设施上投入欠缺,需调动家庭、学校、法律制度、社会行业来推动儿童数字智能教育和改善在线安全状态。连通性对在线安全指数具有重要影响,近年来新兴ICT国家在教育技术基础设施建设上已见成效,为儿童在线安全提供了良好的条件保障。



注:维度/(排名平均数)

图5 国际儿童在线安全指数各维度及内容指标项平均排名

从局部发展看,在数字智能维度,儿童在屏幕时间管理、网络欺凌管理、隐私管理、数字公民身份等方面表现较好,但网络安全管理、数字同理心、数字足迹管理和批判性思维属于薄弱环节。在数字技术使用自控力维度,儿童在参与高频社交和网络游戏活动、屏幕使用时长的自控力较好,但儿童的移动技术拥有率值得跟踪关注,需防止儿童网络成瘾以保证在线身心健康。在网络风险维度,儿童在技术无序使用、风险联系等在线安全防护能力较好,网络欺凌、网络威胁和危险内容是制约其在线安全的薄弱环节,如何通过伦理道德制度、技术监控和教育活动来增强儿童网络欺凌和网络威胁等在线防疫能力,可作为数字智能教育的优先行动计划。在连通性维度,互联网访问可及性及速度均处于中等偏上水平,访问可及性仍需改进。在社会基础设施维度,社会行业参与度低,关于儿童在线安全方面的法律框架及制度未能及时跟上,这与数字世界的行为规范和准则尚处于萌芽状态的已有研究观点基本一致^[8]。在指导与教育维度,学校和儿童家庭的在线安全教育支持严重缺失,学校如何将在线安全教育渗透到学校课程及校外活动,设计和开发高质量的网络健康安全学习资源和实践技术环境,如何保障将数字智能融入家校协同、亲子交流互动的非正式学习情境,可作为数字智能教育和在线安全教育的重要研究问题。

四、推动我国数字智能教育的发展建议

已有研究表明,完善的数字公民教育研究与实践可促进信息技术与教育的深度融合,推动教育公平和均衡发展^[9]。新冠疫情促逼师生全面开展线上教与学,教育信息化2.0时代要实现网络学习空间大规模普及应用,数字智能成为中小学生高效适应数字化学习和生活的关键。如何开展数字智能教育来提高未成年人的数字化生存力和核心能力,成为未来“AI 赋能教与学”的重要研究主题。

(一)顶层设计:数字智能教育发展的整体战略

教育系统可视为由自顶向下的道、法、术、器四个层面构成,以此审视教育发展的不同阶段和形态。人工智能教育、智慧教育、数字智能教育均体现数字技术支持下的教育不同形态及特点,合理分析数字智能教育与人工智能教育、智慧教育之间的关联与差异,使其充分融入我国智能教育与智慧教育的框架(如图6所示)。具体来说,人工智能教育和数字智能教育是采用自底向上的方法发展,由“器”逐步融入“道”的过程,不同的是,人工智能教育是面向机器;数字智能是

面向人,重在人类的新智能的发展。

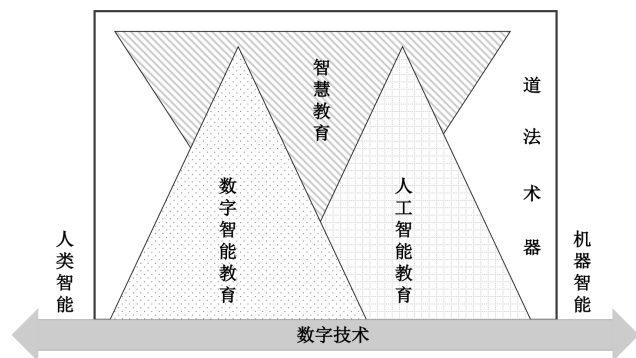


图6 融合数字技术的教育系统分析框架

智慧教育则是更加上位的一个概念,是理想的未来教育范式,从“道”出发,采用自顶向下的方法发展,从“道”和“法”的高度引领“术”和“器”的发展方向。

与此同时,借鉴以政策、学术研究、相关产业、学校领导力、教师专业发展、教育实践为关键要素的教育信息化生态系统观^[10],基于教育生态理念设计数字智能教育整体发展战略。政策上,通过实施在线安全政策营造“道德数字生态系统”。如国家从互联网接入点、网络、家庭数字文化、学校教育、ICT 社会行业参与对数字生态系统建设提供政策支持;建立对不同群体在线安全的立法维权框架,设计针对不同群体在数字公民身份、屏幕使用时间、网络欺凌管理、网络安全管理、数字同理心、数字足迹管理、批判性思维、隐私管理等方面的教育管理制度。学术研究上,目前数字智能教育局限于数字公民教育,且存在基础理论研究薄弱、高质量数字公民教育资源有效供给严重不足、相关课程体系缺乏、家—校—社协同力量微弱等问题^[8]。从针对不同群体的数字智能素养调查,数字智能教育理论体系构建,数字智能教育的课程设计与资源开发,数字智能教育的方法、路径和模式等推进研究实践。社会产业参与上,激励社会企业参与数字智能教育相关的应用产品开发和公益教育服务活动。学校领导力上,学校管理者紧跟国内外数字智能教育发展前沿,推进数字技术支持的智能化教育基础设施建设,组织青年骨干教师建立数字智能教育实践探究团队和开展在线安全教育。在教师专业能力上,教师通过培训、自主学习、同伴教研等方式主动掌握数字智能的关键知识和技能,探索数字智能教育的学科融合教学或综合性跨学科教学模式。在教育实践上,理清政府、企业、学术研究者、社区、学校、家庭等教育利益相关者在数字智能教育中的角色,构建多方协同的数字智能教育协作共同体,开展多层次的数字智能教育实践。

(二)环境支撑:服务数字智能教育的技术赋能

通过数字智能教育专业化支持服务平台和数字智能评估监测服务,提高数字智能教育实践效能。各国在实施数字公民教育常遇到如下瓶颈:缺乏综合性数字公民课程;教师在该领域的主题专业知识有限;难以实施有效评估和反馈机制。鉴于此,国际数字智能研究院搭建 DQ World 在线平台,并联合世界各国开展 DQEveryChild 运动来建立健康、安全的网络支持服务,以简单、快速的一站式解决方案支持各国基础教育系统开展高质量的数字智能教育。其特色表现为:(1)在线平台 DQWorld 为学习者提供 8 天的电子化数字智能课程,儿童在父母和教师支持下自主学习数字智能的 8 类核心知识和技能。(2)获取数字智能知识和技能的实时反馈和评估报告。儿童完成数字智能课程的每项技能后,其家长、学校可通过 DQ 积分卡和技能报告,获取数字技能、个人优势、平衡使用技术和媒体、网络风险潜在程度、所获指导与支持服务效能等信息,了解孩子数字智能发展进度。(3)提供数字化 DQ 育儿手册,帮助提高整个家庭的数字智能技能。

借鉴技术赋能的数字智能教育平台建设实施方案,我国可创新性引入 DQ World 数字智能在线平台,建设集自主学习和智能评估监测于一体的数字智能教育应用综合服务平台,实现全国各省域连接,汇集

形成国家级数字智能评估分析数据库,以大数据分析技术为数字智能教育营造良好的自主学习环境、教学实践环境和家—校—社协同教育环境,支持数字智能教育资源的精准建设和个性化推荐服务,推动我国数字智能教育实践的健康可持续发展。

(三)教研引领:教师胜任数字智能教育的挑战

以发展教师数字化教学创新能力,推动数字智能教育模式创新。数字智能教育需要教师自身具备深厚的数字技术知识和能力,考验教师运用数字技术创新教育教学内容和方法的数字化教学创造力。美国国际教育技术协会《国家教育技术标准》(更新版)已关注教师数字智能教育能力标准,明确提出:教师应在设计、实施和评估教学过程中有效应用和示范数字公民意识和责任;示范并传授如何安全、合法、道德地使用数字信息和技术,以及数字礼仪和社交责任;培养学生的文化理解和全球意识等^[9]。2019 年欧盟 DoCENT 组织提出“教师数字创意教学能力框架”,该框架由创造力(Creativity)、数字技术(Digital Technologies)和教学法(Pedagogy)三大关键能力要素构成,并通过相互作用衍生出创意教学法(Creative Pedagogies)、数字创造力(Digital Creativity)、数字教育(Digital Education)和数字创意教学法(Digital Creative Pedagogies)等其他四个能力要素。因此,教育部门或学校要加强教师在创意教学法、数字创造力、数字教育和数字创意教

表 2 中国儿童及青少年数字智能及在线安全状态数据一览表

数字智能 77(51,98)/8	连通性 81(50,95)/8	数字技术使用自控力 71(49,100)/10	网络风险 58(50,97)/13	社会基础设施 29(51,96)/2	指导与教育 35(52,96)/24
网络安全管理 * 88(52,93)/3	连接速度 * 91(48,98)/5	屏幕使用时间过长 * 89(51,97)/4	风险联系 87(51,99)/3	网络安全基础架构 ** 68(54,85)/14	在线安全教育 *** 48(52,98)/18
屏幕时间管理 * 89(51,97)/4	访问可及度 ** 61(50,99)/14	儿童移动技术应用普及 ** 78(50,97)/7	危险内容 ** 70(52,93)/11	行业参与 *** 16(49,98)/18	父母的引导 *** 26(49,99)/22
隐私管理 * 85(52,92)/5		高频社交和网络游戏 *** 38(46,87)/14	技术的无序使用 *** 46(51,97)/17	法律框架 *** 26(51,87)/22	
数字公民 * 85(51,96)/6			名誉风险 *** 41(51,99)/22		
数字足迹管理 ** 65(49,98)/10			网络欺凌 *** 33(50,98)/23		
网络欺凌管理 ** 65(51,97)/11			网络威胁 *** 0(51,95)/30		
批判性思维 *** 40(49,99)/18					
数字同理心 *** 28(49,99)/19					

注:* 表示指标表现优异;** 表示指标表现为平均水平,*** 表示指标表现呈危险程度。在数据集 A(C,D)/E 中,A 表示中国实际得分,C 表示世界 30 国平均分,D 表示世界 30 国最高分,E 表示中国得分排名。

学法方面的教学能力发展,使教师胜任数字智能教育实践需求。教师需了解不同阶段学习者数字智能发展的现状与特点,分析国内外数字智能教育课程、资源及相关教学实践案例,探索角色扮演的体验式学习、案例学习、混合翻转式学习、基于微视频的学习者自主学习等个性化数字智能教学实践模式。

(四)效果评估:倒逼数字智能教育发展的举措

DQ研究院的2020儿童在线安全和数字公民测量数据显示(见表2):中国儿童数字智能和数字技术使用自控力程度居中等偏上水平;连通性优势明显;网络风险居平均水平;社会性基础设施、指导与教育支持力度远低于平均水平,家—社两层力量处于缺位状态。具体表现为:(1)批判性思维和数字同理心低于世界平均水平,且与世界最高水平呈现巨大差距;数字足迹管理和网络欺凌管理处于世界平均水平,与世界最高水平差距甚远。(2)在数字技术使用自控力水平上,儿童在参与媒体支持的高频社交和网络游戏上的自律程度低于世界平均水平,滥用和成瘾现象严重;移动设备拥有率居中等偏上水平,与世界最高水平存在一定差距。(3)在网络风险水平上,技术的无序使用、名誉风险、网络欺凌、网络威胁等均低于平均水平,网络威胁程度十分严重。此外,危险内容程度处于世界平均水平偏上,需规范管理在线信息及资源环境。(4)在社会性基础设施上,社会行业参与度及专门性法律框架远低于平均水平,表明社会各行业对数字智能和在线安全仍未引起足够重视。同时,网络安全基础架构处于平均水平,仍有待进一步发展。(5)在指导与教育支持力度上,学校系统提供的在线安全教育以及家庭父母的引导参与程度远低于平均水平,表明家、校两个层面的支持严重不足。(6)在连通性上,互联网的访问开放度及服务优质度处于平均水平,互联网连接速度处于领先水平,说明促进智能教育及保障在线安全的基础设施硬件环境远超前于智力层面的服

务环境。

儿童的批判性思维、数字同理心、高频社交和网络游戏成瘾、技术无序使用、名誉风险、网络欺凌、网络威胁、数字智能、相应行业参与度及法律框架制度、学校在线安全教育、家庭教育支持处于危机预警状态,在数字足迹管理、网络欺凌管理、互联网访问可及度、移动技术应用普及度、危险内容抵御能力、网络安全基础架构服务需作为重点改进事项。因此,我国儿童数字智能及在线安全教育可从四个方面考虑:其一,关注儿童的批判性思维发展及网络文化情感价值教育。如学校及教师为学生提供数字公民、线上文化价值等相关的网络课程,以及创建数字简历的学习实践空间;在校园/班级网站上开设以文明、友善为核心的网络交流文化特色展览活动;以项目活动方式引导儿童借助自媒体开展有效参与网络评论的视频作品及其他类型资源创作活动。其二,重视对儿童安全保护的网行为规范及道德伦理制度建设。国家发布上网群体正当的在线行为标准和道德伦理法律法规,提供保证身心健康的维权渠道。引导儿童坚守自尊、自爱的在线交流行为操守,鼓励学生拒绝参与网络欺凌活动,帮助学生提升应对处理网络欺凌的维权知识与技能。其三,加强对网络信息资源的开发和应用管理。加大对危害身心健康的色情及违法犯罪的监管筛查,为儿童及青少年营造健康、文明、有益的学习资源及信息环境。其四,大力推进家—校—社多维度协同的数字智能及在线安全教育支持服务。学校利用教育资源优势,社会行业利用其技术、资金和组织优势,联合为儿童及其家长提供亲子互动的数字智能与线上安全网络课程、数字技术活动体验实践平台。家长通过以身示范积极引导子女在媒体使用、线上行为礼仪、数字责任心及在线安全防范的行为和价值观,对网络成瘾行为、网络欺凌及威胁行为及时干预,并提供知识、技能和解决策略方面的有力支持。

[参考文献]

- [1] Dot United Group. 2018 年度全球移动互联网市场报告[R/OL]. (2019-03-06)[2020-05-04]. http://pdf.dfcfw.com/pdf/H3_AP202001031373468507_1.pdf.
- [2] 中国互联网络信息中心. 第 45 次中国互联网络发展状况统计报告 [R/OL]. (2020-04-28)[2020-05-04]. <http://www.cnnic.net.cn/hlwzyj/hlwzxbg/hlwjtjbg/202004/P020200428596599037028.pdf>.
- [3] DQ Institute. 2018 DQ impact report[R/OL]. [2020-05-04]. https://www.dqinstitute.org/2018DQ_Impact_Report/.
- [4] DQ Institute. DQ Every Child. DQ school report [R/OL]. (2017-01-18)[2020-05-09]. https://www.dqinstitute.org/wp-content/uploads/2017/09/DQ_SchoolReportPremium_new-2.pdf.
- [5] DQ Institute. DQ global standards report 2019: common framework for digital literacy, skill and readiness[R/OL]. [2020-05-04]. <https://www.dqinstitute.org/wp-content/uploads/2019/11/DQGlobalStandardsReport2019.pdf>.

- [6] DQ Institute. Digital Intelligence (DQ): a conceptual framework & methodology for teaching and measuring digital citizenship?[R/OL]. [2020-05-04]. <https://www.dqinstitute.org/wp-content/uploads/2017/08/DQ-Framework-White-Paper-Ver1-31Aug17.pdf>.
- [7] DQ Institute. 2020 Child online safety index[R/OL]. [2020-05-04]. <https://www.dqinstitute.org/wp-content/uploads/2020/02/2020-COSI-Findings-and-Methodology-Report.pdf>.
- [8] 俞思瑾, 郑云翔, 杨浩, 黄星云, 钟金萍. 国际数字公民教育研究的现状、热点及前沿[J]. 开放教育研究, 2018, 24(6): 49-59.
- [9] 杨浩, 徐娟, 郑旭东. 信息时代的数字公民教育[J]. 中国电化教育, 2016(1): 9-16.
- [10] 顾小清, 易玉何. 从教育生态视角审视技术使能的教育创新[J]. 中国电化教育, 2019(11): 17-23, 59.

Digital Intelligence as A Critical Element of Future Ready Competency: Analysis and Suggestions Based on International Data about Online Safety of Children

ZHU Zhiting¹, XU Huanyun², HU Xiaoyong²

(1.School of Open Learning and Education, East China Normal University, Shanghai 200062; 2.School of Information Technology in Education, South China Normal University, Guangzhou Guangdong 510631)

[Abstract] As a larger scale population of digital natives, children and adolescents are facing unprecedented security storm of Cyber-Pandemic, which aroused human attention and new demand for the development of digital intelligence. This paper describes the conceptual framework and key features of digital intelligence firstly, followed by analyzing status of online risks of children from ten countries based on international investigation data, which reveals the problems existing with children's digital intelligence. The analysis results show that: among the six dimensions of online safety index, digital competency, disciplined digital use and cyber risks can be viewed as three key prediction dimensions of online safety index for children and adolescents. Social infrastructure, guidance and education are two important weak areas of children's online safety level. Countries' investment in the guidance and education, social infrastructure is seriously lacking. For digital intelligence, children perform well among these aspect of screen time management, cyberbullying management, privacy management, digital citizenship, and are weak in cyber security management, digital empathy, digital footprint management and critical thinking, which need to be focused on. Finally, strategic recommendations for enhancing digital intelligent education are put forward.

[Keywords] Digital Intelligence; Online Safety; Covid-19 Epidemic; Core Literacy; Cyberbullying