教育部教育信息化战略研究基地(北京)
EDUCATIONAL INFORMATIZATION STRATEGY RESEARCH BASE, MINISTRY OF EDUCATION, P.R.C

智慧教育资讯

Smart Education Newsletter

第4期

Dec. 2022
2022年12月

教育系统网络安全专题

为了服务教育数字化战略行动，推进“智慧教育示范区”、国家智能社会治理实验基地（教育）建设以及人工智能条件下教育社会实验，聚焦智慧教育发展、人工智能教育应用、教育信息化国际比较研究等领域开展战略研究，教育部教育信息化战略研究基地（北京）组织编撰《智慧教育资讯》。

主 办

教育部教育信息化战略研究基地（北京）

地址：北京市海淀区学院南路12号京师科技大厦A座12层
邮编：100082
电话：010-58807213
邮箱：bjjd@bnu.edu.cn
网站：https://cit.bnu.edu.cn
本期特邀主编：焦艳丽
本期编辑：林春艳　　审核：曾海军

目录

雷朝滋：确保教育信息化和网络安全同步谋划、同步推进

2021年7月，教育部等六部门发布《关于推进教育新型基础设施建设构建高质量教育支撑体系的指导意见》，提出到2025年，基本形成结构优化、集约高效、安全可靠的教育新型基础设施体系。《意见》抓住了关键点，提出了重点建设方向，有助于实现教育教学全要素、过程链、价值链的全面链接，打造教育新动能，为教育生态发展开辟新空间。

为更好地理解、贯彻落实《意见》，《在线学习》杂志（2021年9月刊）邀请教育部科学技术与信息化司司长雷朝滋就相关话题进行了解读。

教育新基建——新内涵、新技术和新机制

在线学习：请您阐述下《关于推进教育新型基础设施建设构建高质量教育支撑体系的指导意见》出台的背景。

《意见》的出台主要基于两方面的背景。

一方面，是国家推动新基建。2018年中央经济工作会议上，习近平总书记强调要“加快5G商用步伐，加强人工智能、工业互联网、物联网等新型基础设施建设”。2020年政府工作报告提出，要重点支持既促消费惠民生又调结构增后劲的“两新一重”建设，即新型基础设施、新型城镇化和重大工程。2021年政府工作报告再次强调推进“两新一重”建设，要继续支持建设信息网络等新型基础设施。目前，国家发展改革委已明确了新基建的内涵，正在牵头制定新基建的规划。

另一方面，是教育高质量发展。党的十九届五中全会提出“建设高质量教育体系”。2021年全国教育工作会议明确将高质量教育支撑体系作为“十四五”建设高质量教育体系的八大体系之一，提出抢抓国家布局新基建的重大机遇，谋划和提出“十四五”教育新基建体系构建的思路举措。

在线学习：《意见》提出“推进教育新型基础设施建设”，“新”在何处？

教育新基建的“新”主要体现在三个方面——新内涵、新技术和新机制。

新内涵。新基建是相对于传统基建来说的，两者在内涵上有本质区别。传统基建大多指建筑工程，如公路、铁路、桥梁、大厦等。新基建以信息网络为基础，根据国家发展改革委的表述，可分为信息基础设施、融合基础设施和创新基础设施三大类。

新技术。教育新基建是对教育信息化现有发展基础的传承和创新，更加注重新一代信息技术的广泛应用。它支撑以5G、人工智能、云计算、区块链为代表的新一代信息技术与教育教学实践深度融合，培育教育信息化发展的新动能。

新机制。推动教育新基建，要充分发挥各方力量，构建多方协同的教育供给新生态。要加强部际协同、部省联动和区域协调，促进算力资源、教育数据和教育应用的开放共享，实现集约部署、高效利用。

总之，教育新基建面向未来，要促进信息技术与教育教学的深度融合，构建高质量教育支撑体系。推动教育新基建要跳出技术的逻辑，从教育生态构建和教育事业发展的高度去勾勒发展蓝图。

▼ 六位一体，教育专网和大平台这样建

在线学习：《意见》指出教育新基建的重点方向，包括信息网络、平台体系、数字资源等六大类。这六者的关系是怎样的？

六个重点方向是相互支撑、相互促进的关系。

新网络、新平台、新安全是支撑教育信息化发展的数字底座。其中，网络是连接人与人的桥梁，平台是促进信息技术和教育深度融合的舞台，安全是保障信息化行稳致远的压舱石。新资源、新校园是在新网络、新平台、新安全基础上，根据教育实际建设的、具有行业特色的基础设施。其中，新资源是偏软的，对应知识生产管理；新校园是偏硬的，对应环境设施配套。新应用是基于新资源、新校园，支撑具体应用场景的基础设施。从教学、评价、研训、管理等四大场景进行布局，探索信息技术推动教育变革的路径。

总的来说，新网络是教育空间拓展设施，新平台是资源数据运行设施，新资源是知识思想承载设施，新校园是教育场所升级设施，新应用是教学管理服务设施，新安全是师生发展保护设施，六位一体构建高质量教育支撑体系，面向教育教学主战场，推动教育信息化“课堂用、经常用、普遍用”，支撑教育高质量发展。

在线学习：《意见》提出建设教育专网。如何建设？教育专网可以发挥哪些作用？

2019年8月28日，国务院常务会议明确提出加快建设教育专网，到2022年实现所有学校接入快速稳定的互联网。建设教育专网是总结新冠疫情大规模在线教学经验，为重大公共卫生事件下大规模在线教学做应急准备。同时，应积极应对常态化疫情防控下教育教学的新挑战，构建线上线下相融合的教学新模式。建设教育专网是教育信息化发展的必然选择。全国中小学（含教学点）的未联网学校已实现动态清零，学校网络保障从解决有无向提高质量转变，以支撑信息化条件下的教育教学改革。对于教育专网的建设，我们有以下几点思考。

关于建设目标，教育专网是由教育行政部门统一管理，覆盖各级各类学校和各级教育行政部门，提供高速、便捷、绿色、安全的网络服务的逻辑专网。

关于网络结构，应由国家主干网、省级教育网和学校校园网等三级网络组成。其中，国家主干网将基于中国教育和科研计算机网（以下简称教科网）升级改造建设。

关于建设方式，应在充分利用国家公共通信资源的基础上，按照分级建设的原则推进教育专网建设。教育部会同有关部门推动全国主干网建设；各地政府争取基础电信企业的支持，推进省市局域网建设；各接入学校负责学校校园网建设。

关于网络管理，应遵循网络地址、域名和用户“三统一”的原则，即统一分配网络地址，优先使用IPv6技术；统一使用教科网域名（edu.cn），实施统一备案；统一接入认证，实现实名认证全覆盖。

建设教育专网的作用主要表现为三个方面：**一是提高网络服务质量**。通过网内信息可高速传输的特点，推动各类资源平台和管理平台接入教育专网，满足不断增长的信息化教学和管理需求。**二是降低整体用户成本**。通过分地区集中采购网络接入服务和财政倾斜性支持薄弱地区等方式，为学校提供质优价美的网络保障。**三是保障师生绿色上网**。通过实施教科网网络安全保障能力提升计划，实现网络不良信息的过滤，为未成年人上网营造清朗网络环境，切实维护广大师生的切身利益。

在线学习：《意见》提出建设“互联网+教育”大平台，对此怎么理解？应该如何建设？

“互联网+教育”大平台是教育信息化2.0行动计划中“三全两高一大”目标的重要组成部分，是对现有资源平台和管理平台的深度整合，进而实现平台互联、数据互通、应用协同。

在《意见》中，我们提出建设新型平台体系基础设施，提出从构建新型数据中心、促进教育数据应用、推动平台开放协同和升级网络学习空间等四个方面构建“互联网+教育”大平台。“互联网+教育”大平台的关键属性是共享。鼓励建设地区性的大数据中心，共享算力资源；促进数据在教育教学中全方位应用，共享数据资源；提供多元服务推动业务上云，共享教育生态；依托网络学习空间加强师生互动，共享学习知识。

各地各校在建设“互联网+教育”大平台时，应该遵循以下原则。**一是坚持应用导向。**立足教育高质量发展的迫切需要，固根基、扬优势、补短板、强弱项，致力解决教育均衡、师生减负、评价改革等重要任务。**二是坚持数据驱动。**发挥数据作为生产要素的战略性作用，增强数据在教育教学、管理服务、教育评价等方面的应用。**三是坚持集约建设。**推动教育数据“一数一源”和教学管理“一网通办”，降低开发运行成本、提升应用效果、优化服务体验。四是坚持多元参与。鼓励高等院校、企业和社会组织等提供应用服务，培育多元参与的应用生态。

▼ 教育新基建要适度超前部署

在线学习：您认为，在《意见》落实过程中，要着重处理好哪些关系？

推动教育新基建应注重四个关系。**一是安全和发展的关系**，确保教育信息化和网络安全同步谋划、同步推进，以安全保发展，以发展促安全。**二是传统基建和新基建的关系**，以新基建为传统基建赋能，推动教育的数字转型，促进线上线下相融合。**三是存量和增量的关系**，既要吐故纳新，又要盘活存量，充分利用现有资源设施，发挥一加一大于二的效果。**四是政府和市场的关系**，坚持政府和市场“两条腿”走路，把“看不见的手”和“看得见的手”都用好。一方面要发挥政府主导作用，恪守教育民生底线，规范行业秩序，保障教育公平，另一方面要充分发挥市场活力，培育良好的生态，但不能过度商业化。

在线学习：您之前曾提到“不能因为疫情期间出现网络瓶颈，就在疫情之后对基础设施进行过度投入，但应针对此次暴露的问题进行适度改善提升。”在《意见》实施过程中，应如何把握这个度？

这句话是我接受采访时说的。这里说的不能“过度投入”，是指不能把疫情期间大规模在线教育的应急之举常态化，教育新基建不能以此作为标准。但不可否认的是，疫情期间大规模在线教育加速了教育理念变革的进程，疫情后教师无法回到从前、也不该回到从前。因此，教育新基建也要聚焦未来、提前布局，构建高质量的教育支撑体系。

因此，推动教育新基建要坚持辩证客观的工作思路。**一方面，要实事求是，**根据地方实际，立足教育发展现状，量力而行、循序渐进地推动教育新基建，避免盲目扩张和资源浪费。**另一方面，要解放思想，**充分认识信息化的变革力量，深入应用新一代信息技术，发挥数据作为生产要素的作用，适度超前部署。

在线学习：您认为，智慧教育示范区会对教育新基建发展起到怎样的作用？

试点先行、典型引路是推进教育信息化发展的重要途径。开展智慧教育示范区创建，是落实教育信息化2.0行动计划的一项战略举措，旨在推动教育理念与模式、教学内容与方法的改革创新，提升区域教育发展水平，形成引领教育改革发展的新途径、新模式。我们鼓励智慧教育示范区创建区域在推进教育新基建方面先行先试，发挥示范引领作用，围绕教育新基建的重点方向，开展有益的探索，形成可资借鉴的经验。

来源：《在线学习》杂志2021年9月刊（总第74期）
原标题：《适度超前部署教育新基建》

雷朝滋　教育部科学技术与信息化司司长

单志广：智慧城市建设坚持“可管可控、安全可信”根本原则

智慧城市在中国已经推进了10多年。智慧城市是运用新一代信息技术，包括物联网、云计算、大数据、人工智能、区块链、空间地理信息集成等促进城市规划、建设、管理和服务智慧化的一种新理念和新模式构建智慧城市，安全可信是非常重要的一个需求；在新型智慧城市的5个发展宗旨中，构建自主可控的安全体系也是非常重要的一个要求；在新型智慧城市的5大核心特征中，也包括要实现安全可信。

当前新型智慧城市建设已经实现了统一的入口、统一的后台和可以复用的中台这种体系架构，在这种新型体系架构的引领下，安全体系始终是一个自上而下、贯穿全局的重要要求。

智慧城市的安全挑战

物联网、移动互联网、云计算、大数据、导航定位等新技术新应用不断推动新型智慧城市建设快速发展，同时也带来了新的安全挑战，使得智慧城市建设面临安全脆弱性难题。智慧城市的核心价值是要实现数据和信息的高度集中和共享数据和信息资源越集中，信息安全风险也越集中，信息安全保障也越重要。云计算具有整合和集约化处理信息资源的优势，随着云计算和虚拟化技术的迅速发展，越来越多的数据上传到云端数据库，使得数据资源过于集中，一旦云服务器遭到入侵，数据资源安全将受到严重威胁。大数据涉及国家安全和个人隐私，获取和控制网络海量数据资源，提高数据 掌控权和国家控制力，已成为国际竞争的战略焦点。大数据已成为网络攻击的显著目标，现有的网络安全手段已不能满足大数据时代的网络安全要求。可见，云计算大数据、物联网、移动互联网使得智慧城市建设正面临与传统电子政务、行业信息化完全不同的新的安全需求。

互联网、物联网、云计算、大数据等技术的使用进一步强化了网络空间和物理空间的安全互依赖性智慧城市的各类基础设施之间存在物理互依赖性、网络空间互依赖性、地理互依赖性、逻辑互依赖性，且这些互依赖性之间也是相互作用、相互影响的，导致智慧城市的安全威胁呈现多个层面的“骨牌效应＂，即产生“牵一发而动全身”和多米诺骨牌效应式的关联性影响例如，智慧城市各种物理设施（铁路、道路、港口、桥梁、发电厂等）之间相互关联和影响这种物理互依赖性又与网络空间互依赖性高度交织例如，电力供应系统中断会影响

信息通信系统的运行，信息通信系统的故障也会影响电力供应系统的运转智慧城市广泛涵盖智慧家居、智慧交通、智慧旅游、智慧能源等系统，智慧城市比一般物联网应用、大数据应用的场景更加庞杂，各个系统之间的耦合性和漏洞更多，出错概率更大，容错性要求也更高智慧城市是由众多分立的信息系统组合成的航母级的开放复杂巨系统，从整体上具备高可信属性已成为智慧城市发展的根本前提和必然要求。

近年来，从全球智慧城市实践中发现，安全可信能力不足带来大量问题。2017年达拉斯市的防空警报系统被攻破，产生了错误的报警；2018年IBM发布法国、阿根廷等国家的4个智慧城市系统的17个0Day漏洞。这些都是由于系统安全可信性的缺失、缺陷造成的。

智慧城市的安全可信防护原则

智慧城市建设一定要坚持“可管可控、安全可信“这个根本原则除了传统安全建设要确保数据、网络、主机、系统安全外，对现有安全技术的自主可控也提出了更加强烈的要求。在智慧城市建设中需要进行严格的全流程的信息管理在过去电子政务系统建设时期，安全系统可以和信息化系统异步建设智慧城市则要求安全系统和信息网络数据系统同步设计、同步建设、同步管理、同步运营。在智慧城市的设计阶段，要加强风险论证，合理确定安全保护的等级，同步设计安全防护方案。在智慧城市的实施阶段，要以制度和规范为保障，加强对技术、设备和服务供应商的安全审查，同步建设安全防护手段。在智慧城市的运行阶段，要加强管理，定期开展检查、等级评测和风险评估，认真排查安全风险隐患，增强日常监测和应急响应的处置恢复能力。

要加强对要害信息系统和信息资源的安全防护智慧城市涵盖大量政府、金融、能源、交通、电信、公共安全、公共事业等领域的重要信息系统，要确保这些信息系统的安全可信，完善网络安全设施能力，提高网络管理、态势预警、应急处理和信任服务能力。同时要建设容灾备份体系，推行联合灾备、异地灾备，建立重要信息系统的使用管理和信息评价机制。

在传统电子政务和行业信息化中，安全防护措施都是防火墙、威胁检测、防病毒这老三样，都是针对传统边界非常清晰的条件来实施。智慧城市的范围非常广，涵盖了基础设施、公共服务、社会管理、产业经济、政府决策等方方面面。更为重要的是，在智慧城市范畴下，系统和系统之间、人和人之间的界限不再像过去那样清晰。前沿在哪里，入口在哪里，边界在哪里，如何有效区分内部和外部，这些都成为智慧城市系统安全可信的新挑战。

总体来讲，智慧城市是由多种异构系统、异构数据、异构网络相互连接，通过数据融合、平台集成、整体应用展现形成的一个开放复杂巨系统。未来智慧城市系统安全可信防护应该做到攻击者进不去、非授权者重要信息拿不到、窃取保密信息看不懂、系统和信息篡改不了、系统工作瘫不成、攻击行为赖不掉，和人的免疫系统一样，实现牵一发而动全身的动态的、高效的防护。

如何理解可信

可信是在传统正确安全、容错、可靠概念的基础上延伸出来的新概念，涵盖的范围更大，用可信这样一个属性来界定智慧城市的服务品质是一个更为科学的、合理的评价方式。

一般认为，可信是指一个实体在实现给定目标时其行为及其结果是可以预期的，它强调目标与实现相符以及行为和结果的可预测性和可控制性。“可信的智慧城市”可以认为智慧城市系统的运行行为及其结果总是符合人们的预期，并且在受到干扰时仍能提供连续的服务。这里的“干扰“包括操作错误、环境影响、外部攻击等智慧城市的可信性可有多个不同的考察视角，包括功能、环境和使用等，涉及智慧城市服务的精确性、可靠性、安全性、正确性、时效性、可维护性和可生存性等关键性质。

可信智慧城市的构建

智慧城市系统存在可信性问题的原因是多方面的，如智慧城市系统具有个性化创造的特色、软件用户具有多样化的需求、系统规模和复杂度不 断提高等因此运行在开放和动态环境中的智慧系统，其可信性需要有新的保障措施。可信智慧城市系统需要构建一个完备的体系框架，包括体系结 构可信操作行为可信、资源配置可信、数据存储可信和策略管理可信构建可信智慧城市面临的一些重要核心问题需要业界来共同推动和解决，如智慧城市信息系统可信性如何度量与建模、可信智慧城市信息系统如何构造与验证、可信智慧城 市信息系统如何演化与控制等。

对于智慧城市信息系统可信性的度量与建模，要从过去单一属性、从属性的定性刻画和静态的确定性表达转变为多属性的动态的定量度量过去强调安全往往是在封闭的环境，要求绝对安全，智慧城市强调开放的环境，要实现相对可信。对可信系统的演化和控制，要从过去的静态部署、被动响应转化成动态演化和主动监控。智慧城市的可信属性要从过去对传统信息系统的绝对可信、静态可信、单机可信和被动可信转变成今天对智慧城市管理和服务的动态可信、相对可信、全局可信和主动可信构建可信智慧城市是在安全、容错、正确的基础上构建一种对可信智慧城市的新的能力表达传统封闭和静态环境下发展起来的以安全性为核心的信息系统保障的基本理论、方法、技术和机制，已经不足以适应网络化、开放、动态环

境下的可信智慧城市。尤论是网络系统或软件，其安全和可信实际上是非功能性的属性，只要智慧城市的网络系统和软件存在人机交互，其安全和可信就是一种重要品质智慧城市的可信不是一次性测试出来的，是在智慧城市系统的使用过程中累积出来的，这个使用过程就是通过智慧城市的管理和服务，不断消除一个又一个不可信要素的过程。

区块链技术在可信智慧城市建设中的作用

随着新一代数字技术的不断发展，区块链技术得到广泛的关注习近平总书记在2019年中央政治局第十八次集体学习时谈到，要发挥区块链在促进数据共享、优化业务流程，包括在建设可信体系方面的作用。他专门谈到要推动区块链底层技术和新型智慧城市建设发展相结合。因此在构建智慧城市过程中，要高度关注区块链技术，这对构建可信智慧城市具有非常重要的意义。

区块链是由多种现有技术，包括分布式数据存储、点对点传输、共识机制、加密算法、智能合约等集成创新产生的分布式账本技术。该技术在不信任或弱信任环境下实现信息对称，改变了过去串联的信息系统结构基于分布式账本技术形成了一种新的数据信任机制，保障链上数据的透明性、可追溯和防篡改等。区块链对于构建可信智慧城市是一种非常好的技术手段此外，区块链也在重构信息时代的生产关系和治理机制，把过去信息系统基于对人的信任转化成对机器、规则的信任。因此区块链技术在智慧城市建设中能够更好地帮助实现可信属性。

结论

新型智慧城市是一个开放复杂巨系统，其运行与服务的可信性对智慧城市建设尤其重要。由于数据的融合、技术的融合和业务的融合，可信性成为智慧城市建设的挑战与难点传统信息系统安全保障方式和手段对智慧城市不完全适用，需要建立适应新型智慧城市建设的可信保障体系。可信智慧城市在理念模型、体系架构、技术方法等方面仍然是开放性问题，需要在我国新型智慧城市建设实践中不断强化、优化和完善。

来源：2022年西湖论剑·网络安全大会——数字城市安全治理论坛论文集《信息安全研究》杂志社会议论文集。原标题：《可信智慧城市》

作者：单志广，博士，二级研究员，国家信息中心信息化和产业发展部主任. 主要研究方向为智慧城市、数字经济、区块链和信息安全

沈昌祥：构建“安全可信”网络空间安全防护体系

党的十八大以来，我国网络安全工作进入快车道。新起点，新征程。回望过去，我国网络安全行业取得哪些发展成就？立足当下，面临哪些新挑战？面向未来，将出现哪些新趋势？中国网络空间研究院网络安全研究所、《中国网信》杂志融媒体中心、光明网网络安全频道、安恒信息联合推出系列专访。

本期邀请中国工程院院士沈昌祥进行访谈，于“中国网信杂志”微信公众号2022年7月1日发表。

记者：请您结合自身实践，谈谈网络安全十年来的发展变化，以及行业发展面临的新挑战、新问题。

沈昌祥：当前，网络空间已经成为继陆、海、空、天之后的第五大国家主权领域空间，也是国际战略在网络社会领域的演进，我国的网络安全正面临着严峻挑战。以“没有网络安全就没有国家安全”“安全是发展的前提，发展是安全的保障”为宗旨，按照国家网络安全法律法规、战略要求，推广安全可信产品和服务，筑牢网络安全底线是历史的使命。党的十八大以来，我国在网络安全领域取得可喜成绩。《中华人民共和国网络安全法》（以下简称《网络安全法》）《中华人民共和国密码法》（以下简称《密码法》）《中华人民共和国数据安全法》和《关键信息基础设施安全保护条例》等法律法规治理体系逐步完善，网络安全产业发展有法可依，有章可循；安全可信的网络产品和服务产业生态初步构建，产业结构逐步合理；网络空间安全一级学科确立，人才培养体系初步建立，网络安全人才培养力度不断加大，国家网络安全保障能力大幅提升。

与此同时，我国网络安全在技术、产业和能力等方面与发达国家相比仍存在不小差距，在复杂的网络安全博弈中略显被动：自主创新不足，以“跟随型”为主的安全产业发展思路难以解决核心技术“受制于人”的问题；网络安全防护技术体系尚不健全，重点领域网络安

全保障能力不足，集中表现为“网络安全底数不清”“网络防御被动应急”，难以形成网络安全积极防御体系，网络安全保障措施难以适应快速变化的对抗形势等。为此，我们应以前瞻性布局占据战略制高点，形成一套既富有中国特色又符合世界发展潮流的网络空间安全保障战略思维，以自主创新产业争取战略主动权，着眼国家安全和长远发展，构建世界领先、安全可信的自立自强网络安全产业生态体系，从根本上解决核心技术受制于人的问题，积极参与网络空间国际治理，加强网络空间国际合作，提升我国在网络空间领域的国际地位。在“十四五”期间努力打造安全可信的核心技术产业生态，构筑安全可信的网络安全基础，建立顺畅高效的组织管理体系和系统完备的法律法规治理体系，加强良性循环的经费保障，做好多层次的人才培养工作，为国家网络安全提供有力支撑，为建设网络强国构筑坚实基础。

记者：《网络安全法》对守护网络安全防线、构建安全可信网络体系提出了更高要求。其中也明确提出推广安全可信的网络产品和服务。对于“安全可信”的内涵该如何理解？

沈昌祥：“安全可信”是网络所使用的设备应当具备的安全性能，即在设备工作的同时，内含的安全部件进行动态并行实时全方位的安全检验，确保计算过程及资源不被干扰破坏和篡改，能正确完成处理任务。这就是用主动免疫可信计算3.0技术开发的网络产品和服务，相当于人体具有免疫能力，离开封堵查杀“老三样”被动防护，自主创新解决核心技术卡脖子问题。

随着信息技术的快速发展和网络安全形势的不断变化，我们逐渐认识到，掌握网信核心技术是我国摆脱网络安全受制于人的根本，也是保障重要信息系统及其数据安全的前提。保障芯片、整机、操作系统、数据库等基础软硬件的供应链安全可信，成为建设网络强国的保障基石。

要实现安全可信必须自主创新、自立自强。首先要认清网络安全风险的本质。安全风险源于图灵机原理少安全理念、冯·诺依曼体系结构少防护部件和网络信息工程无安全治理三大原始性缺失，再加上人们对IT逻辑认知的局限性，设计产品不可能穷尽所有逻辑组合，只能处理完成和计算任务有关的逻辑组合，必定存在大量逻辑不全的缺陷漏洞，从而难以应对人为利用缺陷漏洞进行攻击获取利益的恶意行为。

为了降低安全风险，必须从逻辑正确验证、计算体系结构和计算模式等方面进行科学技术创新，以解决存在的漏洞缺陷不被攻击者利用的问题，形成攻防统一的体系，这与人体健康必须有免疫系统一样。这就是中国可信计算3.0的新计算模式和架构，计算同时并行进行防护，即以物理可信根为基础，一级验证一级，通过构建可信链条，为用户提供可信存储、可信度量和可信报告等多种功能，为保证用户的数据资源和操作过程安全提供可信任的计算环境，有效降低系统的安全风险。由此可见，《网络安全法》要求推广使用安全可信的网络产品和服务是科学合理的，也是高效可行的。

记者：在构建“安全可信”网络空间安全防护体系，提高网络安全主动免疫能力方面，我们要从哪些方面着手？

沈昌祥：首先要自主创新发展主动免疫可信计算3.0，为安全可信产业打造良好生态环境。

可信计算3.0源于我国，对新型可信计算的研究开始于上个世纪90年代初，1995年2月通过鉴定，定型装备，经过长期攻关形成了自主创新的可信计算3.0技术体系。

可信计算3.0采用运算和防御并行的双体系架构，在计算运算的同时进行安全防护，将可信计算技术与访问控制机制结合，建立了计算环境的免疫体系，能及时识别“自己”和“非己”成份，禁止未授权行为，使攻击者无法利用缺陷和漏洞对系统进行非法操作，最终达到“进不去、拿不到、看不懂、改不了、瘫不成、赖不掉”的效果，对已知和未知病毒不查杀而自灭。

其次是自立自强建立安全可信创新体系：一是可信体系架构的创新。可信计算3.0创造性地提出了计算节点由运算部件和防护部件并行的双体系架构，在保持原有应用系统不变的情况下，构建主动免疫的可信计算环境，为应用提供主动免疫安全可信的保障机制，主动拦截系统操作运行要素，按预定的策略规则进行可信判定，及时发现并禁止不符合预期的行为，保证全程安全可信的运行。

二是可信计算密码技术的创新。可信计算3.0架构根据国家《密码法》规定的算法标准发布的可信密码模块（TCM）国家标准，满足可信计算需求，并要在三个方面有重要创新：首先是构成了对称与非对称融合的密码体制，全面支持可信功能；其次，可信计算3.0架构下

的可信计算密码技术以国内密码算法为基础，对称密钥算法使用SM4算法，非对称密钥算法使用SM2算法，哈希算法使用SM3算法，高效实现身份认证、加密保护和一致性校验；再是采用双证书体制，用平台证书认证系统，用加密证书保护密钥，并且将加密功能和系统认证功能分离管理，符合《中华人民共和国电子签名法》要求，简化了证书管理工作，提高了系统通过隔离增强加密和认证功能的安全性。

三是可信平台控制模块的创新。提出以可信平台控制模块（TPCM）作为可信根，并接于主机的计算部件，在可信密码模块基础之上增添对系统和外设的总线级控制机制。TPCM是系统可信的源头，它将密码机制与控制机制相结合。目前，TPCM国家标准已发布，并被发展成为插卡、主板SoC和多核CPU可信核三种模式产品，得到大量推广。

四是可信主板的创新。可信平台主板将防护部件与计算部件并接融合，由TPCM和系统中的多个度量点(包括TPCM对Boot ROM的度量机制)组成防护部件，计算部件保持原有架构不变。信任链在“加电第一时刻”开始建立，从而提高了系统安全性。同时在主板上的多个度量点分别设置度量代理，通过这些度量代理实现硬件控制，并为可信软件层提供可信硬件度量和控制接口。

五是可信软件基的创新。可信软件基是在TPCM支撑下，基于双系统体系结构下以原始信息系统宿主软件为保护对象，构成并行的双软件架构。可信软件基在可信计算体系中处于承上启下的核心地位，对上与可信管理机制对接，通过主动监控机制保护应用，对下连接TPCM和其他可信硬件资源，对系统安全机制提供可信支撑，同时与网络环境中其他可信软件基实现可信协同。可信软件基并行于宿主基础软件，在TPCM的支撑下，通过宿主操作系统代理进行主动拦截和度量保护，实现主动免疫防御的安全能力。

六是可信网络连接的创新。针对集中控管的网络安全环境，创造性地提出了三元三层可信连接架构，能够有效防范内外合谋攻击。同时，这一架构在纵向上对网络访问、可信评估和可信度量分层处理，使得系统的结构清晰、控制有序。进行访问请求者、访问控制者和策略仲裁者之间的三重控制和鉴别，实现了集中控管的网络可信连接模式，提高了架构的策略规则可管性、可信性。

记者：强化网络空间安全保障，离不开相关产业政策的支持和引导。今后在进一步打造安全可信的产业生态方面，需要在哪些方面完善政策、创新制度？

沈昌祥：要优化产业政策，打造安全可信的产业生态体系。加强统筹规划，加大投入力度，扶持网络安全产业和项目，加快推广安全可信的网络产品和服务。形成安全可信国产化推进机制，推动安全可信技术产品应用。出台相应政策为自主创新产品提供市场应用空间，促进技术产品创新、性能优化提升与产业应用协同发展。

要以企业为主体，优化网络安全产业创新发展环境。优化企业生存环境，激发大众创业、万众创新的热情。强化企业的创新主体地位，营造公平合理的市场环境，结合国家“一带一路”倡议，打造更有利的国际化发展环境，充分发挥政府机构、行业协会和产业联盟的作用，积极参与国际合作，争取更多的国际话语权。通过建立产业并购基金、共享专利池等措施为企业国际化发展提供支持，减轻国内企业在国际竞争中的压力。

要加强人才培养，建设全方位网络安全人才队伍。加大人才培养力度，打造数量充足、结构合理的网络安全人才队伍。加强网络空间安全一级学科建设，由专业机构、行业企业等梳理人才需求，同时加强用人单位与高校、专业培训机构的合作，进一步缩短人才供需差距。

要统筹规划加大投入，强化经费监管，大幅提升国家资金的利用效率。优化经费支持方式和监管模式，提升经费投入效益。通过成立专业化项目管理机构，统一受理网络安全项目申请，严格公正评审立项，整合原有网络安全项目资源，集中资源重点突破核心技术瓶颈。完善现有经费监管模式，建立合理的经费申请和评审流程，同时在各环节加强审计。加强产学研用管等各方面的配合，前瞻性统筹经费支持方向，在优先支持基础性、公益性项目的同时，充分考虑经费投入将产生的经济效益，设立“产业基金”“创新基金”等实体机构，加快技术研发市场化速度，形成良性循环的市场化经费支持机制。

→ 来源：“中国网信杂志”微信公众号，2022-07-01

作者： 沈昌祥 中国工程院院士

余晓晖：安全发展贯穿于新型基础设施建设全过程

当前，人类社会已迈入第四次工业革命时期，新型基础设施正在成为新一轮科技革命和产业变革的关键支撑和重要物质保障。我国经济社会已转向高质量发展阶段，迫切需要构建新型基础设施来引领和支撑先进生产力的发展。“十四五”时期是新型基础设施全面布局建设的关键五年，要立足国情、统筹全局、放眼未来，明确新型基础设施的建设范围、发展目标、主要任务和保障措施，统筹推进全国新型基础设施建设和发展。

一、把握本质，深刻认识新型基础设施的内涵特征

（一）新型基础设施伴随新一轮产业变革产生。

纵观人类经济发展史，每一轮产业变革都会孕育新的基础设施，并推动传统基础设施改造升级。加速发展的新型基础设施是新技术、新生产要素在全社会广泛普及的必要物质基础，也是新产品、新业态、新经济部门快速成长的关键支撑。当前，第四次工业革命蓬勃兴起，数字经济加速与实体经济深度融合，数据成为关键生产要素，技术演进升级和经济社会发展推动新型基础设施的形成和成长。

新型基础设施是以新发展理念为引领，以技术创新为驱动，以信息网络为基础，提供数字转型、智能升级、融合创新等方面基础性、公共性服务的物质工程设施。信息基础设施、融合基础设施和创新基础设施三方面内容构成当前新型基础设施的主要框架体系。信息基础设施主要是指基于新一代信息技术演化生成的基础设施，如5G、物联网、数据中心、人工智能、卫星通信、区块链基础设施等。融合基础设施主要是指传统基础设施应用新一代信息技术进行智能化改造后所形成的基础设施形态，包括以工业互联网、智慧交通物流设施、智慧能源系统为代表的新型生产性设施，和以智慧民生基础设施、智慧环境资源设施、智慧城市基础设施等为代表的新型社会性设施。创新基础设施是指支撑科学研究、技术开发、新产品和新服务研制的具有公益属性的基础设施。

（二）新型基础设施具有与传统基础设施不同的鲜明特点。

除具备基础性、公共性和强外部性等基础设施一般特征外，新型基础设施具有许多区别于传统基础设施的鲜明特点，这是制定新型基础设施政策的基本逻辑和出发点：

一是多数新型基础设施尚处于发展的初级阶段。与传统基础设施经过百十年的演化发展而逐渐成熟不同，新型基础设施是近些年才出现的，其主导技术、产品形态、市场需求、配

套产业、商业模式等都处于培育阶段，尚未稳定成型。这意味着新型基础设施的规划建设要着眼于长远，很多新型基础设施尚不具备大规模商用部署的基础，应从技术和应用方面培育新型基础设施。

二是多数新型基础设施的自然垄断性大幅下降。从技术工程的角度看，传统基础设施必须进行一次性大规模投资才可使用，初始投资成本巨大。而新型基础设施多在信息网络之上构建，可实现“一点接入，全网服务”，这使得其投资规模可视需求变化弹性增加，初始投资门槛显著下降。更多企业可进入新型基础设施市场开展竞争，但同时也带来盲目投资、重复建设、技术标准难以统一等问题。

三是新型基础设施的技术创新速度快。传统基础设施技术较为成熟、升级缓慢，而新型基础设施所依托的信息技术快速演进升级，并不断与传统基础设施技术交织融合，整体技术体系持续创新优化，基础设施需迭代式的开发和升级。建设和运营新型基础设施需要大批创新性强的高技术公司和人才，并形成与之相适应的融资、监管和发展环境，这是一项长期系统工程。

四是数据和网络安全的重要性进一步突出。一方面，必须构建有效促进数据流通的制度环境和技术标准体系。数据是新型基础设施正常运行的血液，在以市场力量为主的建设模式下，既需要加快健全数字治理体系，更需要形成统一的建设标准、技术规范等，推动不同所有者设施之间的互联互通。另一方面，对基础设施的安全可靠要求更高。信息基础设施和融合基础设施都是联网运行，数字世界和物理世界高度融合，人们生活生产的有序运转将取决于这些新型基础设施的安全可靠运行。

二、分类施策，打造系统完备的基础设施体系

新型基础设施种类多样，不同类型设施发展阶段不同，属性特点也不同。“十四五”时期应以高质量发展为主题，以建设系统完备、高效实用、智能绿色、安全可靠的新型基础设施体系为导向，深化技术创新和制度创新，依据不同设施的阶段特点，选择适合的设施发展方向和演进路径，加速新型基础设施形态的培育和发展，夯实建设现代化强国的先进物质基础和条件。

（一）强化新兴技术引领，加速建设信息基础设施。

不同于传统面向连接的通信基础设施，新一代信息基础设施正向以信息网络为基础，以数据要素为核心，提供感知、连接、存储、计算、处理等综合数字能力的基础设施体系发展。要顺应信息技术发展趋势和基础设施功能演化需求，打造集感知设施、网络设施、算力设施、数据设施、新技术设施于一体的新型信息基础设施体系。对于已有的基础设施，一方面要基于新技术实现设施升级，如推动移动通信网络从4G向5G升级、固定接入网络从百兆向千兆升级、加快下一代互联网规模应用等，另一方面也要适应新需求优化提升设施性能，如适应智

能社会发展需求推动数据中心体系向多层次、体系化算力供给体系演进，适应数据流量增长和流向变化趋势优化网络架构，推进云网协同和算网融合发展。对于新兴的基础设施，要更注重设施的形态培育、技术研发和应用推广，如加大量子计算、下一代通信网络技术等的研发和试验力度，培育新一代智能计算中心、人工智能海量训练库、标准测试数据集和“智能+”行业赋能平台等人工智能基础设施，探索发展安全可扩展的区块链基础设施等。

（二）聚焦经济社会转型，全面发展融合基础设施。

利用新一代信息技术推动新型生产性设施发展，可有效推动传统产业转型升级，带动生产方式、组织方式变革，支撑新产业、新业态发展。新型生产性设施涉及工业互联网、智慧交通物流设施、智慧能源设施、智慧农业农村设施等，每类设施充分考虑行业属性、所处阶段和融合水平的差异性，重点支持支撑范围广、赋能能力强、带动效应好的设施发展，如工业互联网平台、车联网、智慧物流、能源互联网等。建设基于新一代信息技术的新型社会性设施，有利于增加公共服务供给、丰富公共服务内容、提升公共服务水平。要全面覆盖与广大人民群众日常生活密切相关的重要领域，积极发展智慧医院基础设施、智慧养老基础设施、智慧教育基础设施等，提升公共服务的供给数量和质量，促进公共服务的均等化、公平化。发展智慧环境设施、新型城市管理设施等，则有助于创新公共治理模式，形成科学精细智能的治理能力。

（三）着眼提升科技能力，前瞻部署创新基础设施。

“十四五”规划《纲要》提出，“坚持创新在我国现代化建设全局中的核心地位，把科技自立自强作为国家发展的战略支撑”。创新基础设施是实现科学技术突破、促进科技成果转化、支撑创新创业的重要基础，对提升国家科技水平、创新能力和综合实力具有重大影响。可依据从自主研究开发到产业化的创新长链条布局创新基础设施。面向世界科技前沿，聚焦新一轮科技革命重点方向，建设一批重大科技基础设施，提供极限研究手段，帮助提升原始创新能力和支撑重大科技突破。面向国家重大战略需求，聚焦解决重大科技问题，建设一批科教基础设施，构建特色鲜明、水平先进的研究平台体系。面向经济主战场，聚焦提升产业创新水平，整合现有优质资源，建设一批新型共性技术平台和中试验证平台，完善高水平试验验证设施，支撑产业技术升级和企业创新发展。同时，为激发社会创新活力，推动建设一批低成本、开放式、专业化的创新创业服务设施，为中小企业创新发展、大众创业万众创新提供便利条件。

三、创新制度，形成活泼有序的发展格局

新型基础设施建设刚刚起步，与传统基础设施相比，新型基础设施的发展必须引入更多的市场力量，但“政策之手”也不可或缺。为加快我国新型基础设施发展，“十四五”时期要强调深化制度创新，推动有效市场和有为政府更好的结合，形成统筹协调、支持创新、活

泼有序的良好局面。

（一）充分发挥体制优势，形成全国发展一盘棋。

新型基础设施的发展涉及多个领域、多种设施、多方主体，单纯依靠市场力量难以消除基础设施发展中的盲目性，容易形成供给过热、低水平重复建设。政府要加强统筹协调，大力引导支持，使基础设施适应经济社会发展需要，防止发展碎片化。要健全宏观管理部门和各行业主管部门共同参与的协调机制，强化各领域新型基础设施之间的技术融合、互联互通和智能交互，促进数字资源的开放共享和整合利用。此外，还要以需求为导向，强化区域协同、全国布局，优化空间布局和供给结构，提升基础设施的整体发展效能。

（二）积极调动市场力量，打造社会广泛参与格局。

新型基础设施技术创新性强，发展模式和商业模式多处于探索期，投资回报存在明显的不确定性，高科技企业将成为新型基础设施发展的最重要力量。在这种情况下，为充分激发市场和民间的投资活力，一方面，要营造良好市场环境，通过深化体制机制改革、降低市场准入门槛、明确监管规则等措施，吸引更多社会企业参与新型基础设施的建设和应用发展；另一方面，要丰富资金投入渠道，根据不同基础设施发展阶段、投资规模、建设周期、盈利能力、带动效应等特点，发挥财政资金引导带动作用，发展多种融资组合方式，引导社会资本参与新型基础设施建设。

（三）科学把握发展规律，探索创新政策支持体系。

新型基础设施具有鲜明的技术经济特点，要建立与之发展相适应的新型政策支持体系。一是强化数据治理体系建设。推动出台《数据安全法》、《个人信息保护法》的配套规定，明确数据分级分类、安全审查等具体制度和要求，推进不同基础设施之间的数据资源共享和开放，促进数据有序流动。二是强化标准体系建设。提出合理布局基础设施重点领域标准，积极开展设施互联互通标准建设，加强信息基础设施和传统基础设施的标准融合和统一，促进设施的互联互通和共享复用。三是推动绿色节能发展。通过制度建设，加强基础设施之间的协同和合作，强化新型基础设施能耗管理，推进先进节能低碳技术的应用推广。四是加强安全保障制度建设。提出建立安全评估评测机制、可靠性保障机制，完善安全保障责任制度等措施，把安全发展贯穿于新型基础设施建设全过程，防范和化解潜在风险，确保基础设施安全稳定运行。

来源：国家发展改革委官方微信（2021-11-30）
原标题：《系统布局新型基础设施 夯实现代化强国先进物质基础》

作者：余晓晖 中国信息通信研究院院长

黄荣怀：在线教育数据安全与个人隐私保护的五个建议

2020年6月18日，“在线教育数据安全与个人隐私保护”国际网络研讨会召开。研讨会由联合国教科文组织教育信息技术研究所（UNESCO IITE）、农村教育研究与培训中心（UNESCO INRULED）、阿拉伯教科文组织（ALECSO）、北师大智慧学习研究院（SLIBNU）、国际智慧学习环境协会（IASLE）联合召开。

北京师范大学黄荣怀教授对本次网络研讨会做总结。针对在线教育数据安全与个人隐私保护，提出了五个建议：

建议1：在线教育的价值应进一步得到关注。确保包容性和公平的优质教育，促进人人享有终身学习机会”是教育2030可持续发展议程的目标。在线学习是实现这一教育目标的基础，它不仅适用于紧急时期的教育，也适用于未来教育。

建议2：数据安全与个人隐私保护刻不容缓。在线学习过程中，个人数据保护的基本知识，如设置设备、注册在线学习平台、通过平台学习等，对个人数据安全具有重要意义。为了促进在线学习中个人隐私的保护，政府的政策标准、行业的技术保障体系以及其他利益相关者的行为都应该共同为学习营造一个安全的环境。

建议3：在线学习是培养数字公民的重要途径。数字公民拥有有效利用信息技术与他人沟通、参与社会、创建和消费数字内容的知识和技能。在线学习已经成为学生学习的典型场景，在线学习的行为、习惯、观念等必然会影响他们的生活。引导学习者以适当的礼仪参与在线学习，可以培养有准备、有目的和有技能的数字公民。

建议4：网络空间中的合作学习助力提升协同技能。个体通过彼此之间的互动和他们所生活的环境来创造意义。在线学习不仅仅是浏览内容，而是与内容、同伴、教师和环境进行互动。因此，学生可以利用工具和技术在网络空间与同伴和教师交流，同时了解如何在交流过程中保护自己的个人数据。

建议5：融合数字学习与传统教学以支持弹性教学。学生可以自由选择时间和地点、数字资源、教学方法、学习活动和支持服务，这是未来的弹性学习模式。在线学习与传统学习的融合是弹性学习的前提。各界应共享对融合的研究，包括融合过程中的个人资料保护，这将为人类带来光明的未来。

成果链接：《在线学习中的个人数据和隐私保护：面向学生、教师和家长的指导手册》

2020年6月18日举行的“在线教育数据安全与个人隐私保护”国际网络研讨会上，发布了《在线学习中的个人数据和隐私保护：面向学生、教师和家长的指导手册》。该手册由北京师范大学智慧学习研究院发起（SLIBNU），与联合国教科文组织教育信息技术研究所（UNESCO IITE）、联合国教科文组织农村教育研究与培训中心（UNESCO INRULED）共同完成。指导手册确定了以下有关在线学习中如何保护个人数据和隐私的五个方面：

1. 在线学习前准备好设备和工具。在线学习前设置设备、管理网络设置、选择和安装工具，确保良好的学习环境是保障个人数据的基础。手册给出了有关这些问题的多种建议和解决方案。

2. 在登入学习平台时保护个人数据。注册和登录到学习平台需要学习者创建一个可靠的密码，保护密码和生物特征信息，以创造一个安全的在线学习环境。具体来说，在公共电脑上注册和登录时，应特别注意不要保存登录信息、不要在电脑屏幕上留下敏感信息、删除个人痕迹、禁用储存密码的功能等。

3. 浏览学习平台时保护个人隐私。对于参加 LMS 的课程，在线学习过程中利用个人学习服务，使用搜索引擎，识别本地服务，具体的解决方案和实践步骤都在这一部分进行了阐述，本节还讨论了如何备份重要数据。

4. 在使用社交网络工具学习时，确保个人资料的安全。在使用社交网络工具时，要注意合理利用网络研讨会，负责地在线讨论和在论坛发帖，安全上网等，针对这些问题的具体建议已经给出。

5. 在线学习结束后清理个人数据。在完成在线学习后，学习者需要做出是否删除数据的决定。本节讨论了如何删除数据和停用个人帐户的建议和方法。

来源：北京师范大学 2020-06-29

作者：黄荣怀 北京师范大学智慧学习研究院院长、互联网教育智能技术及应用国家工程实验室主任

吴砥：增强感知能力，保障绿色上网，推动可信应用，健全应用监管

一、教育新基建的提出背景和政策要点

我国教育信息化经过1.0时期的“三通两平台”和2.0时期的“三全两高一大”等建设，各方面均取得较大发展，整体水平显著提升，教育信息化处于向全新阶段跃迁的关键节点。2018年12月，中央经济工作会议首次提出，“新型基础设施建设”主要是围绕5G、人工智能、工业互联网等新技术构建。

在此背景下，2020年10月，十九届五中全会明确提出，要建设高质量的教育体系，对教育行业的发展提出了更高要求。教育行业是新型基础设施建设的一个典型场景，《教育部等六部门关于推进教育新型基础设施建设构建高质量教育支撑体系的指导意见》（以下简称《指导意见》）于今年（备注：2021年）7月正式发布，主要强调到2025年基本形成结构优化、节约高效、安全可靠的教育新型基础设施体系。

教育新基建具有重要意义，一方面，教育新基建能有力支撑高质量教育体系建设，近几年教育信息化的发展成果，尤其是疫情期间的情况，突出显示了基础设施的重要作用。另一方面，教育作为新基建的重要应用场景，对于融合新技术、壮大新动能、创造新供给、扩大新需求，促进数字化转型具有重要意义。

二、教育新基建支撑构建智慧教育新生态

教育新基建的启动有助于

加快构建智能时代教育的新型生态系统，可在多个维度对教育教学形成助力，包括推动智能学习资源的聚合服务新生态的构建，为学习者构建更具真实性、更强体验性、更深交互性的学习资源环境；

推动教育智力资源服务新生态的构建，教育新基建将有力支撑“专递课堂”“名师课堂”和“名校网络课堂”等三个课堂的应用，通过教育“大资源”服务改变以往的教育资源，尤其是名师资源等智力资源传播范围、服务渠道相对有限的局面，促进优质资源在更大范围内实现共享；

促进泛在学习与终身学习新生态的构建，通过推进教育信息化转型升级，构建真正意义上的泛在学习环境，实现人人皆学，处处能学，时时可学。

智慧教育建设重要的目标之一是构建智能技术支持下的全新教育生态。它不是某个环节或局部的改革，而是整体创新和重构。因此，《指导意见》主要从信息网络、平台体系、数字资源、智慧校园、创新应用和可信安全等六个方面展开，和各地在发展智慧教育时面临的主要难点和痛点问题基本一致。

一是信息网络，主要包括教育专网和校园网络两个方面的内容。

目前，我国已实现中小学校100%联网，但大部分学校的接入带宽难以满足今后的教育需求，尤其是当虚拟现实、4K或8K高清视频等应用走进学校之后。因此，《指导意见》提出的第一个重点方向是信息网络基础设施，其关键是让各级各类学校显著提升校园接入带宽，做到网络地址、域名和用户的统一管理，深入推进IPv6规模部署和应用，实现校园无线网络全覆盖，以及支持校园物联网建设等。且对各级各类学校接入带宽提出更高要求，明确提出“万兆到区县、千兆到校园、百兆到班”，以期为后续应用提供良好支撑。

这方面的一个典型案例是江西省教育专网的建设。教育专网的概念已提出很长时间，但具体该如何建设，有何成效？江西省教育专网四级网络全部建成并组网促进了教育宽带网络提速降费；实现大规模并发使用、统一应用；可以在统一地址、域名、用户等方面发挥作用；同时有助于构建绿色安全、可管可控的教育网络。

二是平台体系，主要包括新型数据中心和学校服务体系等内容。

目前部分学校热衷于建“教育大脑”、教育数据中心等，但脱离实际条件的过多建设可能会造成“低、小、散”等情况。对于普通中小学校而言，独立构建数据中心、机房、“大脑”等，投入大且运维负担重。因此，此次明确提出不鼓励区、县以下地区，以及中小学独立建设数据中心，倡导整合汇聚、集约建设和高效利用，加强教育数据治理，服务于教育科学决策。

此外，《指导意见》还呼吁推动平台开放协同，尽可能整合此前建设的各级各类平台，包括省平台、市平台、区县平台、学校平台等；升级网络学习空间，网络学习空间是教育信息化1.0、2.0阶段逐步发展起来的服务于师生学习的一个主要阵地，目前该空间的作用已逐步显现，但离真正的深度应用普及还有一个过程，还需进一步深化。

这方面的典型案例包括浙江的之江汇教育广场和武汉教育云。前者是一个活跃度较高、规模较大的省级平台，整体应用较好，尤其是其名师网络空间发挥了重要作用。后者在疫情期间发挥重要作用，基于平台的线上教学为武汉平安度过疫情提供了重要支撑。

三是数字资源，主要包括新型资源和工具、资源供给、资源监管三个方面的内容。

开发新型资源和工具，即通过数字资源供给侧改革，提高资源服务质量，并覆盖各教育阶段；优化资源供给服务，即通过数字资源需求侧改革，实现科学归类、多源汇聚、智能检索；提高资源监管效率，健全数字资源的准入、交易、更新和监管等全链条管理。

这方面的典型应用包括中央电化教育馆针对中小学的虚拟实验教学服务系统和国家教育资源公共服务平台。

疫情期间“停课不停学”，中小学生的课堂教学可以通过在线课程来完成，但是实验教学怎么办？为解决这一问题，中央电化教育馆上线了大规模的虚拟实验教学服务系统，覆盖小学、初中、高中等主要学段的理、化、生课程，整体取得较好效果，在实际应用过程中较受欢迎。

同样应运而生的还有国家教育资源公共服务平台体系。早期许多地方为解决资源供给难题，过多地建设资源平台，随后国家加强平台整合力度，建成国家教育资源公共服务体系，使各地可以相对方便地找到所需资源，或实现更加智能化的主动服务。

四是智慧校园，主要包括智慧教学设施、智慧科研设施和智慧公共设施三个方面的内容。

智慧校园是各级各类学校较为关心且在未来三至五年将重点推进的项目，其建设首先需要完善智慧教学设施，包括通用教室、专用教室、个人学习终端和视频交互系统等；其次需建设智慧科研设施（主要针对高校），包括科研实验改革、科研资源共享和科研协同创新等；此外，还需部署智慧公共设施，包括图书馆、体育馆、食堂、宿舍等设施，实现平安校园、健康校园、绿色校园。例如，在明厨亮灶的基础上，进一步实现智能化餐厅：构建食材供应链管理和师生健康档案，为师生定制最适合个人的健康食谱等。

以华中师范大学为例，华师大新建成一栋智慧教育大楼，集成了一批具有不同功能的智慧教室，能以多种方式支撑不同形态的教学。另一个案例是武汉市第十一中学，该校在五年的建设探索过程中，基本上实现了信息化教学的常态化，实际效果良好。

五是创新应用，包括普及教学应用、创新评价应用、拓展研训应用和深化管理应用等。

其中，教学和严训应用主要针对教师；评价应用主要针对学生；管理应用主要是对学校的管理体系。

在这方面，一个典型的案例是银川市第十五中学的“互联网+3571讲学稿”教学模式，即教学3阶段、课前预习5环节、课堂教学7步骤、课后巩固1过程。通过这一模式，该校确实做到了基于互联网改革全校教学结构，实现整体流程重组。

另一个典型案例是第二批国家“智慧教育示范区”创建区域之一的南昌市。该市已大规模实现了高中学业水平的机考，显著降低了考试成本，同时也屏蔽了可能出现的考试作弊等现象，尤其是其在考试评价改革方面的探索已走在行业前列。

还有一个案例是长沙市通过数据驱动的综合素质评价。中小学生的综合素质评价是教育工作的重点，也是难点。长沙市长期以来推进综合素质评价改革工作，为每一所学校生成教育质量综合评价报告。通过评价引导学校改善教育教学方式减轻学生学业负担。

在研训方面，宁夏回族自治区可作为典型案例，该区也是国家“互联网+教育”示范区，目前已完成全区将近7万名教师的在线信息素养测评，同时进行过程跟踪。通过这一举措，宁夏自治区教师的信息素养水平近两年快速提升。

此外，宁夏自治区的教育数据治理能力也值得肯定。在省一级的行政单位中，能够做到全区教育大数据综合汇聚治理，实现多级教育驾驶舱等服务的很少，而宁夏通过构建智能教育数据管理大平台，已初步实现这一应用。

六是可信安全，主要包括增强感知能力、保障绿色上网、推动可信应用、健全应用监管等四个方面的内容。

安全的重要性不言而喻，而安全相关技术的进步也为教育改革提供了新路径。例如，区块链技术的进步有助于实现数字学位证书的发放。这在国外已有成功案例，国内也有一些地方开始尝试，如湖南省的职教系统已开始建设职教区块链。

通过以上六个重点方向的建设，未来的教室将更为智能化、个性化和泛在化，未来教师将具有更好的信息技术能力、扎实的教学能力和专业功底，而未来教育将以学习者为中心，形成更加开放的教育生态系统，它必然是面向人人、适合人人的新型教育生态，可以实现差异化的教学、个性化的学习、精细化的管理、数据驱动的教学研究，以及智能化的管理服务。

来源：教育信息化资讯（2021-09-07）
原标题：《教育新基建支撑区域智慧教育新生态》

本文根据华中师范大学教授、教育部教育信息化战略研究基地（华中）常务副主任吴砥在2021全球智慧教育大会的报告整理

童莉莉：5G智慧校园的网络安全需求与智能解决方案研究

新冠肺炎疫情对全球线下教育活动造成重大影响。联合国称，新冠肺炎疫情导致了有史以来最大的“教育中断”，世界正面临一场“世代性的灾难”，学校长期停课将进一步加剧学习机会的不平等，国际社会必须采取“大胆措施”，积极应对这场危机[1]。在此背景下，以 5G、人工智能为代表的新一代信息技术使得家校学习空间与网络空间深度融合，在学校、家庭和社会等多个环境中对教育带来巨大赋能。然而，新技术的应用具有两面性，新技术带来教学便利的同时，也引发了安全风险，做好教育应用安全保障是保证智慧校园健康发展的基本前提。本文就智慧校园的安全风险进行剖析，并提出安全架构与实施方案参考。

一、智慧校园业务概述

智慧校园是以物联网为基础的智慧化校园工作、学习和生活一体化环境，以各种应用服务系统为载体，将教学、科研、管理和校园生活进行充分融合 ，利用摄像头、无线传感器等采集设备，结合人工智能、物联网和大数据等技术手段，对环境和人群信息进行严密采集和全面分析，并将分析结果运用于学校的教学、管理、科研等方面，从而提升各项工作的效率和质量[2]。应用 5G、人工智能（AI）等技术的智慧校园系统由下至上可分为终端层、网络层、数据与能力平台层，以及智慧校园服务层，如图 1 所示。终端层涉及手机终端、虚拟现实 / 增强现实（VR/AR）终端、教学仪器终端、各类传感器等；网络层是端到端的 5G 网络，包括无线基站、边缘计算节点（MEC）、承载网络、5G 核心网络，以及从基站到核心网络的 5G 网络切片；数据与能力平台层包括 AI 平台、大数据平台、边缘计算平台和安全平台等公共数据和平台系统；服务层由支持 5G 的智能应用系统组成，如远程教学、双师课堂、远程听评课和虚拟实验室等。

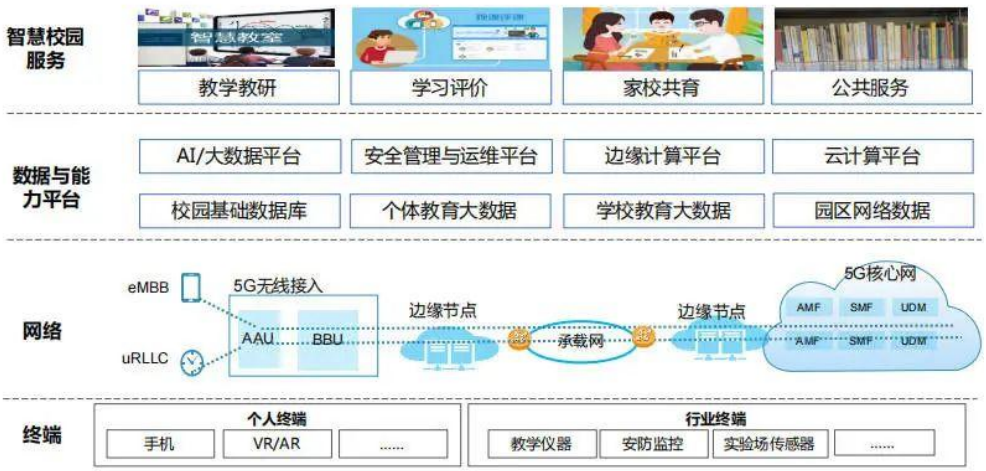


图 1 智慧校园系统模型

5G 校园专网、人工智能等技术赋能智慧校园后，不仅会改变教育传授方式，同时也将使学校的管理工作更加精细化、促进教育公平[3,4]，典型应用场景如表 1 所示。

表 1 5G 和人工智能技术在智慧校园中的典型应用场景

业务场景	场景描述
平安校园	在各级教育单位内，通过 5G 网络覆盖连接，实现以机器人为载体，实现人、车、设备的实时监控管理与智能分析，保障校园安全、高效运行。
全息投影公开课	在边远地区，将名师的真人全息影像同时投射到远端多个听课教室里，打造面对面的自然交互式远程教学体验。
云 AR 交互式教学	在教室内对教学内容进行虚拟仿真，提高教学参与感，实现沉浸式交互学习。
智慧考场	通过网上巡查、巡查指挥、身份认证、作弊防控等系统对考场考风考纪实行实时监控，并提供考务管理系统，满足智能化排考管理需求。支持对突发事件进行实时指挥、事后追溯，对进入考场的考生进行确认，对作弊信号进行甄别和屏蔽，收集、整理系统产生的音视频等非结构化数据，以及考生、监考教师、考点、考场信息等结构数据，服务于教育局、学校、学生和家长。
幼教伴学机器人	基于 5G、AI、人机交互实现学前信息采集，可视化的大数据技术，提供人脸考勤、亲子圈、精彩课堂、班级管理等服务，从幼儿园实际应用场景出发，捕捉幼儿成长的精彩视频图片，让幼儿管理精细化、教学成果数据化、幼儿发展个性化，全方位满足老师、家长、孩子各方需求。
5G 幼儿成长评估	利用 5G+AI 技术，通过伴随式数据收集，辅以教师持续观察记录，为每个孩子形成客观的能力大数据报告，有效解决了学前教育千人一面的现状，满足家长与园所个性化教育教学需求，并为政府幼儿区域化教研提供数据决策支持。

二、网络安全风险

5G 时代的智慧校园面临来自“云（云平台）、管（网络管道）、边（边缘节点）、端（终端）”的安全风险，主要包括业务与数据安全风险、边缘计算安全风险、网络传输安全风险。

2.1 业务与数据安全风险

智慧校园需要部署网络和终端安全管控措施，重点防范不良信息传播风险、隐私泄漏风险，以及业务中断风险。

数据泄露风险：远程同步课堂、远程教研、全息投影公开课等场景中，AR、高清视频面临的数据泄露、隐私窃取风险 [5]。

业务中断风险：全息投影公开课、云 AR 交互式教学等场景中，低时延的性能要求使得复杂安全机制部署受限，而此类业务面临高分布式拒绝服务（DDoS）攻击风险，导致网络可靠性、业务连续性无法保证。

终端管控风险：智慧校园的部署应用，使得学生联网成为必需，而青少年心智不成熟、网络安全意识淡薄，容易网络成瘾，甚至遭受网络诈骗、谣言、陷阱等不良网络内容伤害，需对学生上网行为进行适当管控。

2.2 边缘计算安全风险

智慧校园中部署边缘节点不仅可以提升教学内容和业务处理效率，还可以通过在边缘侧部署第三方应用丰富智慧校园的内涵。节边缘节点需重点防范物理攻击、虚拟化、接口等安全风险。

物理安全风险：MEC下沉到边缘，可能部署到学校园区，物理环境不可控，攻击者可通过近距离接触硬件基础设施，对其进行物理攻击；攻击者可非法访问物理服务器的I/O接口，获得敏感信息，甚至获得MEC平台控制权限。

第三方APP的风险：第三方应用部署到MEC平台，APP安全性不足，易被木马、病毒等攻击。APP存在漏洞，可作为跳板进一步通过接口非法访问用户面功能（UPF），进而入侵核心网；在多个第三方APP入驻MEC的情况下，应用与应用、应用与网元，以及多租户应用下租户与应用间的隔离不当，可能导致租户访问权限越界、数据丢失和泄露等安全风险。

MEC编排和管理系统风险：负责MEC平台和应用管理的软件易被木马、病毒攻击，从而篡改虚拟网络功能（VNF）、APP镜像，在MEP（MEC平台）植入木马等，对MEC管理系统发起拒绝服务、命令注入攻击。

MEC接口安全风险：MEC存在多个外部接口，例如控制面N4接口，用户面N3、N9、N6接口，以及管理面的多个接口，其暴露面多、安全边界多、易受入侵等问题，从外部接口存在多种方式攻击MEC，例如网络嗅探、中间人攻击、流量攻击、暴力破解等。

2.3 网络传输安全风险

校园网除防止来自网络的恶意攻击外，还需考虑低时延场景下使用网络切片的安全问题。远程教学等场景要求时延低，需要使用定制专属切片，应保障专属切片安全，重点防范终端接入切片的安全风险、核心网侧的切片安全风险、切片管理风险。

切片间攻击：通过大量终端或者从网络侧对切片发起 DDoS攻击；单个用户访问多个切片服务，造成切片间数据泄露和篡改；一个切片故障影响其他切片，或消耗其他切片的资源。

未授权接入切片：切片认证被绕过，用户终端（UE）未授权访问切片；恶意用户终端还可能通过合法USIM卡登录切片攻击校园网络。

非法访问：切片key被泄露，攻击者对网元进行非法操作；恶意用户篡改网元 、植入恶意软件。

边界攻击：空口恶意干扰，窃听用户数据信息；仿冒网络应用拒绝特定服务；利用协议漏洞进行web攻击。

三、安全解决方案

对照图 1 所示智慧校园系统模型建设并实现 5G 智慧校园安全解决方案，该方案采用了分层部署模式，包括终端层安全、网络层安全、平台层安全、服务层安全，如图 2 所示。

图 2 智慧校园安全解决方案

3.1 终端层安全

智慧校园中的终端包含学生使用的手机、平台、AR/VR 设备，以及校园中部署的摄像头、传感器等设备。智慧校园的终端安全通常由智慧校园业务运营方主导，终端厂商、网络运营商配合完成。

3.1.1 终端接入认证

为防止海量终端非授权接入可能引发的DDoS攻击风险，并保证授权终端按策略访问指定网络和业务平台，需对接入5G智慧校园的各类终端开展接入认证。实现方法主要有两类。

基于5G网络安全能力：运营商在无线接入（RAN）侧启用基于3GPP终端身份认证标准[6]的终端接入双向鉴权，并在核心网配置终端白名单和机卡绑定，防止非授权终端和合法SIM卡被拔下后插到非法终端上。核心网将网络切片与终端身份、终端可接入的物理位置绑定，确保仅为合法终端且仅在校园内才可合法接入校园专网。

基于智慧校园自有安全认证能力：企业部署AAA（认证、授权、审计）系统为终端提供网络接入的二次认证[7]，对安全性要求高的终端和应用还可以应用内置安全芯片或者安全SIM卡，提升二次认证强度。

3.1.2 终端上网管理

为实现学生终端的上网管理，包括访问站点管理、访问时间管理等，可以通过在终端侧或网络侧部署安全能力实现。

安全终端 ：在终端预置安全管控功能APP，老师和家长可通过管理平台对学生手机进行实时远程管控管理，实现学生的实时定位与轨迹跟踪、应用管理、上网管理，以及手机使用时间管理等功能，引导学生合理安全使用手机。

安全专网 / 网关：在网络侧使用接入点名称（APN）技术方案或者部署安全网关，实现上网安全防护、上网管控等功能。

3.1.3 终端入侵防护

为了防止终端被黑客入侵带来的网络攻击和数据泄露风险，可在终端中内置安全功能，如安全芯片、安全外壳协议（SSH）安全登录、安全传输层协议（TLS）传输加密，以及信令 / 数据加密保护。

3.1.4 终端应用（APP）安全

学生、教师等个人用户使用的终端往往通过APP访问智慧校园中的各类服务，在安装APP前，需确保其通过了监管机构的安全备案和合规检测，不包含隐私窃取、恶意扣费等恶意行为。

3.2 网络层安全

智慧校园的基础网络安全由网络运营商主导，包括无线接入、5G核心网、承载网络和切片等，如果智慧校园涉及自建专网，或在校园侧部署边缘计算节点，那么智慧校园的业务运营方还需要配套部署网络安全方案。

3.2.1 运营商安全能力

为了防范5G网络威胁和攻击，运营商提供基础网络安全保障能力。评估网络架构安全并提供接入网、核心网、边缘节点和互联网出口的端到端安全隔离，根据安全等级给予差异化保护措施。对MEC平台APP进行访问控制和攻击防护，防止MEC节点对核心网的攻击；实现5G网络切片的接入认证、攻击检测、入侵防护和隐私保护；提供网络传输数据的完整性、机密性保护；防止无线空口异常网络攻击，同时防止来自核心网对校园网络、终端的指令攻击［8］。

3.2.2 业务运营方安全能力

对于校园内的网络和业务，智慧校园业务运营方需配套相关安全能力。增强园区内MEC安全能力，需关注MEC 平台物理安全控制，做好平台与APP安全防护，如对MEC平台及其APP软件进行安全加固，使用消息认证码（HMAC）等对MEC平台软件和镜像完整性保护，对敏感数据进

行加密和完整性保护，对MEC APP进行身份认证、授权访问等。增强园区专网安全能力，需在出口边界集中部署安全设备以防止外部威胁，针对云和虚拟化安全，定期执行主机安全扫描，并在特定服务器的管理程序上部署监控软件，以防止虚拟机逃逸攻击等。增强园区5G切片安全能力，访问相应切片时需要用户和运营商进行双重身份验证和授权，确保对切片资源的合法访问和使用。

3.3 平台层安全

平台层提供数据存储分析和服务指令执行等功能，安全通常由智慧校园业务运营方和平台建设运维方主导完成。

3.3.1 数据安全

从数据生命周期环节建立数据安全管理办法并采用不同技术措施保证数据安全。具体而言，针对敏感数据，应具备传输、存储加密能力和数据脱敏能力，并建立数据分权访问、容灾备份、安全审计机制。

3.3.2 应用程序接口（API）安全

平台层机器之间以及平台与上下层之间的通信涉及API调用、组件间操作指令传输等。平台层通信接口安全措施主要包括帐户和密码的维护管理以及通信接口的认证和加密[8]。

3.3.3 云基础设施安全

云基础设施安全包括基础设施组建安全、虚拟机管理组件安全、部署安全和管理平台安全等。智慧校园或其云平台提供方应具备实时的虚拟机监控机制，通过带内或带外的技术手段对虚拟机的运行状态、资源占用、迁移等信息进行监控，支持虚拟机安全隔离，提供虚拟化平台操作管理员权限分离机制，并确保虚拟镜像模板的配置正确性。

3.4 服务层安全

服务层支撑着智慧校园的不同应用，其安全性不仅包括各种应用系统的Web安全、人机交互安全和内容安全，还包括大带宽和低时延等场景下的特殊安全部署。服务层安全通常由智慧校园业务运营方和服务提供方主导完成。

3.4.1 Web安全

通过代码审计、漏洞修补、渗透测试等手段提升软件质量，并部署Web应用防火墙、业务风控等手段，防止针对网站的SQL注入、跨站攻击、网页挂马、口令爆破等安全攻击。

3.4.2 人机交互安全

对服务访问人员进行安全约束和信息控制，如重要敏感操作的多因素认证、基于权限的操作访问控制，以及对运维操作的安全审计等。

3.4.3 内容安全

提供智慧校园消息内容智能审核、过滤和违规内容安全管控，防止涉黄、涉政、涉暴、涉诈骗等低俗、暴力、欺诈信息危害青少年，有效净化了校园网络环境，保护学生身心健康；同时建立数字版权保护系统，对校园内版权内容进行授权使用和传播控制。

3.5 安全管理与运维

除上述分层安全机制外，智慧校园安全管理和业务运营方还需要建立全周期、跨层次的安全管理与运维机制和能力，从管理和技术两方面支撑 5G 智慧校园的安全建设和运行。

3.5.1 安全管理制度与流程

根据安全监管要求和业务发展目标，制定安全管理制度、组建安全团队、明确责任分工，建立覆盖智慧校园全周期的安全风险评估和防护机制；建立业务应急处置流程，在业务发生危害公共安全时及时进行响应、处置；建立数据安全管理制度，根据数据敏感程度级别不同，开展差异化安全管控，实现分类分级管理。

3.5.2 安全技术支撑手段

部署“云、管、边、端”联动的安全能力开展智慧校园内全量数字资产的安全保护，通过专用安全芯片 / 终端，安全检测与审计工具，安全监测、管控与溯源平台，以及内容识别与过滤平台等，实现网络安全防护、业务安全管控、终端安全管理、内容安全保护的目标[9]。

四、安全方案应用实践

依托智慧校园安全解决方案，研究实现智慧校园终端安全管理、智慧校园网络安全防护、智慧校园内容安全防护等产品能力，在校园业务终端安全、网络安全、内容安全等方面应用实践并取得工作成效。

针对终端设备安全风险，智慧校园终端安全管理应用在终端中预置上网管理、入侵防护、APP 安全等能力，结合智能识别、关联学习等人工智能技术实现校园终端设备威胁智能感知、行为智能监测、内容智能过滤等功能。

针对网络安全风险，智慧校园网络安全防护应用通过“云、管、边、端”一体化安全能力，从接入网、边缘节点、校园专网等方面提供终端安全管控、业务可信接入、威胁智能分析、网络立体防护等功能，保障校园专网及边缘节点安全，防止校园网络与 5G核心网相互攻击。

内容安全风险，智慧校园内容安全防护应用提供文本、图片、音视频等内容智能识别技术。智能技术的不良信息识别准确率和审核效率，相比传统技术均实现了显著提高，满足智慧校园业务发展快、保护需求高的要求。

4.1 智慧校园终端安全管理

通过在智慧校园终端设备中预置智能安全管理组件，并结合系统权限、安全合规策略等要素，可帮助学生安全健康地使用5G智慧校园终端。人工智能技术在终端安全管理各个技术环节均发挥重要作用，实现对威胁智能感知处置、内容智能监测清理、行为智能分析告警，并通过集中化态势感知展示供学校管理处置，如图 3 所示。

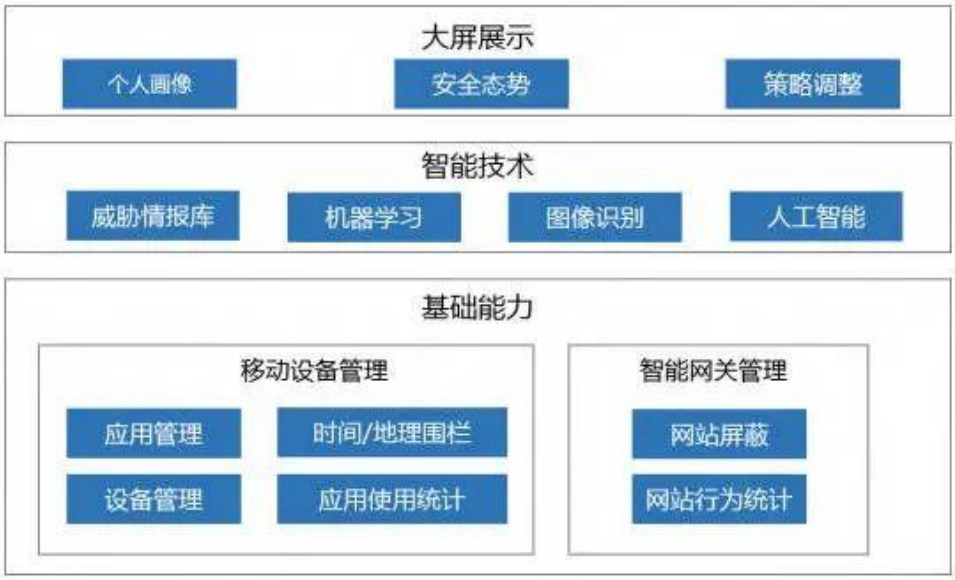


图 3 终端行为安全管理应用

4.1.1 威胁智能感知处置

通过对不良网站、网络攻击等智能识别和失陷检测情报（IOC）生产，可构建并持续完善威胁情报库，并通过智能网关识别校园恶意网站或恶意应用访问过程中入侵风险，针对相关恶意域名进行智能屏蔽。

4.1.2 内容智能监测清理

针对校园网络赌博、贷款等侵害青少年学生的恶意业务，采用机器学习能力进行威胁情报库扩展。结合爬虫、光学字符识别（OCR）、自然语义分析能力，针对网站内容可以实现精准分类，对于涉及网络不良事件的相关网站，进行自主学习分类，实现校园净网。

4.1.3 行为智能分析告警

可提取师生上网个体行为特征，基于人工智能技术，建构网贷、沉迷等针对性的个人画像，辅助校园用网安全管理。

4.2 5G智慧校园网络安全防护

为有效降低5G智慧校园网络安全风险，减少网络攻击、数据泄露、越权访问等入侵行为，可依托“端侧、边侧、云侧”三位一体的安全防护组件实现智能网络安全管控。

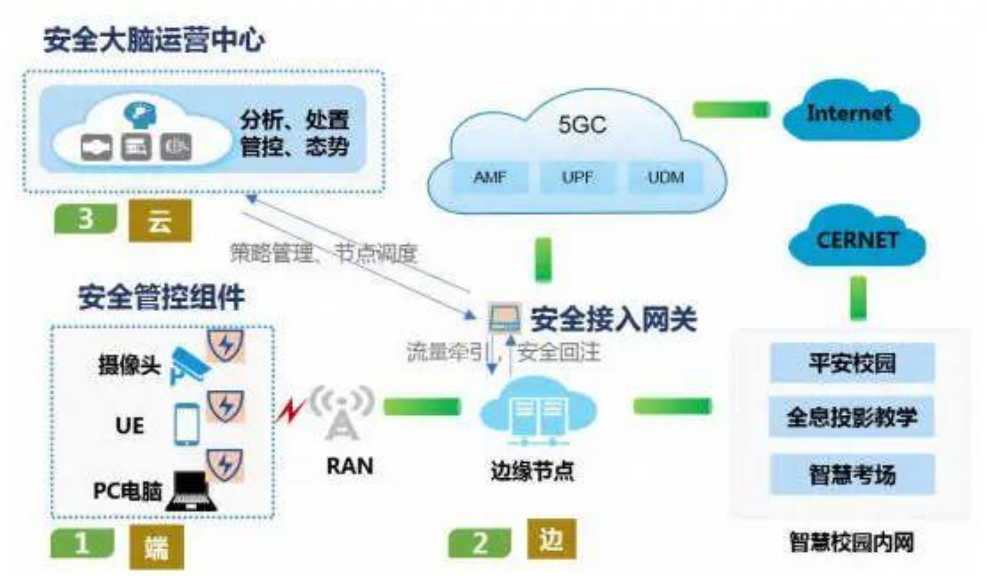


图 4 5G 网络端边云协同联动安全防护应用

4.2.1 端侧：安全管控组件

在手机、笔记本电脑、台式电脑、平板等智能终端上部署轻量级的安全管控组件，实现终端上新爆漏洞、新建文件、进程执行、网络外连、私开终端等行为的监测，从中识别恶意事件并警告或阻断。

安全管控组件可基于设备唯一密钥及动态安全策略，通过智能化安全检测模型、动态安全基线自学习技术、基于群体特征行为的智能分析模型，实现设备认证、动态监测、风险防护、隐私数据保护等功能。

4.2.2 边侧：安全接入网关

安全接入网关在边缘节点侧落地应用，实现业务可信接入、网络立体防护、风险集中管控等效果。通过DNS流量调度技术牵引流量，将智慧校园应用侧暴露面收敛为一处，实现网络流量安全监测、数据资产泄露监测、网站篡改安全防护等功能。

安全接入网关基于AI模型实现已知攻击和未知威胁智能化检测，覆盖全流程攻击链，利用用户和实体行为分析技术（UEBA）等技术实现数据异常行为泄露风险分析，结合自主训练智能引擎识别并防止0day漏洞攻击，实现业务安全托管。

4.2.3 云侧：安全大脑

安全大脑可基于威胁情报实现深层次安全关联分析，借助AI智能分析能力，实现对安全接入网关的策略配置和编排调度；通过对收集信息的深度分析，结合态势感知和编排能力，完成对应安全能力的调度及安全处置。

4.3 5G智慧校园内容安全防护

不法分子借助网络产品以非法营利为目的大规模传播涉黄、涉暴、涉贷、诈骗等不良信息

内容，给心智尚未成熟的学生群体造成了严重的身心威胁。通过目标检测、人脸识别、文本分类、图片识别和富媒体内容识别等技术，建立内容安全防护系统，覆盖多种业务场景、识别多样违规类型、统一审查标准、提升审查实效，实现智能、精准、高质的内容管控。可有效地净化5G智慧校园应用服务网络环境，保障广大师生身心健康。

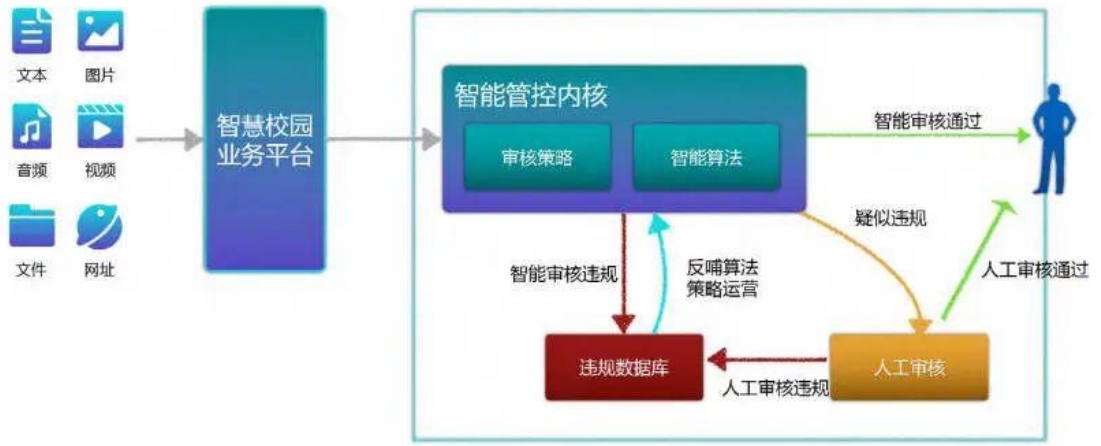


图 5 内容安全防护系统

4.3.1 文本内容安全

采用前沿的自然语言处理算法，结合海量的敏感关键词库，快速准确识别各种变形文本，打造快速、高质量、稳定的文本审核过滤服务。可有效识别、过滤政治敏感、暴恐违禁、色情低俗、违规广告、恶意辱骂低质灌水等内容，并进行审核、管控。

4.3.2 图片内容安全

采用智能的图像视觉算法，结合海量的违规图像数据进行训练建模，对传播的图片内容进行安全检测，识别违规不良内容，可快速识别色情图片、暴恐图片、恶意广告内容、涉政图片、低俗文化图片等。

4.3.3 音频内容安全

使用高效的语音识别算法构建语音识别引擎，将语音内容进行转译处理，可准确识别不良语音内容，可有效支撑多种口音普通话、地方方言识别，可通过音频特征识别技术识别特色场景的语音特征。

4.3.4 多媒体内容安全

使用综合的多媒体算法，处理视频（直播、点播等）、文件、网页等复合型多媒体内容，智能审核其包含的文本、图片、音频等内容。视频内容安全审核包括视频标题、画面截帧、OCR识别字幕、自动语音识别（ASR）。文件内容安全审核可支持常用办公文件类型及压缩包。网页内容安全审核包括对网址页面中包含的图片、文字、视频进行分别提取和审核。

4.3.5 绿色上网

面向校园绿色上网需求，提供安全、省心、放心的上网防护服务。通过电话、消息、流量数据联动，全面识别诈骗、骚扰、黄赌毒等不良信息，提供安全上网防护。通过教学设备、个人终端的安全配置，合理管理上网时间，一键关停游戏APP，防止未成年人上网沉迷、游戏沉迷，清朗网络空间，呵护未成年人健康成长。

五、结束语

5G以及人工智能、大数据等新技术在智慧校园领域的融合应用可显著提升学习空间智能化、泛在化水平，促进优质教育资源按需供给和教育均衡发展，是网络强国、数字中国、智慧社会的重要组成部分。

5G时代智慧校园的安全保障应以促进学生身心健康发展，保障校园活动有序开展，与周边网络信息基础环境和谐交互为基本目标。在提升安全能力实践中，充分发挥人工智能技术的作用，提升智能安全效果。在5G智慧校园安全解决方案实践应用中，结合内容智能识别、数据深度关联、场景态势感知、业务机器学习等人工智能技术，实现了终端行为管理、网络安全防护、内容健康管控等安全保障。借助人工智能技术，提升网络、数据、业务、终端应用安全，加强智慧校园安全风险的监测、预警和处置能力。

智慧校园的安全建设运行离不开内生能力与外部支撑。智慧校园建设运营方应与电信运营商、网络安全服务专业机构等联合开展边缘节点安全管理、网络信息安全管控和威胁情报共享等合作，不断提升抗风险和应急处置能力。

→ 来源：邱勤, 路晓明, 童莉莉, 叶荣伟. 5G智慧校园的网络安全需求与智能解决方案研究[J]. 人工智能, 2022(02):57-67.

邱勤，ISO国际标准化组织召集人，中国移动通信集团科协安全学部专家。
路晓明,ISO/IEC SC27专家.全国协作业务关系管理标准化技术委员会委员。
童莉莉,北京师范大学教育学部副教授，硕士生导师。教育部教育信息化战略研究基地（北京）副主任，互联网教育智能技术及应用国家工程研究中心系统化教育治理实验室主任。
叶荣伟，中移（杭州）信息技术有限公司，高级工程师

全国未成年人互联网使用情况

2022年11月30日，共青团中央维护青少年权益部、中国互联网络信息中心（CNNIC）联合发布《2021年全国未成年人互联网使用情况研究报告》。《报告》基于对全国31个省（自治区、直辖市）的小学、初中、高中及中等职业学校26349名未成年学生、13283名家长、1632名教师的抽样调查，从未成年人互联网普及、网络接入环境、网络使用特点、教育监管、网络安全与权益保护等方面，分析未成年人互联网使用主要趋势及特点，有针对性地提出有关建议。主要发现如下：

未成年人互联网普及率持续提升，网络依赖程度有所下降

2021年我国未成年人互联网普及率达96.8%，较2020年提升1.9个百分点，未成年人过度上网情况有所改善。未成年网民工作日平均上网时长在2小时以上的比例为8.7%，节假日平均上网时长在5小时以上的比例为9.9%，分别比2020年下降2.8个百分点和2.3个百分点。未成年网民对互联网的主观依赖程度和家长认为孩子上网时间过长的主观感受都呈下降趋势。42.0%的未成年网民认为自己对互联网没有依赖心理，较2020年提升3.3个百分点;27.3%的家长认为孩子上网时间过长，较2020年下降4.5个百分点。

未成年人网络使用存在城乡差异，农村未成年网民教育管理相对不足

农村未成年网民上网设备相对单一、长时间上网情况更突出、使用休闲娱乐类应用比例较高、使用学习资讯类应用比例较低。比如，除手机外，农村未成年网民使用笔记本电脑、平板电脑、智能手表等设备上网的比例均明显低于城镇未成年网民;节假日平均上网时长在5小时以上的，农村比城镇高3.9个百分点;经常在网上玩游戏、看短视频的，农村比城镇分别高6.0和8.3个百分点;经常使用网络学习、搜索引擎和看新闻的，农村比城镇分别低8.9、6.8和5.0个百分点。调研发现，超四成农村未成年网民没有和父母双方一起生活，比城镇高近两成。这一方面使得更多农村未成年人需要使用手机进行亲情联络，另一方面也导致农村未成年网民在上网用网上缺少家长的监督约束。只有38.3%的农村未成年网民表示上网时长经常受到家长限制，比城镇低10.4个百分点。

互联网平台监管初见成效，青少年模式有待进一步推广完善

新修订的《未成年人保护法》增设“网络保护”专章，对网络游戏、网络直播、网络音视频、网络社交等网络服务提供者提出未成年人保护相关的明确要求。2021年未成年网民经常在网络上听音乐、玩游戏、看视频、看短视频、看直播的比例，较2020年均有不同程度的下降。2021年6月，中央网信办在全国范围内开展“清朗·‘饭圈’乱象整治”专项行动，推动未成年网民经常参与网上粉丝应援行为的比例从2020年的8.0%下降至2021年的5.4%，减少近三分之一。2019年以来，各大视频、短视频、社交、游戏等网络平台陆续推出青少年模式，在帮助未成年人减少网络依赖和网络不良信息方面发挥了积极作用。调查发现，尽管85.9%的未成年人和91.6%的家长都知道青少年模式，但设置过青少年模式的未成年人和家长均不到五成，四成家长认为青少年模式效果不够明显，一成未成年网民表示对青少年模式不满意。未成年人游戏账号管理趋于严格，但有31.9%的未成年网民使用家长账号玩过游戏。

视频平台成为获取信息重要渠道，对未成年人价值观塑造的影响值得关注

视频、短视频平台已成为当前未成年人获取新闻事件、重大消息的主要渠道之一，其内容质量会对未成年人思想观念产生潜移默化影响。接近半数未成年人通过抖音、快手、B站等短视频、视频平台获取社会重大事件信息，略高于各类官方媒体网站。但当前未成年网民对于网络信息来源渠道的鉴别意识还不高，未成年短视频用户中，会有意识地区分短视频信息是官方还是自媒体发布的不到一半。38.3%的未成年网民在上网过程中遭遇过不良或消极负面信息，其中占比最高的是炫耀个人财富或家庭背景(21.2%)，宣扬不劳而获、躺平思想(16.3%)等消极负面的内容。值得注意的是，随着互联网平台监管工作的有序推进，血腥暴力、唆使犯罪、歪曲历史、淫秽色情等不良信息得到有效控制，但消极负面信息对未成年人世界观、人生观、价值观的影响不可小觑。

网络安全环境持续改善，新风险隐患不容忽视

随着一系列网络环境专项整治行动的开展，以及家长和学校对未成年人网络安全教育管理的日益重视，网络安全环境持续改善，未成年人网络素养有所提升。比如，未成年网民在过去半年内遭遇过网络安全事件的比例为25.5%，较2020年下降1.7个百分点;79.8%的未成年网民知道可以通过互联网对侵害自身不法行为进行权益维护或举报，较2020年提升5.7个百分点;66.3%的未成年网民会在日常生活中关注未成年人上网相关的新政策新法规。与此同时，网络安全方面也出现一些新风险隐患。一是部分未成年网民网络安全防范意识不强，20.0%的未成年网民对于防范网络诈骗、信息泄露、网络谣言等没有概念，且年龄越小，防范意识越弱。二是网络安全陷阱也在“与时俱进”，与2020年相比，未成年网民中遭遇账号密码被盗、电脑或手机中病毒等传统问题的比例持续下降，但遭遇网上诈骗、个人信息泄露等形式多变、“套路满满”的新问题的比例略有升高。三是新型上网设备存在信息安全风险，智能手表、智能台灯、智能音箱、词典笔等新型上网设备在未成年网民中迅速普及，功能丰富多样，但在信息内容、隐私安全等方面标准不一，56.0%的未成年网民、56.8%的家长和79.0%的教师表示对这类设备的信息安全风险感到担心。

家庭对未成年人上网影响重大，提升家长网络素养实有必要

家庭是未成年人上网的主要场所，家长对未成年人上网的管理和引导方式直接影响未成年人上网行为和习惯。上网时长是否受到家长限制、是否与父母共同生活，显著影响未成年网民的网络依赖程度。经常受到家长限制的未成年网民，对互联网有依赖心理的比例为10.0%，比不受家长限制的未成年网民低27.4个百分点。与父母双方共同生活的未成年网民中，其认为自己非常依赖或比较依赖互联网的比例为16.2%，而与父母中的某一方或其他亲属生活的未成年网民中，这个比例分别为22.4%和21.3%。家长自身的上网行为和网络素养也对未成年网民有直接影响。在家长经常玩手机游戏或看短视频的家庭中，未成年人工作日上网2小时以上、节假日上网5小时以上的比例，分别比家长不经常玩手机游戏或看短视频的家庭高5.6和8.5个百分点;还有31.9%的未成年网民使用家长账号玩过游戏。26.8%的家长表示对互联网懂得不多，7.4%的家长表示自己不会上网，25.3%的家长认为自己对互联网存在依赖心理，难免会影响对子女上网的管理效果。

来源：中国青年网 2022-11-30

《2021年全国未成年人互联网使用情况研究报告》

我国网络安全工作成就综述

没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。

党的十八大以来，我国网络安全政策法规体系不断健全，网络安全工作体制机制日益完善，全社会网络安全意识和能力显著提高，网络安全安全保障体系和能力建设加快推进，为维护国家在网络空间的主权、安全和发展利益提供了坚实的保障。

▼ 健全网络安全政策法规体系

2022年6月1日，网络安全法正式施行五周年。 这部我国网络安全领域的基础性法律，对保护个人信息、治理网络诈骗、保护关键信息基础设施、网络实名制等方面作出明确规定，成为我国网络空间法治化建设的重要里程碑。

近年来，我国加快推进网络安全领域顶层设计，在深入贯彻落实网络安全法基础上，制定完善网络安全相关战略规划、法律法规和标准规范，网络安全“四梁八柱”基本确立。

加强战略部署。 发布《国家网络空间安全战略》，颁布数据安全法、个人信息保护法、《关键信息基础设施安全保护条例》等一系列法律法规，出台《汽车数据安全管理若干规定（试行）》等政策文件，让网络安全工作在法治化轨道上运行。

强化网络安全风险防范能力。 实施《国家网络安全事件应急预案》，有效提升网络安全应急响应和事件处置能力;建立网络安全审查制度和云计算服务安全评估制度，发布《网络安全审查办法》《云计算服务安全评估办法》，有效防范化解供应链网络安全风险;出台《数据出境安全评估办法》，提升国家数据出境安全管理水平。

健全网络安全国家标准体系。 印发《关于加强国家网络安全标准化工作的若干意见》，对网络安全国家标准进行统一技术归口，制定发布340余项网络安全国家标准，推动发布多项我国主导和参与的国际标准，我国网络安全标准国际话语权和影响力显著提升。

▼ 共筑网络安全防线

当前，网络空间与实体社会深度交融，数字化程度不断加深，为经济社会高质量发展增添动能的同时，也带来了许多前所未有的挑战。

积极应对风险挑战，共筑网络安全防线，近年来，有关部门不断提升个人信息保护工作水平和监管力度。

2019年以来，中央网信办等四部门联合开展App违法违规收集使用个人信息专项治理，对存在严重违法违规问题的App采取公开通报、责令整改、下架等处罚措施，有力震慑了违法违规行为。

针对非法利用摄像头个人隐私画面、交易隐私视频、传授偷拍技术等侵害公民个人隐私的行为，2021年5月起，中央网信办会同有关部门开展摄像头等黑产集中治理工作，督促各类平台共处置相关违规有害信息3万余条，处置涉违法交易等活动的账号5600余个，下架违规产品3000余件。

网络安全为人民，网络安全靠人民。 维护网络安全是全社会的共同责任，需要政府、企业、社会组织、广大网民共同参与。

自2014年以来，中央网信办等部门连续9年在全国范围内举办国家网络安全宣传周活动，以通俗易懂、百姓喜闻乐见的方式，宣传网络安全理念、普及网络安全知识、推广网络安全技能，有力推动全社会网络安全意识和防护技能的提升。

党的十八大以来，各方面齐抓共管的良好局面已经形成，凝聚起全社会建设网络强国的强大实践力量，进一步筑牢全民网络安全的“防火墙”，亿万人民群众在网络空间拥有更多获得感、幸福感、安全感。

▼ 加快人才培养提升防护能力

2022年7月1日，在中央网信办指导下，网络安全学院学生创新资助计划正式启动。 天融信科技集团、奇安信集团、蔚来、蚂蚁集团、中国互联网发展基金会网络安全专项基金作为资助方，将连续五年资助1200名学生开展创新研究。

网络空间的竞争，归根结底是人才竞争。党的十八大以来，各地各部门出台系列政策举措，推动加快网络安全学科建设和人才培养进程，推进网络安全教育、技术、产业融合发展。

创新网络安全人才培养机制。 《关于加强网络安全学科建设和人才培养的意见》印发，设立网络空间安全一级学科，实施一流网络安全学院建设示范项目。 目前，国内已有60多所高校设立网络安全学院，200余所高校设立网络安全本科专业，每年网络安全毕业生超过2万人。

中央网信办会同相关部门指导武汉市建设国家网络安全人才与创新基地，打造国家网络安全人才高地、创新高地、产业集聚区。 建设国家网络安全教育技术产业融合发展试验区，探索网络安全教育技术产业融合发展的新机制新模式。

各地工作同样成果丰硕。 在北京，国家网络安全产业园区重点推动网络安全产业集聚发展、网络安全核心技术突破;安徽合肥聚力发展网络安全产业，行业龙头企业迅速发展，领军企业高频出现，创新型中小企业快速成长;全国首个跨省域国家级网络安全产业园区落地成渝，打造引领西部网络安全产业创新发展的高地……

一项项强有力的政策举措，助力网络安全人才培养、技术创新、产业发展的良性生态正在加速形成。

来源：新华网 2022-09-05

原标题：《筑牢全民网络安全“防火墙”——我国网络安全工作成就综述》

第50次《中国互联网络发展状况统计报告》

2022年8月31日，中国互联网络信息中心（CNNIC）在京发布第50次《中国互联网络发展状况统计报告》（以下简称：《报告》）。《报告》显示，截至2022年6月，我国网民规模为10.51亿，互联网普及率达74.4%。

▼ 互联网基础建设全面覆盖，用户规模稳步增加

《报告》显示，在网络基础资源方面，截至2022年6月，我国域名总数为3380万个，“.CN”域名数为1786万个，IPv6地址数量为63079块/32，较2021年12月增长0.04%。在信息基础设施建设方面，截至2022年6月，我国千兆光网具备覆盖超过4亿户家庭的能力，已累计建成开通5G基站185.4万个，实现“县县通5G、村村通宽带”。三家基础电信企业的固定互联网宽带接入用户总数达5.63亿户，比上年末净增2705万户；其中100Mbps及以上接入速率的固定互联网宽带接入用户达5.27亿户，占总用户数的93.7%。三家基础电信企业发展蜂窝物联网终端用户16.39亿户。

▼ 网民规模持续提升，网络接入环境更加多元

《报告》显示，在网民规模方面，我国网民规模持续稳定增长，较2021年12月新增网民1919万，互联网普及率较2021年12月提升1.4个百分点。农村地区互联网基础设施建设全面强化，我国现有行政村已实现“村村通宽带”，推动农村地区互联网普及率较2021年12月提升1.2个百分点，达58.8%。在网络接入环境方面，网民人均每周上网时长为29.5个小时，较2021年12月提升1.0个小时。网民使用手机上网的比例达99.6%；使用台式电脑、笔记本电脑、电视和平板电脑上网的比例分别为33.3%、32.6%、26.7%和27.6%。

▼ 互联网应用持续发展，短视频增长最为明显

《报告》显示，截至2022年6月，我国短视频的用户规模增长最为明显，达9.62亿，较2021年12月增长2805万，占网民整体的91.5%。即时通信用户规模达10.27亿，较2021年12月增长2042万，占网民整体的97.7%。网络新闻用户规模达7.88亿，较2021年12月增长1698万，占网民整体的75.0%。网络直播用户规模达7.16亿，较2021年12月增长1290万，占网民整体的68.1%。在线医疗用户规模达3.00亿，较2021年12月增长196万，占网民整体的28.5%。

中国互联网络信息中心（CNNIC）副主任张晓认为，今年上半年，我国互联网发展稳中有进。本次《报告》呈现了2022年上半年我国互联网发展的以下特点：

一是互联网基础建设持续推进，助力网民规模稳步提升

2022年上半年，我国5G网络规模持续扩大，已经累计建成开通5G基站185.4万个，实现“县县通5G、村村通宽带”。与此同时，为更好地满足老年和特殊人群需求，工业和信息化部已组织完成对452家网站和APP的适老化、无障碍化改造和评测，让智能生活有温度、无障碍。截至2022年6月，我国网民规模达10.51亿，较2021年12月新增1919万；互联网普及率达74.4%，较2021年12月提升1.4个百分点。农村地区互联网普及率为58.8%，较2021年12月提升1.2个百分点。

二是互联网应用持续发展，部分应用用户规模实现增长

面对复杂严峻环境和诸多风险挑战，我们仍能看到部分互联网应用用户规模在今年上半年实现一定增长。本次《报告》显示，截至2022年6月，我国即时通信用户规模达10.27亿，较2021年12月增长2042万，占网民整体的97.7%。网络新闻用户规模达7.88亿，较2021年12月增长1698万，占网民整体的75.0%。网络直播用户规模达7.16亿，较2021年12月增长1290万，占网民整体的68.1%。短视频用户规模为9.62亿，较2021年12月增长2805万，占网民整体的91.5%。

三是网络安全形势持续好转，遭遇安全问题用户比例进一步下降

2022年上半年，工业和信息化部纵深推进APP侵害用户权益专项整治工作，累计完成630万次APP检测，实现对我国主流应用商店在架APP的全覆盖，APP治理能力显著增强。本次《报告》显示，截至2022年6月，63.2%的网民表示过去半年在上网过程中未遭遇过网络安全问题，较2021年12月提升1.3个百分点。遭遇个人信息泄露的网民比例为21.8%，较2021年12月下降了0.3个百分点。

→ 来源：中国互联网络信息中心，2022-08-31

《中国网络诚信发展报告2022》

2022年中国网络文明大会网络诚信建设高峰论坛于2022年8月29日在天津举行。论坛期间发布了我国网络诚信发展年度报告——《中国网络诚信发展报告2022》（简称《报告》）。

《报告》由中国网络社会组织联合会、北京邮电大学教育部战略研究基地、中国经济信息社联合编撰，记录了2021年以来我国网络诚信建设取得的新进展新成就，分析了网络诚信领域面临的新问题新挑战，提出了加强网络诚信建设的思考建议。

▼ 网络诚信领域面临的问题挑战

一是算法滥用问题凸显，欺骗和误导消费者。算法本身是一种技术手段，合理地利用算法，可以提升经营效率，为消费者提供更丰富、优良的产品和服务。但近年来，部分市场主体滥用算法侵害消费者合法权益，比如，流量劫持、刷单炒信、操纵榜单等，引起了社会广泛关注。

二是恶意使用技术手段，网络诈骗花样翻新。在公安机关持续严厉打击下，不法分子利用传统电信、互联网等技术渠道，通过发送短信、拨打电话、植入木马等手段，实施电信网络诈骗行为已得到有效遏制，但近年来不法分子又瞄准互联网行业的新业态、新模式、新人群，恶意使用网络新技术进行网络诈骗，且呈现出精准化、智能化、场景化的趋势，诈骗方式更趋隐蔽，令治理难度增加。

三是利用平台垄断优势，开展不正当的竞争。拥有掌控平台规则、技术手段、数据和算法优势的一方，通过并购投资、限制竞争等行为控制流量和生态，对其他中小型企业的发展形成挤压，侵害用户权益。

四是流量变现急功近利，直播带货良莠不齐。出于对经济利益的过度追求，对“流量变现”的急功近利，个别明星艺人、网红达人没能正确认识作为公众人物应承担的社会责任，由此导致的直播带货售假、虚假交易等言行失范行为，造成负面影响。

五是资本“绑架”粉丝经济，网络“饭圈”乱象频发。部分粉丝的追星行为因资本的无序扩张而演变成以“爱”为名的违反社会规则和道德准则的不当行为，进而形成网上盲目应援打榜、刷量控评、群体对立、互撕谩骂等网络“饭圈”乱象，破坏清朗网络生态，对此群众反映强烈。

来源：人民政协网，2022-08-30

数字中国发展评价指标体系

2022年7月23日，在福州举行的第五届数字中国建设峰会开幕式上，国家互联网信息办公室发布《数字中国发展报告（2021年）》。

由国家网信办组织有关单位，结合国务院办公厅电子政务办公室、国家统计局、工业和信息化部、科技部、教育部、农业农村部、人力资源社会保障部、国家卫生健康委、交通运输部、中央党校（国家行政学院）、中国互联网络信息中心（CNNIC）等部门和机构的统计数据和评价指数，开展了2021年数字中国发展水平评估工作，重点评估了31个省（区、市）在数字基础设施、数字技术创新、数字经济、数字政府、数字社会、网络安全和数字化发展环境等方面的发展水平。同时，为了解各地区群众在数字中国建设中的感受情况和意见建议，首次开展了数字中国发展情况网络问卷调查活动。评价指标如表所示。

数字中国发展评价指标体系

一级指标	二级指标	重点评估要素
数字基础设施	网络基础设施普及水平	5G用户普及情况、5G基站覆盖情况、千兆宽带接入用户情况等
	网络基础设施服务能力	固定宽带下载速率、移动通信网络平均下载速率、互联网省际出口带宽、重点网站IPv6支持水平等
数字技术创新	创新投入	ICT相关产业R＆D人员及经费投入情况等
	创新产出	ICT相关高新技术企业情况、信息领域学术成果影响力等
数字经济	数字产业化	ICT相关产业营业收入、IT项目投资情况等
	产业数字化	农业生产信息化水平、企业两化融合水平、网上零售交易情况等
数字政府	政务服务	在线政务服务情况、省级行政许可事项网上办理水平、网上政务服务能力等
	政务网站和新媒体建设	政务网站无障碍水平、政务新媒体影响力等
	共享开放	政务数据共享与数据开放水平
数字社会	教育服务	多媒体教室、师生网络学习空间等教育服务情况
	医疗服务	远程医疗、预约诊疗等医疗服务便捷水平
	生活服务	电子社保卡、生活服务线上缴费便捷水平等
	交通服务	数字出行服务便捷水平
	法律服务	电子诉讼等法律服务情况
	城市管理	城市管理信息化平台建设情况、城市管理信息化平台运行水平等

续表

一级指标	二级指标	重点评估要素
网络安全	产品和服务安全	重要信息系统网络安全防护水平等
	网络安全监测和应急能力	网络安全检查评估、网络安全监测预警、网络安全应急等
	网络安全教育技术产业融合发展水平	网络安全人才培养、网络安全教育技术产业融合发展、网络安全宣传等
	国家网络安全重大工作支撑情况	网络安全重大工作支撑
数字化发展环境	统筹协调	政策环境建设、网络安全工作责任制等
	建设投入	信息化项目建设投入情况、网络安全经费保障等
	示范引领	重点领域先行先试情况等
网民评价（参考）	互联网应用使用情况	基本互联网应用使用情况
	数字基础设施感知情况	网络基础设施建设、5G网络使用体验等
	数字公共服务感知情况	数字防疫应用、数字政务服务、新媒体平台政务公开、数字出行服务等
	网络空间治理感知情况	网络空间治理、网络安全知识等

注：网民评价暂作为参考指标，不计入综合得分，拟在优化完善后下一年度正式纳入指标体系。

■ 数字基础设施建设评价情况

北京、上海、浙江、江苏、天津、广东、重庆、河南、山东、四川等10个省（市）位列各省（区、市）数字基础设施建设水平全国前10名。上述地区超前部署5G、千兆宽带等数字基础设施，推进数字应用服务普及完善，构建区域数字化发展的优势基础环境。

■ 数字技术创新评价情况

北京、上海、广东、江苏、天津、浙江、湖北、四川、陕西、福建等10个省（市）位列各省（区、市）数字技术创新水平全国前10名。上述地区积极发挥创新要素聚集优势，围绕人工智能、大数据、云计算、量子信息、区块链、虚拟现实等数字技术前沿领域，构建产学研用融合的创新生态体系，推动产业链创新链融合发展，构建区域数字技术创新高地。

■ 网络安全建设评价情况

山东、北京、天津、上海、湖北、四川、浙江、广东、重庆、辽宁等10个省（市）位列各省（区、市）网络安全建设水平全国前10名。上述地区强化重要信息系统网络安全防护，加快推进网络安全监测预警和应急体系建设，积极开展网络安全知识教育，培养网络安全专业人才，推动提升网络安全整体风险防范能力。

→ 来源：中国网信网 2022-08-02，《数字中国发展报告（2021年）》

新基建竞争力指数指标体系

▼ 新基建竞争力指数指标体系

一级指标	新型网络基础设施指数		新型应用基础设施指数			新型行业基础设施指数					
二级指标	感知网络发展指数	宽带网络发展指数	大数据发展指数	云计算发展指数	人工智能发展指数	智慧能源设施指数	智慧医疗设施指数	两化融合设施指数	智慧教育设施指数	智慧交通设施指数	智慧农业设施指数

新型网络基础设施指数：包含感知网络发展指数和宽带网络发展指数 2 个二级发展指数，主要反映新一代信息网络发展情况。

新型应用基础设施指数：包含大数据发展指数、云计算发展指数和人工智能发展指数 3 个二级发展指数，主要从要素投入角度来衡量新一代应用基础设施的建设情况。

新型行业基础设施指数：包括智慧能源设施指数、智慧医疗设施指数、两化融合设施指数、智慧教育设施指数、智慧交通设施指数、智慧农业设施指数 6 个二级发展指数，主要评价在网络基础设施和应用基础设施支持下形成的各类行业基础设施发展情况。

来源：《中国新基建竞争力指数白皮书（2020）》
编制单位：福建省经济信息中心 、清华大学互联网产业研究院、长威信息科技发展股份有限公司

▼ 《中国新基建竞争力指数白皮书(2021年)》

《中国新基建竞争力指数白皮书(2021年)》显示，广东、江苏、北京的新基建竞争力指数在80以上，浙江、福建、上海、山东、河南、安徽、四川的新基建竞争力指数分布在70到80之间，其他省份的新基建竞争力指数均在65到70之间。中国新基建竞争力较强的地区主要集中在粤港澳大湾区(广东)、长三角城市群和京津冀城市群。

从该白皮书可见，中国新基建总体呈现“一快”“三个更加”“一个引领”的发展态势。

“一快”，即新型基础设施建设已驶入快车道。2020年，中国新基建竞争力指数为70.1，在工业互联网、大数据中心、5G、人工智能等新基建重点领域投资规模约1万亿元(人民币，下同)。在多重政策红利催化下，“十四五”时期中国新基建相关投资有望达十万亿元量级。

“三个更加”，即信息基础设施网络更加完善，融合基础设施应用更加广泛，创新基础设施支撑更加有力。截至2020年底，中国已建成全球规模最大的5G网络，物联网行业规模达万亿元，工业互联网产业规模达3万亿元；卫星互联网进入了与地面通信系统互补合作、融合发展的宽带互联网时期，朝着低轨化的方向发展，在轨卫星数量居世界前列；人工智能、区块链已从概念进入落地应用阶段，专利申请数量均位居世界首；云计算、数据中心市场保持高速增长，企业上云深入推进。

“一个引领”，即东部地区引领全国新基建的发展。中国各省区市围绕自身特点和战略定位陆续出台相关行动计划和政策举措，大力推动新型基础设施建设，初步形成东部引领、竞相发展的良好态势。东部地区凭借资金、人才、技术以及市场上的绝对优势，新基建建设超前、应用广泛、业态创新活跃，整体发展水平较高。

→ 来源：中国新闻网 2021年4月22日

国家安全教育知识要点-网络安全

2020年9月，教育部印发了《大中小学国家安全教育指导纲要》（以下简称指导纲要）。指导纲要明确了国家安全教育主要内容，包括政治、国土、军事、经济、文化、社会、科技、网络、生态、资源、核、海外利益等12个领域安全，以及太空、深海、极地、生物等4个不断拓展的新型领域安全，围绕各领域安全的重要性、基本内涵、面临的威胁与挑战、维护的途径与方法等方面提出学习要求。附录国家安全教育知识要点在正文基础上，拓展出一级二级知识点，提出起点学段和学科覆盖建议，对每个领域安全主要学习内容进行具体化细化，帮助各学段各学科准确把握、系统融入。

网络安全包括网络基础设施、网络运行、网络服务、信息安全等方面，是保障和促进信息社会健康发展的基础。面临网络基础设施安全隐患和网络犯罪等威胁。维护网络安全必须践行“没有网络安全就没有国家安全,没有信息化就没有现代化”的理念，强化依法治网、技术创新、国际合作等，树立网络空间主权意识。

网络安全				
知识要点		开始讲授起点学段建议	中小学（含中职）学科覆盖建议（大学在公共基础课中全面落实，各学科专业主动结合相关内容落实）	
一级知识点	二级知识点		主要学科	全学段相关学科
事关国家安全和发展、事关国家网络主权、事关广大人民群众生活、事关经济社会稳定运行		初中	信息科技	思政、信息技术、外语
基础设施安全	关键设施、设备安全	初中	信息科技	信息技术
运行与服务安全	防攻击、防渗透	小学	信息科技	信息技术
	信息系统连续可靠运行	初中	信息科技	信息技术
	网络软件产品安全	初中	信息科技	信息技术
信息安全	数据传输安全	小学	信息科技	信息技术
	网络信息加密	小学	信息科技	信息技术
	有害信息监察监管	小学	信息科技	信息技术、思政
	防范网络诈骗、网络暴力	小学	信息科技	信息技术、思政

续表

网络安全				
知识要点		开始讲授起点学段建议	中小学（含中职）学科覆盖建议（大学在公共基础课中全面落实，各学科专业主动结合相关内容落实）	
一级知识点	二级知识点		主要学科	全学段相关学科
网络信息影响民众意识形态和价值取向	不良不实网络信息误导民众价值取向风险凸显	初中	信息科技	信息技术、思政
	网络意识形态安全问题凸显	初中	信息科技	信息技术、思政、语文
	民众网络安全意识薄弱，应对网络安全风险能力亟待提升	初中	信息科技	信息技术、思政、语文
	网络舆情事件呈现高发态势	高中	信息技术	思政、语文
关键基础设施面临的安全隐患增大	关键基础设施的低国产化和产品应用现状加大了隐患风险	初中	信息科技	信息技术
	针对国家关键信息基础设施攻击的威胁增大	初中	信息科技	信息技术、思政
网络犯罪呈现高发态势	网络违法犯罪造成重大危害	小学	信息科技	信息技术、思政
	网络窃密高发、后果严重	小学	信息科技	信息技术、思政
依法治网	全面推进网络空间法治化	初中	信息科技	信息技术、思政
	加强网络安全信息收集、分析、通报和应急处置	大学		
	建立监测预警与应急处置制度	大学		
	建立网络安全审查制度	大学		
网络管理	采取监测、记录网络运行状态和网络安全事件的技术措施	大学		
	采取数据分类、重要数据备份和加密等措施	初中	信息科技	信息技术
技术支持	技术创新，确保安全技术领先	初中	信息科技	信息技术
	加强保护国家关键信息基础设施的安全	初中	信息科技	信息技术
宣传培训	建立维护国家网络主权的思维	初中	信息科技	信息技术、思政
	加强社会网络安全意识的教育	小学	信息科技	信息技术、思政
国际合作	网络空间治理	高中	信息技术	思政
	网络技术研发和标准制定	高中	信息技术	
	打击网络违法犯罪	初中	信息科技	信息技术、思政、外语

来源：教育部 2020-10-27

影响高等教育信息化安全发展的趋势/关键技术/未来场景

2021年2月16日，《2021年 EDUCAUSE 地平线报告(信息安全版)》在EDUCAUSE官网正式发布，报告介绍了影响全球高等教育信息化安全发展的六种重要趋势、六项关键技术与实践、四种未来场景，并列举了高等教育信息化安全的七个经典案例。EDUCAUSE 高等教育版地平线系列报告已成为国际高等教育发展的风向标和研究热点。

影响高等教育信息化安全发展的六种重要趋势

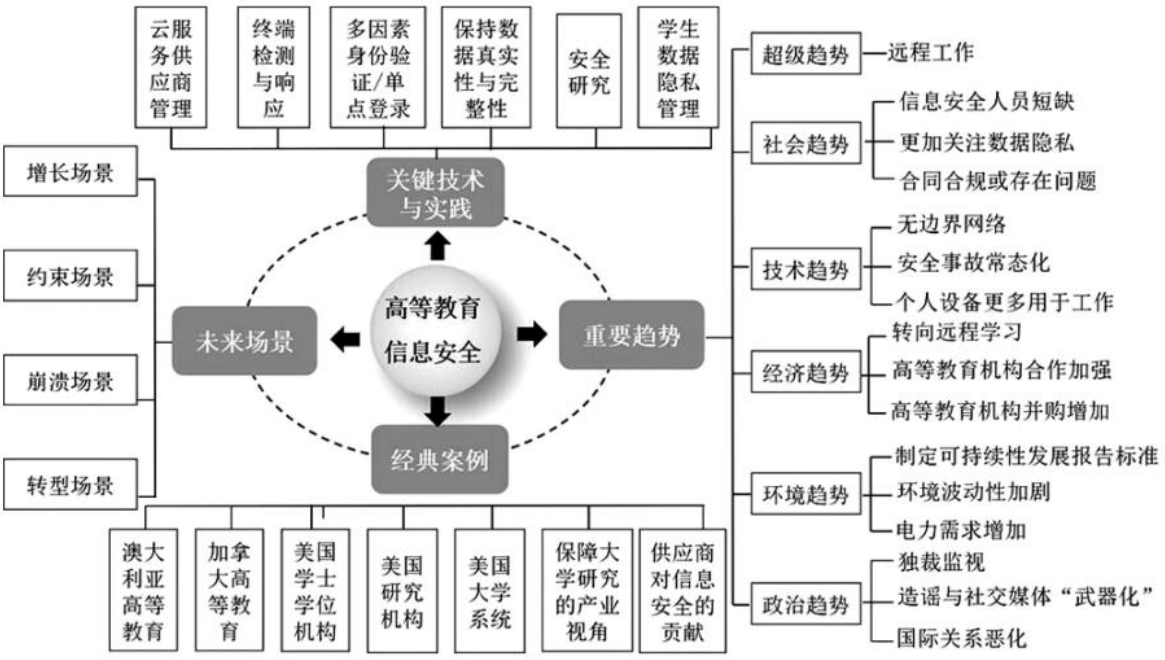
六种重要趋势	描述
1.超级趋势：转向远程工作	远程工作极为重要，而且在其他趋势中也会出现，所以被单独列为“超级趋势”。
2.社会趋势：信息安全人员供不应求，数据隐私和合同签订引发关注	社会趋势主要为三个方面。一是信息安全人员短缺。二是更加关注数据隐私。三是合同合规或存在问题。
3.技术趋势：个人设备更多用于工作，网络安全事故成为常态	技术趋势主要为三个方面。一是无边界网络。二是安全事故常态化。三是个人设备更多用于工作。
4.经济趋势：资金供给不足，高等教育机构间合作与并购不断加强	经济趋势主要为三个方面。一是转向远程学习。二是高等教育机构合作加强。三是高等教育机构并购增加。
5.环境趋势：环境波动性加剧，需制定可持续发展报告标准	环境趋势主要为三个方面。一是制定可持续发展报告标准。二是环境波动性加剧。三是电力需求增加。
6.政治趋势：造谣与社交媒体“武器化”趋势明显，国际关系恶化	政治趋势主要为三个方面。一是独裁监视。二是造谣与社交媒体“武器化”。三是国际关系恶化。

▼ 影响高等教育信息化安全发展的六项关键技术与实践

序号	关键技术与实践
1	云平台供应商管理：远程学习和工作的首选解决方案
2	终端检测与响应：避免安全事故的重要网关
3	多因素身份验证 / 单点登录：保护数据安全的强大工具
4	保持数据真实性与完整性：实现信息安全的重要方式
5	安全研究：研究机构助力信息安全的有效途径
6	学生数据隐私管理：提升学生对高校的信任程度

▼ 影响高等教育信息化安全发展的四种未来场景

1	增长场景，即高等教育信息化安全蓬勃 发展 。
2	约束场景，即高等教育信息化安全在不 同方面被削弱 。
3	崩溃场景，即无法控制的变革力量使高 等教育信息化安全走向崩溃 。
4	转型场景，即高等教育成功转型并建立 了新的信息安全发展范式 。



《2021年EDUCAUSE地平线报告(信息安全版)》整体框架

表 高等教育信息化安全的经典案例

区域	概述
澳大利亚高等教育	疫情带来的远程工作和学习的“新常态”深刻改变了我们的生活、工作和互动方式，虽然这在2019年是一种必要的、临时的反应，但疫情过后也应采用远程工作和学习，因为这种方式更高效、成本更低，也被越来越多的师生所接受。
加拿大高等教育	技术有助于社会进步，但必须谨慎引导安全使用，否则很容易造成伤害。高等教育应发挥领导作用，确保数据的安全性，研究数据治理问题，找到信息安全问题的解决方案。
美国学士学位机构	年轻一代的大学生意识到泄露私人信息带来的潜在影响，并会确认数据存储、使用的信息。高等教育机构应该认识到这一事实，并采取相应的措施，如保障数据收集、处理和存储的政策和程序都有完整的记录，培训员工关于数据管理的法律要求和正确使用数据的方法。
美国研究机构	研究机构虽然在创造经济价值、培养未来人才方面发挥了重要作用，但是在合作、监管、隐私等方面面临着风险。
美国大学系统	信息安全的未来趋势和关键实践将影响大学系统。终端设备数量的大量增加，为设备的管理和检测工作带来诸多困难。在许多机构中，管理数据隐私是首席信息安全官的职责，但大学系统的复杂性要求这些职责由独立的办公室来管理。COVID－19大流行加剧了网络犯罪分子通过各种阴谋手段带来的挑战，为保证高校系统网络的完整性，应提高信息系统的适应性和防护性。
保障大学研究的产业视角(企业视角)	供应商不能只销售产品，而应该努力帮助机构建立符合其具体要求的有效的网络安全环境。可采取的措施包括：供应商与高等教育机构合作；寻找快速见效的安全工具；使用“云智能”实现高效启动、运行和管理；使用集成化和自动化工具以提高安全管理的效率。
供应商对信息安全的贡献(企业视角)	高等教育机构对网络安全的需求空前高涨，供应商应努力帮助高等教育抵御网络攻击。终端检测和响应能力是高等教育机构的必备能力，安全供应商可以在不同领域为高等教育提供终端检测和响应服务。此外，供应商还可以通过提供云服务、安全工具、自动检查和修复功能等，帮助高等教育抵御网络攻击。

来源：钟秋菊等. 提升高等教育信息化安全：趋势、变革与挑战——《2021年EDUCAUSE地平线报告（信息安全版）》要点与启示[J]. 高教探索. 2021,(10):47-54+101.

天津河西区改造网络新基建，提升教育网络监管、防护、专业化服务能力

党的十九大以来，教育信息化进入2.0阶段，全面开启了智慧教育的新时代。加快推进教育信息化是实现教育现代化的必由之路。天津市河西区作为全市的政治中心、文化中心、商务中心和创新驱动先行区，近年来，牢牢把握教育信息化发展的历史机遇，深刻认识信息技术对教育发展的革命性影响，坚持以数据为驱动，聚焦教学方式变革、智慧校园建设、教育治理智能化建设，因势而谋、应势而动、顺势而为。目前，河西智慧教育实践已取得一定成果，初步呈现出“校园智慧化、治理精准化、资源共享化、教学个性化”的河西智慧教育发展新样态。

河西区依托区域教育云服务体系和智能技术及教育大数据，推进教育教学方式变革和教育治理智能化建设，构建以七大工程为主要内容的“慧育河西、智联河西、至善河西”的三大行动计划，全面推进智慧教育示范区建设。

一、区域智慧环境构建设计

1. 建设目标

高水平建成“5G+智慧教育”支持系统建设，推进中小学智慧校园全覆盖，实现教学环境智能化提升。完善“5G+智慧教育”的个性化学习支持系统和智慧课堂支持系统，通过创新实验、虚拟现实、智慧感知、物联网、智能终端等智能技术，实现动态感知、体验学习，重构智慧化学习环境。

2. 建设内容

构建智能认证系统。加快河西区教育认证体系建设和应用推广，实施实名统一身份认证和校园智慧化应用推广，逐步实现一人一号、跨校使用、课堂与校园场景适用。为教师、学生、家长提供便捷的集互动教学、考勤门禁、行为轨迹、成绩分析、就餐消费、图书借阅以及家校互动等功能于一体的智慧系统，同时，全程伴随式自动数据采集，为各主管部门提供教育大数据决策辅助帮助，推进本区各类教育规范有序接入教育生态系统。

网络新基建提升改造。融合IPv6、Wi-Fi6、5G等技术，全面优化区域网络覆盖能力，完善教育城域网运行管理机制，将区内所有教育单位纳入统一管理。建立网络缓存、加强网络安全、改善网站加速等配套设施设备。提高师生人均互联网带宽，提升网络监管、防护、专业化服务和运行保障能力。

全面推进数字校园建设。推进基于物联网的校园感知环境、智慧安防、智慧后勤建设，提升教学安全管理等级。推进学科数字实验室、创新实验室、虚拟实训环境、数字场馆、智慧学习中心、人工智能体验式学习中心建设，探索智能化课堂教学模式研究与应用推进，开展“智慧教育”示范校建设。

建设5G+智慧教育支持系统。构建5G全覆盖下的优质精品教育资源共享应用场景，依托高速低延迟特性常态化实施“同上一节课”远程扶贫帮困计划。建设超高清视频制作中心，打造若干精品优质资源建设示范校，引入高质量社会教育制作资源协助课程开发与资源建设。

建设智慧教育大脑。与天津市政府、市教委、河西区政府现有的数据中心与机房共享合作，建设以“校云朵”为代表的校级微型数据总控机房，推进公有云与私有云深度融合，建立市、区、校一体化混合机房，形成分布计算、动态存储、算力均衡的集容灾、应用于一身的智慧教育大脑。

二、建设的策略

1. 加强领导，明确责任

智慧教育示范区建设总体采用“政府引导，智库规划，企业参与，学校应用”的保障机制。成立领导小组、顾问小组、执行小组、专家小组、督导小组，建立统筹协调、分工协作、定期调度工作机制，明确各方成员单位的职责分工，定期召开研讨会、联席会、专题会、推动会等，共同推进项目规划、经费保障、技术研发、融合应用、经验推广等工作。与科研院所、高校、企业深度合作，组建专家咨询委员会，为“智慧教育示范区”建设提供智力支撑、专业指导与服务保障。

2. 同步建设，互通共享

河西区作为智慧教育先行区，要在互联互通、共建共享、智慧服务等方面下足功夫，率先实现智慧教育示范区建设。坚定有力地推进智慧教育高质量发展，与教育教学改革相向发展，共同打造智慧教育示范区。三大行动维度、七大实施工程优化布局，提升能级，彰显品质，既唱好主题曲，又唱好大合唱，同步建设，互通共享。

3. 多元投入，完善保障

全面落实党对“智慧教育示范区”创建工作的全面领导，把“智慧教育”摆在全区优先建设的战略地位，充分发挥政府与企业两方面的作用，为该项目提供包括教育经费、专项经费、直达资金、校企合作在内的共计2.5亿经费保障，为推进智慧教育示范区建设提供良好的政策环境、产品服务与发展空间。

4. 创新机制，强化监督

坚持试点先行、典型引路的推进机制，总结提炼先进经验与典型模式，形成以点带线绘面的发展路径，发挥辐射引导效应。建立市场准入机制，引导智慧教育标准规范体系的建立、应用示范和推广，保障智慧教育的规范建设。区教育监督部门建立、健全长效监督机制，将区域智慧教育相关工作指标纳入督导指标，并根据相关规定进行专项督导检查，并将评估结果作为重要依据纳入绩效考核体系，确保示范项目工作高效、有序地开展。

5. 梯次推进，以用促建

根据项目目标和当前需求，将三大行动维度七大实施工程推出重点，制定推进建设的时间表、路线图，细化分解，建立台账，组织专人循序渐进，一个项目一个项目，一个阶段一个阶段地在实践运用过程中按梯次扎实推进。

三、构建智慧育人环境实践

1. 天津市第二新华中学

第二新华中学大数据中心

2021年5月，世界智能大会期间，作为天津市唯一的基础教育学校代表，天津市第二新华中学接待20余家央视媒体采访，中国新闻网、光明网、每日新报、中国青年网、海外网、天津广播、津云新闻等众多媒体纷纷对天津市第二新华中学科技赋能智慧校园建设，打造阅读明智、创新启智、美育冶智、书法益智、劳动开智、体育强智、数据汇智、非遗传智、思政培智、安防护指等十个智慧教育新场景进行专题报道。

第二新华中学智慧足球俱乐部

2021年7月，由中央电教馆主办的全国智慧教育示范区经验交流会在天津召开，天津市第二新华中学作为河西区智慧教育唯一样板学校，接待了全国各地近500位专家教师参观，实地了解学校在教育管理、学生管理、课堂教学、课程开发、资源应用等方面的数字化与智能化建设成果。在人工智能背景下，学校坚持思想引领，立足党建优势，高度重视党史学习的推动，学校不断探索直播教学平台的构建，通过自研平台使直播常态化。通过“专递课堂”的形式，实现了津陇两地“同上一节课，共享一名师”的思政课教学模式，开辟了远程优质教育资源共享的新路径。智能是硬件，智慧的关键则是人，未来已来，第二新华中学用“幸福教育”的文化理念来引领智慧校园发展，比理念和认识更重要的是决心，比方法和方案更关键的是担当。学校将建立学生未来发展规划指导机制，根据学生的兴趣、爱好、特长等，利用大数据为其未来成长提供专业选择、报考方法、专业热度、生涯规划等服务。第二新华中学正在教育信息化的路上不断实践，不断创造，以小我之力量带动教育现代化的发展。

2. 天津市第四中学

天津四中目前建有能够为全校提供信息化服务的数据中心，可实现校园内数据资源的存储，能够保证数据实时更新和高度一致，为实现“网上办公、网上管理、网上教学、网上服务”提供全面的系统支持。校园网络以万兆光纤为主干，实现有线无线全覆盖，通过联通、长城宽带、教育网等多条线路接入互联网，总出口带宽1000M。

目前学校已实现班班有无尘交互式电子白板一体机、电子班牌、电子书包柜、云桌面授课系统。建成精品多媒体录播教室1间，云镜教室20间。搭建智慧教育互动课堂、建设智舵创新实验室、校园电视台、微课录课室等。为教师配备了数位手写板、笔记本电脑、微课录课笔等设备。除了在常规教室的信息化建设上下功夫，学校还新建了物、化、生、史、地、政等9间学科教室，同时在原有理化生实验室基础上进行提升，开设3间理化生创新实验室，建立了数字地球、科技创新工作室、VR未来教室、STEAM工作室、机器人活动室、智慧书画教室等特色学科教室。

天津市第四中学创客教室

四中拥有多种教学辅助设施并通过校园智能物联网系统对这些设施进行统一管理和控制。如基于物联网技术的校园智能一卡通系统、校园门禁智能控制系统、车辆出入管理系统、空调控制系统校园一卡通系统、校园门智能控制系统、访客系统、周界防护报警系统、安防消防报警系统、车辆出入管理系统、停车场管控系统、智能节能管理系统、明厨亮灶系统、图书借阅系统、智能测温系统等。实现教育教学辅助设施资源远程、集中、直观统一查询和控制，保障了教学辅助设施资源的高效利用。

在完善硬件设施的同时，四中不断丰富软件平台，加强资源建设，提升应用水平。学校搭设了校园综合管理系统，通过统一身份认证平台，实现系统单点登录，提高了智慧校园系统的安全性和一站式信息服务能力。学校积极推动人人通平台、网络教研平台的常态化使用，做到教师学生人人会用、常用。学生在平台上熟练地提交作业、开展读书活动、交流讨论，教师在平台上教研、备课、分享资源。学校配备有智慧课堂、大数据精准教学、智能排课、教务管理、选课及教学评价等各种应用系统，开通了学科网、组卷网等多项资源服务，为教师开展信息化教学提供了有力支持和保障。依托人工智能、大数据等技术和多种优质资源，学校实现了考试、测练、练习等全场景数据的采集，通过人工智能的知识图谱和习得顺序，精准分析每个班级的学业情况和每个学生的学习情况，帮助教师实现精准施教和学生个性化学习，提升了教学效果。

智慧校园不仅为师生提供了良好的智慧学习空间和平台，也为学生生涯规划和成长提供助力。利用大数据技术，帮助学生从不同角度了解自己，深挖学科潜能。利用信息技术手段进行学科潜能测试和数据分析，进而帮助学生寻找自己的兴趣志向，对学生进行选课指导，计划未来学习和职业的发展方向。

来源：天津市河西区教育综合服务中心　原标题：《天津市河西区智慧教育环境的建设与实践》

苏州市教育系统网络安全体系构建策略

在推进教育信息化高质量发展的过程中，苏州市贯彻信息化项目与网络安全“同步规划、同步建设、同步使用”的原则，从网络安全建设与管理相关要素出发，通过减少系统弱点信息泄露、加强信息资产管控和预警监测、推动教育城域网网络基座提档升级等举措，逐步形成具有本地特色的市级教育系统网络安全模式。

苏州市教育信息化工作起步早、发展快，目前全市教育系统互联网资产数量已逾1600个。与此同时，近年来苏州市教育系统网络安全风险漏洞通报数量也一直居高不下，网络安全事件时有发生，成为制约苏州市教育信息化工作进一步提档升级的瓶颈。为此，苏州市教育局高度重视，由教育网络安全和信息化工作领导小组分析网络安全问题根源，研究应对策略，统筹协调全市教育系统网络安全和信息化工作，取得明显成效。

一、苏州市教育系统网络安全现状分析

苏州市教育信息化工作起步早、发展快，目前全市教育系统互联网资产数量已逾1600个。与此同时，近年来苏州市教育系统网络安全风险漏洞通报数量也一直居高不下，网络安全事件时有发生，成为制约苏州市教育信息化工作进一步提档升级的瓶颈。为此，苏州市教育局高度重视，由教育网络安全和信息化工作领导小组分析网络安全问题根源，研究应对策略，统筹协调全市教育系统网络安全和信息化工作，取得明显成效。

对江苏省教育厅、苏州市委网信办2020年度通报的苏州市教育系统网络安全漏洞和事件梳理分析后，发现我市教育系统网络安全管理主要存在以下问题。

（一）网络安全责任意识薄弱

教育系统网络安全人才整体较为匮乏。区域间、学校间网络安全技术与管理水平差异大，未形成专业网络安全队伍。学校网络安全工作人员基本为兼职教师，对承建企业的依赖性高，有的学校甚至将所有系统管理权限悉数交给承建企业技术人员。与此同时，学校网络管理人员、系统管理人员、业务管理人员的网络安全、数据安全意识不足，弱密码、信息泄露事件频发，网络安全责任未压实，存在较大的安全风险。

（二）网管团队业务能力不足

在日常运维过程中，部分学校网络安全工作仅着眼于边界防护，疏于内网安全防护。不少学校采用DHCP实现动态地址分配，且未采用上网认证，一旦病毒、挖矿木马在校园网内大肆传播，很难做到问题的迅速定位和及时有效处置；个别学校未在教师终端安装恶意程序防护软件，让恶意软件的传播有机可乘。

（三）信息资产管控力度不大

一是信息资产集成度不高。基层学校信息系统小、散、乱，同一学校系统间数据割裂现象较为严重，系统整合度不高，承建单位技术水平参差不齐，代码漏洞较多。各区县教育信息化机构采用网站集群方式实现对本地学校网站统一纳管的占比不到50%。

二是信息资产外网暴露面过大。学校信息系统与学校网站一般都开放外网访问，个别学校甚至将数据库服务器直接暴露在外网，软件代码漏洞风险较大。

三是信息资产过程管理制度缺失。大部分学校未建立信息资产过程管理制度，很多停用的信息资产并未进入资产销毁流程。特别是系统经手人员调动后，对于部分前期已建系统未履行交接手续，出现很多游离于网络管理视野之外的“失效资产”“失控资产”“失陷资产”，存在一定的潜在风险。

（四）应急预案实效性不强

各基层学校虽已普遍制定网络安全应急预案，但极少有学校对应急预案的科学性、合理性进行论证分析、实践检验。个别学校在出现网络安全事件后才发现所制定的应急预案流程设计不合理、可操作性不强；各类学校普遍存在应急预案制定后即束之高阁的现象，应急预案实效性不强。

二、苏州市教育系统网络安全工作整改思路

根据应急演练中入侵者的攻击路径（侦察—初步入侵—植入后门—横向移动—达成目的），我们初步确定网络安全体系的构建思路为：

一是要减少系统弱点信息泄露，防范撒网式侦察，让入侵者“筛不到”有价值的信息。

可能泄露的弱点信息主要包括系统漏洞信息和与系统配置、用户账号密码相关的情报信息等。

二是要减少对外发布的系统漏洞，增强风险隐患的主动发现能力，让入侵者“攻不进”。

三是要加强内网防护，防止立体化渗透，让入侵者即便单点攻破，也“打不通”内网其他系统。

四是要加强重要系统对攻击行为的感知，让入侵者“拿不到”核心资产重要数据。

五是要落实敏感信息加密保护要求，入侵者即便非法获取了关键数据，也因难以解密而“看不懂”。

与此同时，还需要通过技术提档升级、组建专业团队集中运维等措施，切实降低基层学校网络管理难度；需要通过网络安全攻防演练，提前发现安全策略中存在的问题与缺陷，实现安全策略科学合理、隐患通报数大幅下降、风险漏洞处置及时有效的管理目标。

三、苏州市教育系统加强网络安全管理的实施举措

（一）加强责任落实和宣传培训，有效减少系统弱点信息泄露

在信息化应用高度普及的今天，学校各业务部门、所有师生都是信息的使用者和生产者。因此，防范信息泄露风险需要采取有效手段，压实网络安全责任，开展广泛宣传培训，增强广大师生网络安全防范意识，形成群防机制，才能取得实效。

1. 完善管理体系。

苏州市教育局制定并出台网络安全责任制考核实施办法，明晰各区县和学校网络安全责任制考核要点，保障网络安全主体责任和监督责任的落实；每年制定《全市教育系统信息化与网络安全工作要点》，明确常态化进行网络安全检查、深入开展网络安全宣传培训等工作任务；出台《苏州市教育信息系统日常监测制度》《苏州市教育系统网络与信息安全事件应急预案》等具体管理制度，规范网络安全工作流程和方法。苏州市教育网信工作领导小组与各区县、各直属单位逐级签订网络安全责任书，层层责任落实、压力传导，使全市教育系统各级网络安全管理人员提高了政治站位和重视程度。通过推进组织机构建设、制度建设、责任落实，市、区、校三级纵向衔接、横向协调的网络安全工作组织管理体系正式形成。

2. 组织网络安全“校园日”系列活动。

苏州市教育局每年年初制定《苏州市网络安全校园日活动实施方案》，部署网络安全宣传工作。在网络安全宣传周，各校深入宣传贯彻习近平总书记关于网络强国的重要思想，宣传相关配套法律法规；充分利用学校LED、板报、校园广播、校园电视台、展板、班会、党务会议、社区宣讲、家校互动、微信公众号、企业微信等方式营造宣传氛围；组织师生收看江苏省教育厅网络安全校园日启动仪式；开展国旗下网络安全讲话、校园日有奖问答、网络安全主题班会、网络安全宣传黑板报评比、网络安全主题短视频比赛等活动。通过各种形式的深入宣传，普及网络安全知识，提升全体师生网络安全意识和防护技能。苏州市电化教育馆(以下简称市电教馆)选取部分学校制作了网络安全校园日专题采访节目，并通过市内电视、地铁、公交、教育局大屏等渠道播出，提升宣传效果。

3. 开展“网络安全师”培训。

苏州市教育局制订学校“网络安全师”的培养计划，将其作为全国智慧教育示范区创建内容的重要组成部分，构建适应未来教育信息化发展需要的网络安全人才队伍。市电教馆结合年度培训计划，面向各单位信息化分管领导、网络管理员、一线教师，通过线上线下相融合的方式持续组织开展各级各类网络安全培训。培训内容包括信息安全、应急响应操作规范、网络安全法解读等，全面提高教育系统各单位网络安全的意识和能力。2021年全市各地区网络安全师培训人数有980人。

(二)加强信息资产管控，有效减少系统漏洞

1. 推行信息资产全生命周期管理。

市电教馆以开展重要时段网络安全保障专项行动为抓手，排查梳理全市教育系统资产，关闭并注销“双非”“僵尸”风险隐患网站等；通过落实责任制考核要求，配合资产探针、人工核查等手段，指导和帮助学校逐步建立信息资产全生命周期档案，规范信息系统、IP地址、域名等互联网资产的采购、上线、运维、销毁等各环节管理，建立健全有效的常态化数据更新机制，支撑网络安全日常管理和形势分析研判，切实解决苏州市教育系统互联网基础资产“底数不清”的问题。

2.缩小信息资产的外网暴露面。

针对仅向教师、学校管理者开放的校级应用系统，责成相关单位按期切换至教育城域网内部访问，同时开通外网访问VPN通道，缩小应用系统的暴露面，降低系统遭受外部攻击的风险。

3.逐步推进敏感信息加密保护。

依据《密码法》相关要求，全面梳理教育系统信息资产中承载的各类敏感信息。根据信息系统的重要性、密码保护紧迫程度，列出敏感信息加密保护需求清单，排定加密保护整改优先级，申请专项经费，力求通过两年时间逐一完成落实整改、清单核销。

4.加强重要信息资产防护。

对访问承载重要信息系统服务器的用户、地址、策略和工具进行有效管控。运维人员采用“VPN+堡垒机”的方式单点登录服务器，通过口令、U盾等多因素认证的方式维护服务器；对系统账号等进行访问控制，对超过安全策略之外的语句和高危操作进行有效阻断；所有操作记录和视频都保存在服务器本地和日志服务器中，以备查证，做到“事前阻断，事中审计，事后可追溯”。

(三)加强预警监测，增强风险隐患的主动发现能力

1.应用态势感知平台进行常规管理。

苏州市教育局于2018年部署态势感知平台，经多次系统升级，目前已通过与其他安全设备(如IDS/防火墙、日志大数据平台等)的联动，构建闭环处置流程，提升了网络安全的整体监测响应能力。自态势感知平台运行以来，监测推送风险地址5万个，阻断高危IP地址400个(其中境外地址300个)，督促基层学校整改网络隐患120起，实现“事态可评估”“趋势可预测”“风险可感应”和“行为可管控”。

2.开展网络安全攻防演练集中检测。

苏州市教育局联合市委网信办、市公安局，定期开展网络安全攻防演练，通过模拟黑客的真实攻击行为，发现网站、信息系统、网站集群中存在的隐患和漏洞，测试各单位安全策

略的有效性及应急处置能力，提升发现问题、整改完善、加强防护的综合维护水平。在“苏州教育网安2021网络安全应急演练”中，技术团队共扫描全市716个教育单位的1317个在网应用系统，重点测试市教育局各处室、直属学校、单位179个信息系统，随机抽查下属市(区)应用系统800余个，共发现问题单位85个，突破率11.85%。随后，市电教馆组织专业团队逐一走访检出问题和漏洞的区域和学校，督促完成整改，指导完善方案。

(四)全面加强信息资产集成，推动教育城域网网络基座提档升级

积极推进网站集群建设与集中运维管理，解决学校网站代码漏洞频出问题。以创建全国智慧教育示范区大平台建设为契机，整合全市各区县、各校、各单位应用系统，逐步采取以区域统一建设、各校共享使用为目标的校级应用系统建设模式，切实解决应用分散、数据割裂、数据安全缺少保障的问题。运用SDN技术重构教育城域网网络基座，加快苏州市教育云网升级改造，实现底层网络硬件资源池化，提高教育云网资源灵活调度，做到云网融合、网随人动、策略随行，为教育系统每一位用户提供专属的网络策略和服务，满足日益严格的数据安全与个人信息保护需求，全面优化和提升教育城域网的安全组网和服务能力，有效解决基层学校内网防护薄弱问题。苏州市教育城域网SDN改造完成后，可实现学校新增设备网络配置策略的自动下发，有效解决基层学校网管专业技术能力不足问题。

网络安全是系统工程，涉及思想观念、人员配备、资金投入、制度执行、技术保障、监督问责等诸多环节，仅靠单个职能部门无法有效实施，必须统一领导、协调各方、形成合力，才能形成政府引导、需求引领、市场主导的良性生态，才能真正落实教育系统网络安全职责，全面优化教育系统网络环境。经过几年来的努力，苏州市教育系统网络安全整体形势明显好转，成功保障了“停课不停学”期间、重要安保任务开展期间全市教育系统网络的安全稳定运行，在近年省、市网络安全责任制考核中取得了较好的成绩。

来源：皇甫绎达，曹海榕. 设区市教育系统网络安全体系构建策略——以苏州市为例[J]. 江苏教育. 2022, (12) :12-15.
皇甫绎达 苏州市电化教育馆网运中心副主任，工程师，主要研究方向为网络工程
曹海榕 苏州市电化教育馆副馆长，高级工程师，主要研究方向为软件工程

温州市打造教育网络安全新高地，护航国家“智慧教育示范区”创建

2021年初，教育部科技司发布了2020年度“智慧教育示范区”创建项目名单，浙江省温州市成功入围，成为教育部第二批、浙江省首个国家“智慧教育示范区”创建城市。

坚持信息技术与教育教学深度融合，建立“大共同体”平台建设推进机制，以区域(学校)智慧教育发展指数和智慧校园建设为主要抓手，以教育“数字大脑”体系建设为创新引擎，以“试点-提升-复制-重构”为推进路径。温州市教育技术中心主任侯元东认为，在“智慧教育示范区”的创建探索中，必须更新教育理念、优化要素环境、创新体制机制、重塑流程架构。而筑牢教育系统安全屏障，强化“智慧教育示范区”网络安全保障体系和能力建设至关重要。

有网络安全能力距离“教育新基建”要求仍有差距

2021年7月，教育部等六部门印发了《关于推进教育新型基础设施建设构建高质量教育支撑体系的指导意见》(以下简称《意见》)，指明了“安全可靠”的教育新型基础设施体系建设方向，提出完善教育信息资产数据库，建立教育系统应急指挥网络，提升安全事件发现、应急报告、协同处置、追踪溯源等能力要求。

“应用和数据的重要性越来越高，但是反观网络安全的建设，其实是相对不匹配的。”侯元东表示，现有的网络安全保能力距离《意见》中提出的要求仍有较大差距。

在资产方面：教育城域网中信息化资产越来越多，资产价值不断提升，但安全防护却相对落后，安全运维人员严重不足，教育信息化资产逐渐成为黑客攻击的“香饽饽”；

在顶层设计方面：由于网络安全建设前期整体规划缺位，导致防护效果不佳，后期运维困难。并且面对数据平台、物联网等新技术应用也缺乏安全防护的可生长性；

在管理落地方面：温州市教育技术中心作为温州市教育城域网的运维管理者，需要承担起教育城域网及下属单位的安全监测及预警职能。因此，如何有效发挥教育局的安全监管职责，推动安全工作落地，也成为教育技术中心亟需深度思考的问题。

围绕“技术、人员、制度”三大机制构建安全运营中心

如何强化网络安全保障体系和能力建设，筑牢教育系统安全屏障?温州市教育局选择跳出传统安全建设模式圈，倡导在持续投入相对较低的情况下，获得长期有效的安全建设收益。

侯元东分享道：“我们从网络安全顶层规划切入，围绕‘技术工具、组织人员、制度流程’三大机制，构建了教育城域网安全运营中心。”

技术工具机制采取“总-分”逻辑，在顶层构建了安全运营平台，以“体系化、实战化、常态化”的方式打造和提升教育城域网的安全能力，既实现了网络安全的集中监测、又避免了重复建设。

组织人员机制是关注的重点，包括管理架构、市区协同、运营人员、意识提升等。从2005年开始，温州市教育局就组建了市教育系统骨干网络管理员队伍，定期开展网络安全培训，并在全市中小学推行持证上岗制度。

在制度流程机制上，配套制定了安全管理制度与不同场景工作流程，并依托安全运营平台将部分日常安全工作流程电子化，并且量化了安全工作结果，推动安全工作落地闭环。

基于以上三大机制，温州市教育局展开了网络安全综合治理行动，完成了对信息化应用系统和主机资产的摸底调查，“家底”摸清后，教育局又推动了全市网站等保合规建设与主机安全管理系统建设，初步构建了面向教育城域网信息化资产的安全防护基线。

携手深信服构建安全运营体系，保障安全工作落地持续有效

目前，在深信服等安全厂商的助力下，温州市教育局建设了安全运营平台，实现了在一个平台上对温州市教育城域网安全工作的统一监测与管理，后续安全能力的补充也将围绕平台进行生长。同时，厂商还提供了安全服务专家作为教育局运营能力的补充。

“安全运营中心与传统安全方式相比，最大的好处就是对于安全工作的过程管理，安全事件通报和处置更为顺畅且有效。”侯元东表示，以前传统的安全建设采用工作群或邮件向下通报的方式，很难实现安全的管理和闭环。构建了安全运营中心后，日常的安全工作流程都可以在运营平台上进行电子化操作，既打通了技术工具与组织人员的对接，又保障了每一个流程的管理有效性。同时，他们还探索了SOAR(安全编排与自动化响应)在教育城域网的应用，通过自动化处置的能力降低部分人力运维工作量。

在结果管理方面，为了更好地呈现安全工作效果，温州市教育局制定了安全工作决策。基于运营平台集中监测和流程电子化的数据，量化了各下属单位的安全指数，使得安全工作可视程度进一步提升，极大地提高了各单位安全工作意识，保障教育局安全监管职能有效行使。

来源：中国教育信息化网 2021-08-30
原标题：《打造教育网络安全新高地 护航国家“智慧教育示范区”创建》

南昌市以安全新基建为保障，提升网络安全防护能力

智慧教育示范区建设是在国家层面推进智慧教育发展的重大顶层设计，是以区域为单位整体推进智慧教育发展的重大构想，是为推动教育信息化融合创新发展，实现教育理念与模式、教学内容与方法的改革创新，提升区域教育水平，探索积累可推广的先进经验与优秀案例，形成支撑和引领教育现代化的新途径和新模式。2021年初，南昌市获得了创建国家智慧教育示范区的资格，这是南昌市实现智慧教育大发展的重大机遇和挑战。

近年来，南昌市在推动经济社会高质量发展过程中，统筹推进以云计算、5G、大数据、虚拟现实和人工智能等为代表的基础设施建设，加快实体经济数字化、网络化、智能化升级。在此背景下，南昌教育信息化取得长足发展，正从教育信息化1.0阶段迈向2.0阶段，为智慧教育示范区创建奠定了坚实基础。一方面，南昌市积极推进智慧教育环境升级，打造“互联网+教育”大平台，实现全市中小学教育专网100%覆盖，高质量班班通100%接入；另一方面，以应用为抓手，通过机考改革突破传统学业成绩评价模式，构建“线上学习答疑、线下专项辅导”免费立体教辅体系，专递课堂覆盖301所农村学校，学业大数据应用有效助力精准教学和个性化学习，受到了广大中小学师生一致好评。未来三年，结合国家“教育新基建”政策要求，南昌市创建国家智慧教育示范区建设将围绕“培育适应未来的智慧型、创新型人才”的总体目标，以数据驱动为主线，优化教学环境，创新教学模式，强化数据治理，努力打造智慧教学新生态和智能治理新样态，促进区域教育跨越式发展，主要抓好以下五个方面的工作。

一、以“网络新基建”为基础，提升智慧环境建设水平

一是打造南昌教育云数据中心。按照“集约高效、共享开放、安全可靠、按需服务”的原则，建设教育专网统一资源池，满足全市中小学对网络资源不断增长的需求，整合学校“低小散旧”的数据中心，实现全市基础设施环境共建共用、整体部署、数据共享和业务协同，保障教育资源的统一规划、按需调配、即需即用和有效共享。

二是推进教育专网“有线+无线”有机统一。高效利用5G高带宽、低延时、大并发的技术优势，实现光纤基础网络和5G移动网络的有机统一，丰富“5G+教育”应用场景，打造高速稳定、绿色安全、泛在化的智慧教学环境。

三是建设教育专网运维服务体系。制定服务标准和规范，构建教育专网运维机制，强化对计算、存储、网络等资源池的统一监控、分析和故障处理，有效保障教育专网万兆到县、千兆到校、百兆到班。

二、以“平台新基建”为支撑，推进洪教云生态建设

一是完善“洪教云”生态建设。推动国家、省、市、区（县）、校五级云平台互联互通，推进服务上云和应用落地，打造优质教育资源和服务的能力引擎，强化教学应用需求的快速响应和迭代，促进教育管理业务重组和流程优化，实现教育公共服务能力及共享开放水平明显提升。

二是打造“教育大脑”中枢系统。提升教育大数据汇聚和共享开放水平，形成教育数据与城市治理数据互联互通，构建数据中台，赋能“教与学”应用场景，有效提升教育管理和决策水平，实现基于数据驱动的智慧治理。

三是推进“洪校通”体系建设。推进以“区校一体”的智慧校园标准化建设，搭建以“教师画像”为核心的网络学习空间，推进智慧教学场景化建设，引领推动千人千面的教师空间发展格局。

三、以“资源新基建”为抓手，推进优质资源供给侧改革

一是构建资源开放共享体系。打造以校本课程、选修课程和阅读课程为特色的各类教学资源库，推进技术环境下的“英语教学”创新应用，普及深化“三个课堂”应用，有效弥合区域、城乡、校际间优质教育资源差距，推进优质教育资源全覆盖。

二是建设VR智慧教育基地。搭建全市中小学VR教学云平台，开发本地优质VR教学资源，推进VR教学应用中小学全覆盖，探索VR+教学场景新样态，打造VR教学应用示范校和职业教育VR实训基地，探究虚拟备课、虚拟授课、虚拟考试等教育教学新模式。

三是提升优质资源“课后服务”水平。落实国家“双减”政策，打造“双师”公益课堂，围绕德智体美劳五育内容，引入高质量专题教育资源，推进课后自主学习和在线互动答疑，提升课后服务水平，促进优质教育资源课后共享。

四、以“应用新基建”为突破口，推进技术与教学深度融合

一是推进智慧考场建设和学考机考改革。完成“题库建设标准、考务管理标准、考场（机房）建设标准、学业评价标准”四大标准建设，建成学业水平考试命题研究中心，完善艺术素养评价顶层设计，探索体育成绩过程性评价与体育素养的信息化评价手段。

二是推进“智慧作业”全市中小学全覆盖。落实国家“双减”政策和作业管理要求，构建以学习者为中心的学业评价体系，全域贯通课前、课中、课后学习场景，切实解决义务教育阶段学生学业负担重、课后辅导难等突出问题，实现基于数据驱动的智慧学习。

三是推进“教学通”应用全市覆盖和常态应用。聚焦课堂教学核心场景，增进课堂学习的交互与协作，实施精准备课和有效导学，实现教学全场景数据伴随式采集，助力教师差异化教学和分层辅导，实现基于数据驱动的智慧教学。

五、以“安全新基建”为保障，提升网络安全防护能力

一是强化网络安全技术防护。增强应急处置和灾难恢复能力，有效防范和抵御网络安全风险，构建可信、可控、可查的网络安全环境，保障网络系统硬件、软件稳定运行，营造安全可靠的教育网络环境。

二是强化专网全流量监测。践行“实战有效、常态保护”的理念，依托安全态势感知大脑，利用人工智能、大数据技术、全网威胁情报对海量日志进行分析研判，洞察攻击行为特征，及时发现未知威胁，通过联动安全设备的自动化响应机制对安全事件提前干预和防范。

三是保障业务数据安全。保护重要数据的存储与传输安全，防止和防范数据被篡改，加强对重要敏感数据信息的保护，部署安全防御系统，抵御病毒、恶意代码等对信息系统发起的恶意破坏和攻击，确保系统与数据的完整性、安全性。

来源：中国教育信息化 2021-11-25
南昌市现代教育技术中心副主任 万亚军
原标题：《以“教育新基建”助力智慧教育新生态》

长沙雨花区智慧教育建设积极推进5G/人工智能等新技术安全应用

长沙市雨花区以“智能技术与人文关怀相结合”的发展思路，区校一体推进雨花区智慧教育环境建设。一方面，以教育新基建为引领，积极推进以5G、人工智能、区块链、物联网为代表的新型技术在智慧教育建设中的应用，加速推进雨花教育数字转型和智能升级。另一方面，坚持以人为本，在区级统筹的框架下，从学校实际需求出发，在 “双减”背景下，以“减负提质”为核心，将智慧教育建设落实到为教师“赋能”、为教学“提质”、为学生“减负”。在“智能技术+人文关怀”思路的贯彻下，雨花教育在数字转型和智能升级中注入了人文关怀，使雨花教育既“有高度”又“有温度”。近三年来，逐渐形成了以“一空间、两中心、三应用”为主体的雨花智慧教育特色框架。

“一空间”：雨花智慧教育聚合空间

雨花智慧教育聚合空间是基于长沙市教育局智慧教育云平台打造的区域特色应用聚合空间，包括“资源汇聚”、“应用汇聚”、“空间汇聚”、“活动汇聚”与“成果汇聚”等五个方面，汇聚了教、学、研、管、评、测全方位的各级各类网站与应用平台，不仅汇聚了国家、省、市各级应用，同时重点融合并发展了以智慧“新三好”为代表的雨花区特色应用。空间在长沙市“统一用户、统一应用、统一认证、统一权限”的基础上，实现统一认证、统一登录，提高了教师工作效率，减轻了教师工作负担。

雨花智慧教育聚合空间

▼ “两中心”：智慧教育数据中心、智慧教育设计中心

智慧教育数据中心是集展示、宣传、数据分析、决策指挥于一体的“智慧教育大脑”。动态、可视化地呈现全区智慧教育教、学、研、管、评、测六个维度相关数据，为教育发展、学校布局、师资配备等提供科学依据，进一步提升教育治理智能化水平。

图2 雨花智慧教育数据中心数据大屏

智慧教育设计中心涵盖人工智能、智慧课堂、智慧体育、智慧阅读、智慧书法、VR情景教学等最新教学设备和应用，为学校提供一站式体验、现场培训、需求分析、方案设计等家装式定制服务。

雨花智慧教育设计中心

▼ “三应用”：三个雨花特色应用

“健好身、读好书、写好字”是雨花区多年来结合区域生命化德育、生命化课堂、生命化学校文化，探索出的一条具有雨花学子“新三好”特色的基础教育培养模式。在教育信息

化2.0时代，雨花区结合长沙市智慧教育示范区创建工作，以长沙市人人通空间为载体，将雨花“新三好”从线下发展到线上，从雨花“新三好”升级为智慧“新三好”，构建了可量化的监测机制和可操作的评价体系，形成了旗帜鲜明的雨花教育应用服务体系，建成了覆盖全区的“新三好”数据画像。

智慧体育管理应用自动采集教学数据，备课数据、课堂数据、运动数据、成绩数据，从更多维度的数据分析中找到更多有价值的信息，更便捷地指导教学、更科学地保证学生运动安全，并给教育管理决策者提供更加精准的数据支撑。

智慧阅读分析应用根据阅读主体的需求进行分层、分类、提炼、筛选阅读内容，进行个性化推送，让阅读内容智慧化。并对阅读的评价采取过程性评价及奖励评价，实现阅读评价智慧化。

智慧书法教学应用以汉字拟人书写为基础，结合智慧书法教室，解决了书法教学环境问题以及书法教师缺乏等问题，通过线上线下混合式教学和远程同步课堂教学，不仅大大提高学校的书法教学效率，也提升学生学习书法的兴趣。省市各级领导先后来我区实地调研，充分肯定雨花区智慧教育所取得的的成绩。

在“一空间、两中心、三应用”的整体框架下，长塘里小学、长塘里阳光小学、长郡雨花外国语学校、砂子塘吉联小学等一批未来学校和智慧校园脱颖而出，逐步构建了智能技术与人文关怀结合、强校引领与全面推进结合、市级规划与雨花特色兼顾、区域统筹与学校发展兼顾的雨花智慧教育生态。

雨花“新三好”

来源：长沙市雨花区教育局
原标题：《智能技术与人文关怀结合，区校一体推进智慧环境建设》

重庆两江新区安全数据应用助力智慧教育管理

新基建是教育转段升级的必然要求。2019年10月10日，两江新区发布《两江新区开展智慧教育“双进”工作的实施意见》，勾画了智慧教育与智慧城市双向奔赴的十大任务，彰显了教育新基建的社会紧密关联属性。2021年7月7日，《重庆两江新区智慧教育发展规划（2021-2023年）》正式发布，明确了两江新区智慧教育十大工程二十一项目标，为两江新区教育新基建全面推进指明了方向。

教育新基建层级深、纬度广，无论是狭义还是广义，均包含软硬件平台、融合资源、创新应用、生态治理、可信安全等。近年来，两江新区教育系统在智慧教育环境打造，智慧教育要素均衡布局，信息技术与教育教学深度有效融合、教育智能治理、教育资源交流协作与共享，信息素养提升等教育新基建层面开展优质化建设探索与实践更新。

一、智慧教育设施普及化

新区学校均实现交互式超短焦班班通、互联网万M到校、校园无线覆盖、数字广播、红外可视监控、人工智能机器人和编程课全覆盖。包括先期启动7所智慧校园示范校建设，智慧门禁、智慧阅读、智慧体育、智慧书法、智慧美术、智慧音乐、智慧英语、智慧语音、智能阅卷、全息投影、智慧智笔、VR/AR、会议转写、智慧照明等全面进入新区校园；建设10个机器人创客教室，在社团推广应用和信息特色素养提升上全面探索；所有公办中小学和幼儿园全面配置大中小型人形机器人、积木式机器人和配套课程，实现人工智能机器人配置和课程开设校校全覆盖；重点打造星光学校智慧校园标杆性建设项目，以高标准、科技化、场景化、体验式、集中性和实用性为宗旨，遵循共享原则；完成5G教育专网建设，实现不同个体资源高效共享和不同班级教学优质交互。

二、智慧教育管理智能化

全新打造两江新区智慧教育云平台，实现全区教育系统数据伴随式收集、态势感知、能力评测和服务集成。完成区域数据中心建设，通过驾驶舱教学、教研、评价、安全等八个维度的看板，对区域教育动向具备实时掌控能力，有利于及时作出科学决策和管控措施。整合学校现有各类应用数据，形成学校和个人评价参考。

三、智慧教育资源共享化

充分发挥新区教研人员、骨干教师和全体教师力量全面建成13万条区域数字资源；实施10个100工程建设1000节优质课程资源，实现人人贡献资源；以两江智慧教育云平台为纽带，链接国家中小学智慧教育平台、渝教云、智学网等上亿条优质资源。以学校特色建设实际为基准，建设书法、烹饪、中药等个性化资源。

四、智慧教育模式创新化

各学校结合学段、所处区域、师资优势等自身特点，不等不靠，主动探索、积极实践，先后形成星辰中学“依托智慧教育的精准教学”、行远小学“多课型混搭”、星光学校“无边界学习”、礼嘉实验小学“编程学院”、云慧小学“云上书法”等智慧教育品牌，以及多所学校共同探究构建的智慧评价、智慧劳育体系，实现区域共性化和校际个性化共存的新区智慧教育创新模式特色品牌。

五、智慧教育教研AI化

2022年4月，新区全面启动了智慧教育AI教研，依托远程音视频互动、同步录制直播、全场景数据采集、AI语音转写等技术，打造线上与线下相结合的混合式教研，助力教师线上自主学习考核等，打造跨区域、多学科教师智能研修平台。

六、智慧教育交流多元化

2021年，重庆市教委和两江新区管委会联合承办的智慧教育大会（重庆）成功举行，来自全国各地的智慧教育专家、全国智慧教育示范区代表、中小学校长等参与了大会，共同见证了这一落地两江新区的全国性智慧教育交流平台的诞生。各学校先后承办或搭建“教育装备展”、“5G技术下的学校教育生态”等全国性、区域性交流平台，迎接上百次其他省市团队莅临新区参观学习。新区组织65名骨干团队赴北京、上海等地学习考察，借助北师大等院校资源，呈现新区智慧教育的多元性、开放性、时代性。

七、智慧教育素养增强化

从四个层级全面谋划增强全区师生智慧教育信息素养能力。一是强化一把手信息素养，组织全区校长开展智慧教育理论认知和实践规划演讲比赛，邀请全国智慧教育专家到新区开展智慧教育领导力培训；二是增强骨干力量信息素养，组织100名骨干教师进行技术能力和编程知识体系化培训；三是提升全体教师信息素养，组织全员6000余名教师开展信息能力提升培训；四是培养学生信息素养，通过课堂、社团等形式全面普及信息技术教学，组织参加机器人创新挑战赛、科技创新大赛、编程大赛等，全面构建智慧教育信息素养能力提升和技术服务支撑体系。

在各级领导和专家的关注和支持下，两江新区教育人勠力同心，一步一个脚印踏实前行。两江新区成功申报国家八部委组织的国家智能社会治理教育实验基地和国家两部委组织的5G+智慧教育应用试点项目，约三分之一的学校获评重庆市智慧校园创建示范学校。

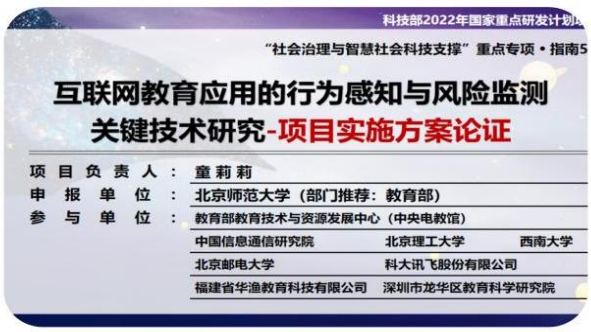
当下，各行业各领域正全面推进数字化转型探索。两江新区教育在数字化转型之路上，既不受“硬件设备堆砌”观点影响而弱化智慧教育环境打造，也不受“巧妇难为无米之炊”观点左右而放弃教育教学新模式探索。两江新区将保持“让每一个孩子成为更好的自己”初心，下一步将在多网合一校园网络升级改造，数据能力平台、教育治理、精准教学与优质资源、教育教学模式和教科研体系、信息人才培养建设等方面继续发力，坚守“应用为王”导向，从实际出发，全面优质推进教育新基建。

来源：重庆两江新区教育局　原标题：《重庆两江新区全面优质推进教育新基建》

2022国家重点研发计划“互联网教育应用的行为感知与风险监测关键技术研究”项目启动

2022年12月24日，北京师范大学牵头承担的2022年度国家重点研发计划项目“互联网教育应用的行为感知与风险监测关键技术研究”（项目号：2022YFC3303500）实施方案论证暨启动会以线下线上相结合的形式召开。本项目由北京师范大学教育学部、互联网教育智能技术及应用国家工程研究中心童莉莉副教授主持，联合了教育部教育技术与资源发展中心(中央电化教育馆)、中国信息通信研究院、北京理工大学、西南大学、北京邮电大学、福建省华渔教育科技有限公司、科大讯飞股份有限公司、深圳市龙华区教育科学研究院共9家单位承担，项目国拨经费为938万元。会议由北京师范大学科研院林小鹃副处长主持。





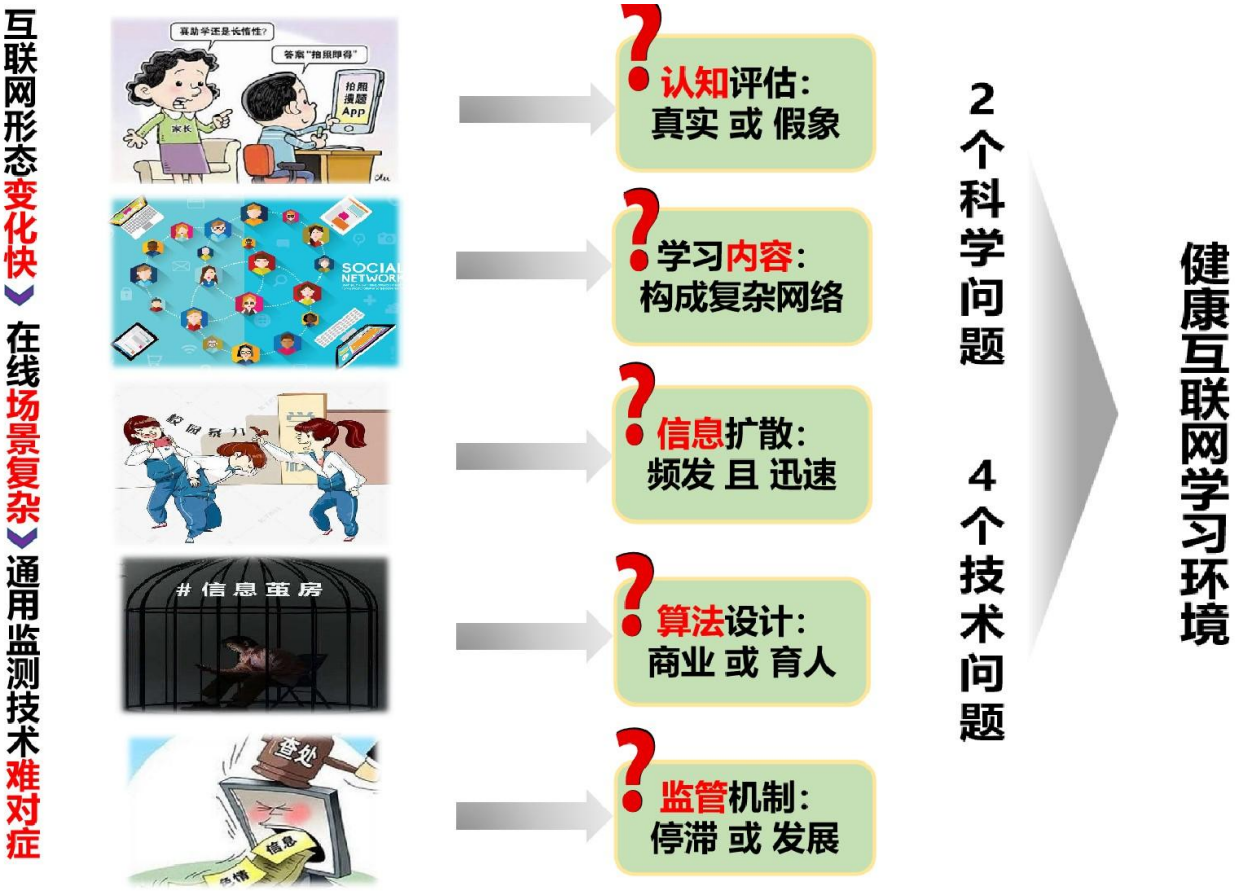
北京师范大学副校长康震代表学校对科技部、教育部、工信部、专家组等各方在项目申报和启动阶段的关心指导表示真诚感谢，学校已安排科研院专人跟进、资产处与项目组协同完成监管平台招标、财务处做好经费专项管理等具体工作，希望项目组所有成员单位能齐心攻关，顺利启动并完成关键技术攻关目标。

科技部社会发展科技司调研员陈振介绍了“社会治理与智慧社会科技支撑”国家重点专项的设计思路，强调本项目需聚焦互联网教育应用的治理症结，与前序立项的学生发展追踪项目和同年立项的教师资源类项目形成专项内的数据共享、机制协同、应用联动，促进智慧教育在“安全”与“发展”的原则下科学发展。

教育部科学技术与信息化司副司长舒华代表推荐部委祝贺项目立项，希望研究团队要深刻认识到互联网环境中的学习行为精准感知和风险监测技术对推进教育数字化的重要意义，聚焦真问题多出好成果。在“内容审查-信息保护-算法智能-认知适用-风险可控”的系统性思路指导下，以教育部已经出台的内容审查有关规范、教育APP管理制度为基础，促进算法设计契合育人规律、实现互联网学习环境对真实健全人格的培养作用。

首都师范大学教授方海光、国家信息中心信息化和产业发展部主任单志广、工业和信息化部产业政策与法规司政策研究处处长李琰、北京国嘉瑞联合会计师事务所所长徐胜怀、北京理工大学教授嵩天、北京师范大学智慧学习研究院副院长曾海军等项目责任专家和特邀专家全程参会并指导项目与课题实施方案的论证环节。

项目负责人北京师范大学教育学部副教授童莉莉就当前互联网教育应用网络场景杂、监管覆盖面缺、评价精度低的问题，介绍了4类公共数据集建立、5项核心技术性能提升、1个综合监管平台对接支撑国家智慧教育公共服务平台的项目实施方案。教育部教育技术与资源发展中心(中央电化教育馆)副主任杨非、中国信息通信研究院技术与标准研究所产业互联网研究部副主任臧磊、北京理工大学赵馨宁老师、西南大学教授刘革平分别就各子课题的实施方案进行了详细汇报。参研单位科大讯飞副总裁王士进、深圳龙华教育科学研究院院长袁再旺、北京邮电大学郭三川老师、华渔教育科技有限公司CTO陈宏等在会研讨。



北京师范大学原副校长陈光巨教授代表项目组在会议总结环节中表示，本项目将围绕《关于加强科技创新支撑平安中国建设的意见》确立的“平安中国”战略总目标，围绕论证会的系统性开展建议，聚焦智慧教育理论体系、研究互联网教育应用的风险监测关键技术体系、开展智慧教育示范区/教育特色型国家智能社会治理实验基地等典型区域的示范应用，构建事前-事中-事后闭环的互联网教育应用监管平台，突破多模态内容审查技术、个人信息保护溯源技术、用户行为建模/画像与算法感知技术、认知发展评估与人机协同诊断技术和复杂行为序列风险监测等5项关键技术，推进互联网教育应用业态的健康有序发展，促进在线教育关联主体的获得感和安全感，助力互联网教育治理能力的现代化。

→ 来源：北京师范大学

中央网信办印发《关于切实加强网络暴力治理的通知》

2022年11月2日，中央网信办印发《关于切实加强网络暴力治理的通知》，旨在加大网暴治理力度，进一步压实网站平台主体责任，健全完善长效工作机制，有效保障广大网民合法权益，维护文明健康的网络环境。主要内容节选如下：

一、建立健全网暴预警预防机制

1. 加强内容识别预警。网站平台要建立网暴信息分类标准和典型案例样本库，在区分舆论监督和善意批评的基础上，明确细化涉网暴内容标准，增强识别预警准确性。结合网站平台业务特点和具体处置案例，不断更新分类标准，持续完善样本库。

2. 构建网暴技术识别模型。网站平台要综合考虑事件类别、针对主体、参与人数、信息内容、发布频次、环节场景、举报投诉等维度，建立符合自身特点的网暴行为识别模型，及时发现预警网暴倾向性、苗头性问题。

3. 建立涉网暴舆情应急响应机制。网站平台要组织专门工作力量，及时收集网暴相关热点话题和舆情线索，强化网暴舆情事前预警，做到防微杜渐、防患未然。根据陌生人私信显著增加、相关话题热度迅速攀升、搜索量快速增长、举报频次加大等情况，及时发现网暴异常行为。

二、强化网暴当事人保护

1. 设置一键防护功能。网站平台要根据自身特点，建立完善紧急防护功能，提供一键关闭陌生人私信、评论、转发和@消息等设置。用户遭遇网暴风险时，网站平台要及时发送系统信息，提示其启动一键防护，免受网暴信息骚扰侵害。

2. 优化私信规则。进一步完善私信规则，对接收陌生人私信附加数量、时间、范围等限制，用户可根据自身需要自主设置仅接收好友私信或拒绝接收所有私信。对照网暴信息分类标准，采取技术措施，防范网暴内容通过私信传输。

3. 建立快速举报通道。在网站平台评论、私信等位置设置网暴信息快捷投诉举报入口，简化投诉举报程序，网站平台对于明确为网暴信息的应在第一时间予以处置。向用户提供针对网暴信息的一键取证等功能，方便当事人快速收集证据。坚持最有利于未成年人的原则，优先处理涉未成年人网暴举报。

三、严防网暴信息传播扩散

1.加强评论环节管理。网站平台要加强对涉网暴风险的新闻、帖文、话题等信息的评论环节管理，及时清理过滤涉网暴违法违规评论，严控涉网暴不友善评论泛化传播，优先展示权威信息。重点网站平台要将用户公共空间发布的评论在本人账号主页进行公开集纳展示，强化公众监督。

2.加强重点话题群组和版块管理。及时解散网暴信息集中的话题版块，暂停新设相关话题版块。密切巡查以相关事件名称、当事人及相关人员姓名命名的词条、话题、群组、贴吧，及时清理涉网暴内容。排查关闭以匿名投稿、隔空喊话等名义发布导向不良等内容的话题版块和群组账号。

3.加强直播、短视频管理。加强直播和短视频内容审核，及时关停网暴内容集中的直播间，封禁违规主播，对存在网暴风险的短视频先审后发，清理含有网暴信息的短视频，拦截过滤负面弹幕。密切关注网暴当事人开设的直播间，及时管控诱导逼迫自残自杀等信息。

4.加强权威信息披露。各地网信部门要密切关注涉网暴舆情和信息动向，督促协调有关部门和地方加强权威信息发布。对于存在网暴风险的热点事件，网站平台要及时转发推送权威信息，引导网民理性发声，共同抵制网暴行为。

四、依法从严处置处罚

1.分类处置网暴相关账号。一是加强账号发文前警示提醒，对发布不友善信息的账号，提示理性发言。二是对参与网暴的账号进行警示教育，并视情采取禁言、暂停私信功能等措施。三是对首发、多发、煽动发布网暴信息的账号，依法依规采取关闭账号等措施，情节特别严重的，全网禁止注册新账号。四是涉及违法犯罪的，移交相关部门依法追究法律责任。网站平台要强化曝光力度，及时对外公布热点网暴事件处置情况。

2.严处借网暴恶意营销炒作等行为。坚决打击借网暴事件蹭炒热度、推广引流、故意带偏节奏或者跨平台搬运拼接虚假信息等恶意营销炒作的行为，进一步排查背后MCN机构，对MCN机构采取警示沟通、暂停商业收益、限制提供服务、入驻清退等连带处置措施。对于将账号名称临时修改为事件相关机构、人员的，网站平台应当加强用户真实身份核验。

3.问责处罚失职失责的网站平台。对于网暴信息扎堆、防范机制不健全、举报受理处置不及时以及造成恶劣后果的网站平台，依法依规采取通报批评、限期整改、罚款、暂停信息更新、关闭网站等处置处罚措施，从严处理相关责任人。

→ 来源：中国网信网 2022年11月04日

2022年国家网络安全宣传周在安徽合肥举行

2022年9月5日上午，由中宣部、中央网信办、教育部、工信部、公安部、人民银行、广电总局、全国总工会、共青团中央、全国妇联等十部门共同举办的2022年国家网络安全宣传周在安徽合肥开幕，并对首批国家网络安全教育技术产业融合发展试验区进行授牌。中央宣传部副部长、中央网信办主任、国家网信办主任庄荣文出席开幕式并讲话。

庄荣文指出，党的十八大以来，在习近平总书记关于网络强国的重要思想指引下，我们大力加强网络安全保障体系和能力建设，我国网络安全战略、政策、法规体系不断健全，关键信息基础设施保护、数据安全管理、个人信息保护、新技术新应用风险防范等能力持续加强，网络安全教育、技术、产业等基础更加坚实。

庄荣文强调，要深入学习宣传贯彻习近平总书记关于网络强国的重要思想，大力营造网络安全人人参与、人人有责、人人共享的浓厚氛围，全面提升网络安全保障能力和水平，为党的二十大胜利召开提供有力服务、支撑和保障。要践行为民理念，认真解决涉及人民群众切身利益的网络安全问题，提升全民网络安全意识和技能，凝聚起共筑网络安全防线的强大合力。要聚焦重点领域，全力筑牢国家网络安全防护屏障，着力构建全国一体化的关键信息基础设施安全保障体系，确保网络空间平稳有序运行。要强化风险防范，大力加强网络安全监督管理，全面落实网络安全工作责任制，坚决防范出现重大网络安全事件。要坚持依法治网，不断优化网络安全发展环境，进一步健全完善网络安全法律体系，加强网络安全执法，引导全社会依法规范网络行为。要推动融合发展，积极培育网络安全良性生态，加强基础设施和资源整合利用，形成以企业为主体、市场为导向、产学研用深度融合的网络安全技术创新体系，开创网络安全工作新局面。

本届网络安全宣传周以“网络安全为人民，网络安全靠人民”为主题，聚焦网络安全教育技术产业融合发展，通过重要活动与主题活动相结合，线上活动与线下活动相结合，着力提升全民安全意识、防护技能，提升网络安全水平，促进产业发展。

2022年国家网络安全宣传周共安排展览、论坛和主题活动三大方面内容，设置了网络安全博览会、网络安全技术高峰论坛、八场分论坛、六个主题日，以及网络安全进社区、进农村、进企业、进机关、进校园、进军营、进公园“七进”活动等。

首批国家网络安全教育技术产业融合发展试验区授牌仪式现场

开幕式上，首批国家网络安全教育技术产业融合发展试验区授牌。首批国家网络安全教育技术产业融合发展试验区分别为：安徽省合肥高新技术产业开发区、北京市海淀区、陕西省西安市雁塔区、湖南省长沙高新技术产业开发区、山东省济南高新技术产业开发区。

该试验区由中共中央网信办、中国教育部、中国科技部、中国工业和信息化部共同组织实施。通过推动试验区建设，旨在探索网络安全教育技术产业融合发展的新机制新模式，形成一系列鼓励和支持融合发展的制度和政策，培育一批支撑融合发展的创新载体，进而总结形成可借鉴可复制可推广的经验做法，推动在全国范围内形成网络安全人才培养、技术创新产业发展的良性生态。

→ 来源：人民网－安徽频道，中国新闻网 2022-09-05

国际智慧学习环境协会(IASLE)

▼ 关于国际智慧学习环境协会

国际智慧学习环境协会（International Association of Smart Learning Environments；IASLE）是一个面向智慧学习环境研究的专业学术社群，成员包含研究人员、学者、从业者和行业专业人士，探讨前沿智慧学习环境的创新教学法、新兴技术应用、和教学与技术融合，进而改革未来的教学和学习方式。

- Pedagogy (教学): learning paradigms, assessment paradigms, social factors, policy
- Technology (技术): emerging technologies, innovative uses of mature technologies, adoption, usability, standards, and emerging/new technological paradigms (open educational resources, cloud computing, etc.)
- Fusion of pedagogy and technology (教学与技术的融合): transformation of curriculum, transformation of teaching behavior, transformation of administration, best practices of infusion, piloting of new ideas.

■ 执行团队（Executive Team）

- President: Dr. Dejian Liu (2022/1-2023/12)
- Vice-Presidents: Dr. Nian-Shing Chen and Dr. Maiga Chang
- Secretary / Treasurer: Dr. Elvira Popescu
- Directors: Dr. Kinshuk, Dr. Ronghuai Huang, Dr Junfeng Yang, Dr. Ahmed Tlili and Dr. Richard Tortorella

▼ 协会官方期刊：《智慧学习环境》

《智慧学习环境》（*Smart Learning Environment*；*SLE*）期刊于2014年成立，是国际智慧学习环境协会(International Association of Smart Learning Environments；IASLE)的官方期刊。SLE期刊旨在探讨推进当前的学习环境向智能学习环境发展来改革教学和学习方法的相关问题。其创刊以来，已发布9卷（Volumes）共202篇高质量学术论文。值得一提的是，SLE是一个完全开放获取的期刊，对作者和读者都是免费的，不收取任何订阅费和注册费。在2021年SJR排名中教育维度下的1381个期刊中，SLE排名第216名(216/1381)，成功进入Q1区。

SJR（SCImago Journal Rank）是国际期刊评价分析、期刊排名的门户网站，涵盖了几乎所有国家发行的学术期刊。SJR指标是由西班牙学术团队SCImago所开发，于2007年起根据Scopus数据库（Elsevier BV）的指标对期刊数据进行分析，通过可视化技术进行信息分析、呈现和检索，并对不同的期刊进行分类和综合排名。被评估的期刊按主题领域（27个主题领域），主题类别（309个子主题类别）或国家进行分组。SJR指标不仅考虑引文的绝对数量，也考虑引文的质量，如在总被引频次相等的情况下，期刊越多地被高声望期刊(如Nature或Science)所引用，此期刊的声望越高。

根据斯普林格·自然出版社（Springer Nature）的2021卓越编辑（Editorial Excellence）榜单，SLE排在第八名（前10%）。此排名是根据斯普林格·自然出版社开展的“期刊作者满意度”调查结果得出。该调查是由斯普林格·自然出版社逐年开展的调查问卷，邀请期刊作者在期刊论文发表一周内对其出版体验提供反馈，以筛选出2021年表现出卓越编辑水平的期刊。排名先后是通过期刊作者对以下两句陈述的打分（满分5分）取平均值来确定的：“在整个过程中，期刊编辑提供的建议和评论有助于我提升我的论文”；“期刊的编辑们对同行评审过程进行了很好的管理”。期刊获得的分数越高，其在卓越编辑榜单的排名越靠前。

其他进入榜单前10%行列的教育领域著名期刊包括《青年与青少年杂志》（Journal of Youth and Adolescence）和《学校心理健康》期刊（School Mental Health）。

《智慧学习环境》期刊主页网址：https://slejournal.springeropen.com/about

▼ 智慧学习环境国际会议（ICSLE）

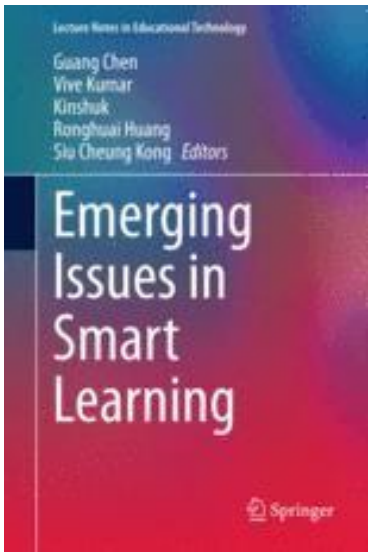
2022年8月18日至20日，以“智能技术增强智慧学习”为主题的2022智慧学习环境国际会议（ICSLE 2022）在杭州师范大学成功举办。本次会议采用线上线下融合模式，在全球三地同时举行，由国际智慧学习环境协会主办，杭州师范大学（中国）、拉里奥哈国际大学（西班牙）和近东大学（塞浦路斯）联合承办，互联网教育智能技术及应用国家工程研究中心为支持单位，国际智慧学习环境协会主席刘德建、北德克萨斯大学Kinshuk教授、北京师范大学黄荣怀教授担任大会主席。

杭州师范大学线下会场

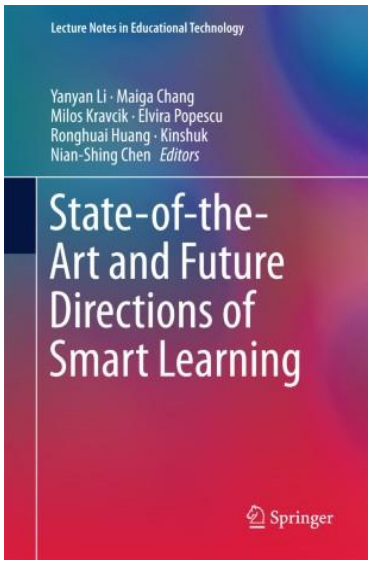
2014-2022年6届智慧学习环境国际会议（ICSLE）列表

2014: The 1st International Conference on Smart Learning Environments (香港)
2015: The 2nd International Conference on Smart Learning Environments (罗马尼亚)
2016: The 3rd International Conference on Smart Learning Environments (突尼斯)
2018: The 4th International Conference on Smart Learning Environments (中国)
2019: The 5th International Conference on Smart Learning Environments (美国)
2022: The 6th International Conference on Smart Learning Environments (中国+西班牙+塞浦路斯)

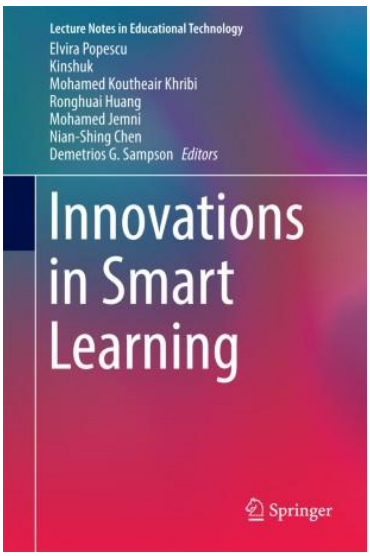
国际智慧学习环境协会年度论文集和官方期刊



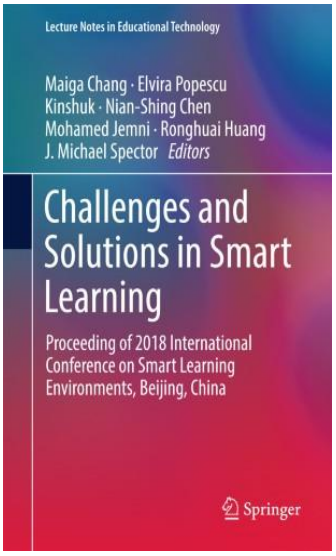
2014 ICSLE



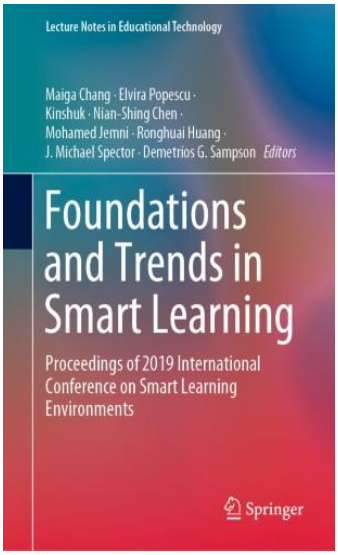
2015 ICSLE



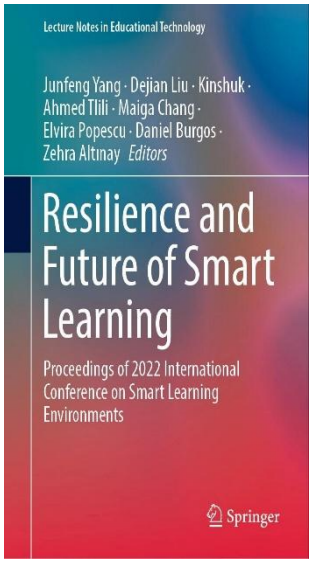
2016 ICSLE



2018 ICSLE



2019 ICSLE



2022 ICSLE

Smart Learning Environment 期刊

来源：https://slejournal.springeropen.com/about

http://iasle.net/icsle-2022/

北京师范大学智慧学习研究院、 杭州师范大学经亨颐教育学院（2020-08-19）

世界互联网大会成立大会

2022年7月12日，世界互联网大会成立大会在京举行。世界互联网大会国际组织总部设在中国北京，宗旨是搭建全球互联网共商共建共享平台，推动国际社会顺应数字化、网络化、智能化趋势，共迎安全挑战，共谋发展福祉，携手构建网络空间命运共同体。

世界互联网大会组织机构包括会员大会、理事会、秘书处、高级别咨询委员会和专业委员会等。会员来自国际组织、全球互联网领域领军企业、权威机构、行业组织及顶尖专家学者。世界互联网大会将为广大会员搭建深度交流合作平台，为会员在自身发展、能力提升和展览展示等方面提供服务和支持。世界互联网大会（乌镇峰会）将转型为国际组织年会，此外还将举办区域性、专题性论坛或研讨会。

顺应数字时代的发展，回应国际各方的期盼，世界互联网大会国际组织将承担新的历史使命。**一是在增进理念共识上**，着眼当前网络空间的新挑战、新问题，坚持开放包容，更好推动国际社会化解分歧、凝聚共识。**二是在数字经济发展上**，发挥好数字经济对经济社会发展的推进器作用，成为全球数字化转型和数字赋能的重要动力源泉。**三是在数字技术创新上，**加强国际社会协同创新，培育更多创新成果，推动人类科技进步。**四是在文化交流上，**推动网络媒体合作，加强网络文化建设，促进文明互鉴，提高公众数字素养，促进网络文化产业健康发展。**五是在规则制定上，**持续推进全球互联网治理进程，推进全球会员企业、研究机构、高校等在治理规则和技术标准等方面的探讨交流。六是在对话合作上，更好为各国政府、国际组织、跨国企业、技术社群搭建交流合作平台。

据了解，已有来自6大洲近20个国家的百家互联网领域的机构、组织、企业及个人加入，成为世界互联网大会初始会员。其中包括享誉全球的互联网领军企业、权威行业机构、互联网名人堂入选者等。

来源：央视网 2022-07-12

智慧教育资讯
Smart Education Newsletter

教育系统网络安全专题

主 办

教育部教育信息化战略研究基地（北京）

地址:北京市海淀区学院南路12号京师科技大厦A座12层 邮箱:bjjd@bnu.edu.cn
网站:http://cit.bnu.edu.cn 电话:010-58807213 邮编:100082