



大连理工大学
DALIAN UNIVERSITY OF TECHNOLOGY

畅通信息，服务师生

大工e刊



2020/4

2020年第一期（总25期）

主办单位：网络与信息化中心（信息化建设管理办公室）

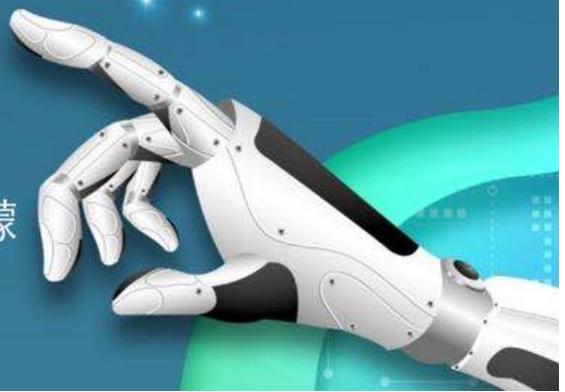
总策划：张巍

策划：翟鸣宇、于广辉、张鹏、刘凤伟

本期责编：王苏

本期编委：郭晓明、刘化总、李降宇、刘柱、杨雨濛

美编：宫萍



人工e刊

目 录

e 校园

系统观

招牌秀

锐关注

新视界

酷科技

强安全



e校园 2020 e Campus

工作进展

1 月

- WebVPN 服务正式上线
- 完成 2019 年度信息化建设评优工作及 2020 年信息化项目任务书签订工作
- 软件开发——办事大厅流程【废旧家具和大型设备外包装等集中清理服务申请】按教育部要求完成全国教育信息化工作管理信息系统学校数据填报的相关工作
- 完成教育部 2019 年网络安全年度考核工作，取得了 99 分的好成绩
- 完成超算中心 2019 运行年报

2 月

- 校园一卡通系统换代升级，线上办理各项业务更加方便快捷
- 编制教师主页升级项目的建设方案，开展面向科研团队的主页 UI 设计工作
- 软件开发——办事大厅流程【学校土地证书使用申请】、【学生交流项目申请服务】、【国际化基金资助学生海外交流项目审批】、【学生因公出国（境）申请】、【防疫物资申请】
- i 大工上线“健康打卡”及“上报统计”功能，实现健康动态的及时报告
- 启动师生返校管理系统建设工作
- 为教育部、辽宁省及大连市等相关部门召开的视频会议提供技术保障
- 为留校学生集中住宿点老专家楼加设 DLUT 无线，优化楼宇网络，提升网络速度
- 参加 CERNET 疫情防控视频会议，落实 CERNET/CERNET2 大连节点保障工作，严格运维规范、确保主干网畅通
- 全力保证学校 WebVPN 和 VPN 等系统平稳运行
- 启动疫情防控期间的学校网络安全保障工作
- 部署校内 CARSI 联盟认证服务，为师生的学习、科研提供学术资源访问保障
- 超算系统运行维护

3 月

- 南门、西便门、新北门等校门增设 DLUT 无线
- 软件开发——办事大厅流程【教工亲属关系及独生子女证明】
- 为网上办事大厅平台以及相关业务的网上预约等功能提供技术支持，确保疫情防控期间机关线上业务工作正常运转
- 继续开发师生返校管理系统并在开学报到流程演练中试用
- 完成 Adobe 项目采购工作
- 完成我校教育移动应用的整改和备案工作，并形成相关材料上报教

近期规划

2020 年
4-6 月

- 育部及辽宁省教育厅
- 编写信息化项目管理系统、智能助手等公共服务平台的建设方案
 - 开展“大连健康码”、“大连电子通行证”、“大连健康码专属码”的使用及推广工作，定期上报大连市疫情防控指挥部
 - 初步完成学校 2019 年度网络安全工作年报的编制工作
 - 完成超算二期建设方案编写工作
- 电子支付平台、决策支持平台换代升级
 - 校门进出管控系统、校内点餐系统上线
 - 启动大连理工大学智能助手、i 大工（三期）、信息化基础平台（三期）、信息化项目管理系统、学院一张表平台建设等项目的招标工作
 - 正版 Adobe 校园版软件包（Creative Cloud for teams All Apps）上线试运行
 - 启动“大工岁月”主题数据画报推送活动
 - 开展教师主页升级实验室网站的设计
 - 优化公共数据平台数据质量检测配置
 - 预先准备涉密及非涉密计算机的保密检查工作
 - 校史馆后楼、新幼儿园及人才公寓光缆施工
 - 完成修订《大连理工大学电子邮箱管理办法》
 - 完成 CERNET 大连地区核心路由器的割接工作
 - 发布学校 2019 年度网络安全工作年报
 - 启动数据中心资源清理及安全配置调整工作
 - 开展信息化项目网络安全管理相关工作
 - 超算二期方案讨论
 - 完善超算平台运行监控系统
 - 调研超算重点保障支撑政策

系统观 2020
System Overview
第 1 季度网信中心各部门系统运行情况

系统名称	总量 截止 2020 年 3 月 31 日	新增数量 1-3 月
校园电子邮箱	学生注册总量：107101 教工总量：8558	新增学生数量：141 新增教工数量：123
i 大工	激活用户总数：71490 各种应用访问总量：2504 万	新增访问量：260 万
调查问卷系统	共发布 274 份问卷	发布了 1 份问卷 参与答卷共计 3 人次
统一身份认证	总访问量：3790 万	新增访问量：382 万 日均访问量：42023 人次
校园门户	总访问量：1590 万	新增访问量：118 万 日均访问量：13008 人次
办事大厅	总访问量：50.7 万人次	发布 89 个填表服务、285 个链接服务
一卡通	在用卡数：66846 张	1-3 月消费次数 139 万次 补换卡：1160 张，开卡：103 张
网站群	网站数量：234 个 总访问量：11251 万人次	网站增量：0 个 新增访问量：738 万人次
会议网平台	浏览总数：131 万人次 会议总数：49 次	新增会议：1 个
VPN 服务	总登陆人次：103686 人次	新增登录：29430 人次
视频会议系统	召开会议：335 次	新增会议：25 次
超算中心	计算服务总量：12859 万核时 作业量：44.2 万份	新增计算服务：657 万核时 新增作业量：12286 份
玉兰卡微信平台	绑定人数：43483 人	1-3 月大工微信交易：42949 笔
云盘服务	用户数：22951 群组数：632	新增用户：784 新增群组：29
正版软件平台	登录总人数：9252 人 激活成功数：16437 次	新增登录人数：1068 人 新增激活成功：908 次
教师个人主页	开通总人数：2951 总访问量：6759 万人次	新增访问量：336 万人次
高清视频平台	总访问量：54 万人次	新增访问量：7 万人次
机构知识库	总访问量：4366 万人次 总日均访问量：75280 人次	新增访问量：582 万人次
正版软件平台	登录总人数：9252 人 激活成功数：16437 次	新增登录人数：1068 人 新增激活成功：908 次

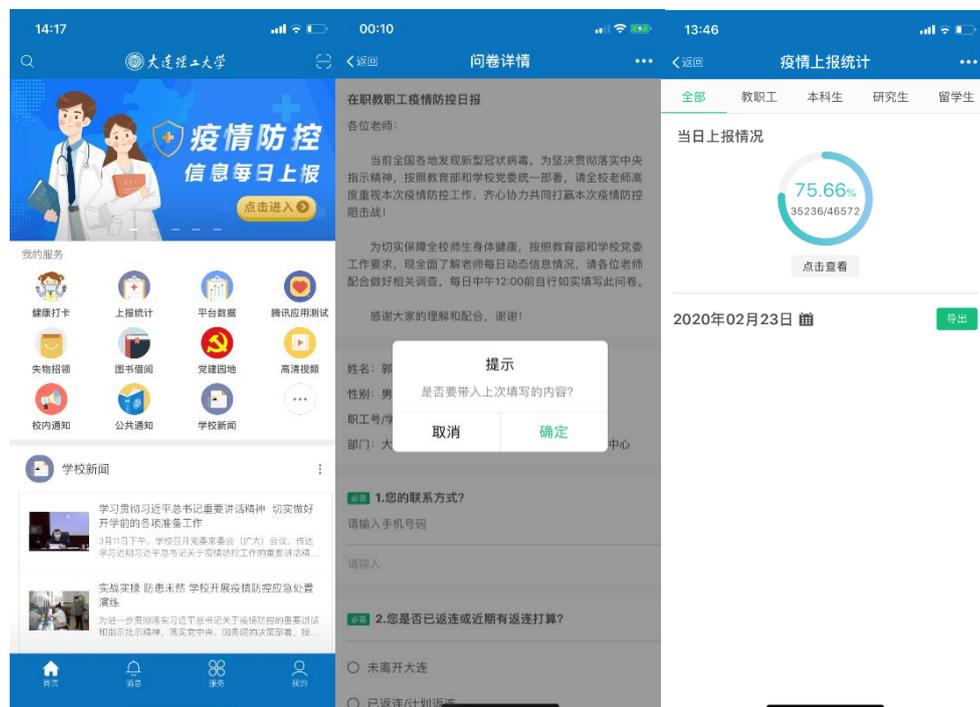
招牌秀 2020 Specialty Show

依托平台化建设成果，推出“i 大工”防疫相关功能

学校 2016 年规划建设全新移动校园平台“i 大工”，2017 年，完成“i 大工”全面升级，以多终端入口兼容（APP、微信企业号、QQ 校园号）的方式，打造了集师生教学、办公和服务等多场景多维度支撑的移动校园平台，向广大师生和学校的管理者提供掌上校务服务和移动办公服务。

2020 年疫情初期，在综合分析疫情防控相关需求基础上，考虑到学校“i 大工”作为学校官方移动校园平台，已稳定运行多年，一直持续为师生提供各类服务，受众面大，师生认可度高；同时“i 大工”已将学校基础数据与移动端访问进行了集成对接，能够快速接入并搭建起可用的服务，学校最终决定在原有“i 大工”基础上新增“健康打卡”等疫情防控的相关功能。

健康打卡+上报统计，助力疫情防控



1、每日平均打卡 2.9 万人次

“i 大工”平台疫情防控功能于 2020 年 2 月 22 日上线，为全部在职教职工、在读研究生、在读本科生、在校留学生提供健康打卡服务。党委教师工作部、党委研究生工作部、党委学生工作部、机关党委、后勤党委、国际教育学院（留学生办公室）负责各自

的人员管理，网信中心负责技术支撑和协调沟通。

学校主要通过两种方式宣传推广。一是通过线上通知和推送，在学校校园门户、官微发布和推送通知；二是通过各管理部门自上向下的逐步传达。截至目前，“i大工”健康打卡功能平均每日打卡人数超过 2.9 万人次。

2、健康打卡+上报统计，高效防控疫情

疫情防控采用的解决方案主要体现在“健康打卡”和“上报统计”两个功能上，两者以“i大工”为运行支撑，依托学校公共数据平台提供的各类基础数据，按照教育部、辽宁省等上级部门的要求，结合校园实际情况来设计填报内容。“健康打卡”面向师生进行每日打卡，依靠手机位置定位等手段科学化采集数据，确保了数据填报的准确性及可操作性。“上报统计”提供给二级管理人员健康打卡情况及统计结果。两者有效满足学校对疫情防控的基本需求。

技术创新+有力保障，实现“线上防疫”

通过信息化手段助力疫情防控，对于高校所有信息化从业者来说都是全新的，都是在逐步实践过程中发现问题并解决问题。学校“健康打卡”等“线上防疫”功能的成功推广和应用，主要有以下三方面的原因：

1、多部门紧密合作共同推进建设

业务导向是信息化建设的关键。业务部门负责明确业务需求、建设目标，信息化技术人员做好支持、配合和实现。业务部门加强业务管理，确保采集准确、打卡及时，真正将系统用起来、用好，确保“健康打卡”数据准确、及时、完整。业务部门和信息技术部门协同发挥合力，共同做好信息化工作。

2、发挥业务二级管理和基层管理的重要作用

健康打卡的推广和持续使用，各二级单位、学部学院是关键：对于教师，各单位管理人员是关键；对于学生，辅导员、级队、班级是关键。二级管理的快速便捷，使工作能有效落地、落实。

3、通过管理保证信息传递的有效性

疫情防控涉及到学校师生中每一个人，每人每天都需要打卡，虽然学校的消息平台会提前给相关人员推送提醒，但效果并不明显。一方面师生接收到的消息太多，不能保证关注到提醒消息，另一方面是往往存在偶尔忘记的情况。要保证打卡功能的全面执行，需要通过人为的监督，让基层管理人员通过“上报统计”及时了解上报情况，确保精准

地进行信息传递。

高校疫情防控信息化建设，考验信息化基础建设水平

疫情防控的信息化建设是检验学校信息化基础建设的一个很好契机。学校已建成移动校园平台“i 大工”、信息化基础平台两大支撑平台，并一直持续开展全校范围的数据治理工作，通过学校成熟的信息化队伍建设管理机制，学校整体信息化建设在逐步有效提升。此次“线上防疫”相关功能，完全依托于学校两大支撑平台和已有的数据治理成果基础上建设而成：“健康打卡”功能采用封闭方式填写，师生需使用学校统一身份认证登录学校“i 大工”平台完成；所有人员数据来源于学校公共数据平台，通过数据交换方式完成同步，并通过身份信息进行打卡问卷的精准发布；二级管理人员通过学校岗位角色平台统一维护调整，实现分层分级管理；功能运行基础设施依托于现有“i 大工”运行服务器进行微调和优化。

学校信息化基础建设成果助力防疫期间的学校相关防控工作的开展，也使学校积累了特殊时期信息化建设的经验，同时为今后智慧校园的建设与发展奠定了坚实的基础。

（来源：郭晓明网络与信息化中心）

沈富可：从疫情防控反观高校 IT 的未来

（沈富可：中国高等教育学会教育信息化分会副理事长兼秘书长，华东师范大学信息化治理委员会秘书长兼信息化治理办公室主任）

近几年，经过相关方面的努力，高校信息化建设与应用都取得了很大成绩。在这次大范围的疫情防控过程中，我们看到，高校信息化发挥了很好的支撑作用。但同时，也应看到，这次疫情防控对高校信息化的各种平台、系统及工具，尤其是信息化队伍的支撑反应能力提出了挑战。

因此，有必要就疫情防控下高校信息化的问题进行分析，从而总结出应对这些挑战的措施，真正使信息化能做到与学校各种业务常态化的“深度融合”。

疫情防控下，高校信息化的挑战

疫情防控期间，总体来看，高校的 IT 挑战主要反映在如下几个方面：

第一，在线教学平台和系统的不稳定。疫情前，琳琅满目的各式教学平台、视频会议系统目不暇接，很难选择，其中有的是基于公有云而建，有的是学校自己搭建的，声称的效果都不错，很多学校也有各种经验分享。然而在“停课不停学”相关行动下，却屡屡发生“某某平台崩了”事件，这些“崩了”的平台和系统一部分是学校自己建设和维护的，另一部分是互联网企业提供的。在此背景下，师生、家长以及媒体发出了“开学上课第一天，你准备好了吗？”的齐声质疑。由此可见，这些平台或系统在应用的流畅度、易用性和参与用户的人数上限等方面都没有经历过大规模的演练与考验。

第二，OA 系统功能不完善，不能有效满足远程办公需求。几乎所有高校都有自己的办公自动化 OA 系统，疫情防控期间，员工在家办公期间，发现学校原来的 OA 系统不足以有效满足人们远程办公的实际需求，如缺乏“文档共享”、“协作编辑”等。此外，在疫情之前的平常使用中，也有学校为了保证安全，将学校 OA 限制在校内网络使用，使得远程办公效果不理想。

第三，移动客户端功能过于复杂，不够简洁。我们一直引以为豪的“一站式”服务、移动客户端在此期间，被师生用户纷纷呼吁“回归简洁”。因为“满屏都是服务应用，

自己想用的功能却找不到”，那些平常很少使用、疫情期间不得不用“一站式”系统的用户则抱怨系统“功能太多”。

第四，信息整合难。校园管控所亟需的“人员定位”、“信息采集”、“健康上报”、“动态监测”等功能难以为学校提供及时的定制，只能使用不同的问卷、文档共享等工具临时、零散满足个别需求，信息难以整合。

疫情防控下的突发需求对高校信息化部门的快速反应能力也提出了各种挑战，如面对“明天需要一个疫情捐款功能”、“需要下周开始收集学生的健康信息”、“需要立即启动校门管控”等需求，信息化部门很难满足职能部门需求，已有的系统不能满足这些场景，自主开发能力又不足，平时合作伙伴提供的系统又难以完全套用。在这种情况下，决策层及职能部门对信息化团队的质疑就不足为奇了。

挑战背后的原因

出现上述问题并非个案。可以说这些状况在很多学校都存在，其背后的原因是什么？

首先，各种系统、平台平常期间的压力测试不够。疫情期间使用的很多系统、平台在平常很可能没大范围使用过。没有经过足够的考验和演练，真正上战场的时候往往容易掉链子。

例如，针对业务系统的 10 个人的压力测试很常见，100 人的压力测试也是可能的，但要协调 1000 人的真实环境压力测试就比较困难了。更何况，平常如果发动大规模测试，很难找到足够多测试的用户，造成的结果就是，系统的性能指标到底是多少，最大的处理能力是多少，系统的瓶颈在哪里，这些问题都无法回答，答案只能是“理论值是多少”。

而信息化系统性能问题的尴尬之处在于，系统的上限如果是 500，当面临 1000 用户时受影响的不仅仅是第 501~1000 人，而是所有 1000 人都受影响，也就是说，系统崩溃后对用户的服务数是零，而不是 500，这就造成了所有用户的抱怨。

其次，高校信息化建设的多元主体参与机制设计不足。教学业务设计、管理服务需求主要来自于其他职能部门及院系，信息化部门往往被定位成“技术支撑部门”，也就是“业务不需要信息化部门关心，流程定了信息化部门来实现就行”，信息化部门缺乏参与决策的机会，最后的结果是信息化需求方给出的需求往往是“零散的”、“基于管理岗位要求的”、甚至“不同岗位之间的需求是相互抵触的”，可想而知，基于这种需求建设的系统很难满足“以用户为中心”这一服务理念。可以深度分析“高校大数据平台”、“一站式服务”、“AI 平台”、“校园智能管理”等等，其中也有类似现象。

可见，信息化系统常态化应用需要演练，更需要不断修改优化、快速响应，这就是信息化部门需要配备适当数量的二次开发人员的原因。系统的容量要经得起考验，系统功能的优化、基础数据的准确性等，都需要在常态化使用过程中不断地完善和提升，在这个过程中逐步实现“信息技术与教育教学、管理的深度融合”。在此过程中，需要技术实时、及时地为业务服务，而不是业务“将就”技术，因此二次开发队伍是必不可少的。这个过程不会一蹴而就，只有不断“融合”、“改善”，才能磨练出具有学校自身特色的平台与系统。

因此，高校信息化要做到持续可用，实现信息化长期目标，需要关注信息化需求确定者的信息化素养问题，需要重视设计与建设信息化过程中的多元主体参与架构，也需要承认一点一滴实现信息化与教育教学以及教学管理的常态化、深度融合是一个长期的过程性问题，信息化只有开始没有结束。

面对挑战，逐步走向信息化治理

如何在后续的信息化规划及建设中规避上述“尴尬”和“问题”，将学校有限的财力用到“刀刃”上，从而使信息化真正在高校的各项事业中发挥“革命性影响”的作用？

这就需要信息化部门与学校的各级决策者一起探索与实践信息化的多主体参与机制，构建信息时代下的“智慧校园”，明确信息化部门、职能部门及院系的作用，构建教育教学、管理、服务的常态化信息化融合模式，共同推进学校由信息化管理走向信息化治理。

首先，信息化部门要与学校各级决策者们一起讨论、明确需求，共同提高信息化领导力。大数据时代要了解“数据”，注重增强在决策时“用数据说话”的意识，学校的主要决策部门在决策过程中也应倾听信息化专业人员对业务流程的意见和建议；各级管理人员积极亲自使用信息化的工具或手段，在使用和体验中形成信息化思维。

其次，在信息化的规划和设计中，校领导、业务部门与信息化部门一起讨论，不仅仅是形成一个信息化的规划或使用信息化解决业务部门的部分问题，而是需要一起回答如何在物理空间的大学的基础上构建另外一个数字空间的大学，物理空间与数字空间的大学是融合的、一体的，这就是 Gartner 提出的“数字孪生”校园的概念，也是教育部提出的信息化与教育教学深度融合的要求。

今天，高校的教学、科研、管理与服务等活动是在两个空间中进行的，因此，高校的教育教学、管理服务等活动主体，除了信息化部门人员之外，包括教师、学生、管理者等，都是智慧校园的设计、建设、使用的主体，校园中的各个不同主体发挥着不同的作用，要分别在数字空间中找准自己相应的定位，不能缺位、错位、越位。

其中，信息化部门的主要职责是将支持多元主体参与的信息化技术框架搭建好，包括梳理好基础数据，搭建好身份认证、授权等 API 接口，来自其他职能部门或院系的系统可以通过这个框架、接口实现互联互通。

（来源：中国教育和科研计算机网）

CERNET 发布全球学术资源共享平台 CARSI 全力支持高校疫情防控 科研攻关

为满足广大高校疫情防控期间的科研需要，中国教育和科研计算机网 CERNET 近日发布全球学术资源共享平台--CARSI。通过该系统，高校师生在家就能访问国内外超过 14 万种期刊、超万种实验和教学视频。这也是 CERNET 落实党中央抗击疫情精神，以网络支持科研和教学的系列重要举措之一。

以往大量的学术资源库一般以校园网 IP 地址为身份认证基础，但疫情期间师生大多无法返校，因此难以顺利访问相关学术资源库，对于日常科研活动，尤其是针对疫情的科研攻关都产生一定影响。针对这一迫切需求，CERNET 网络中心紧急部署，在试运行并完善的基础上，日前正式发布全球学术资源共享平台 CARSI，以充分满足高校师生居家科研与教学的需要。

作为国家下一代互联网示范工程的一部分，CARSI 是 CERNET 联邦认证和资源共享基础设施（CERNET Authentication and Resource Sharing Infrastructure）的简称，是一项由北京大学发起，CERNET 网络中心组织管理，北京大学计算中心研发并提供技术支持，为已经建立统一身份认证的高校和科研单位，提供联邦认证和全球学术信息资源共享的服务。

2019 年 5 月，CARSI 服务加入全球联邦认证组织 eduGAIN，实现了与 60 多个国家的联邦认证，这其中包括 2600 多个国外高校与科研单位，1800 多个学术信息资源提供商。为已实现统一认证的高校及科研单位与学术信息资源提供商之间搭建了一个全球相互信任的大平台，彻底改变了传统高校和科研单位人员过去只能通过所在单位 IP 地址优惠或免费访问全球学术信息资源的局限。

基于 CARSI 系统，高校师生在任何时间，任何地点，通过任何终端，以任何联网形式，均可通过校园网账号访问资源。全程网页操作，无需下载插件或 APP，无需使用校园网 IP 地址，可支持师生在校外直接访问国内外需要身份认证的海量科研学术资源。

新冠疫情发生以来，为全力支撑高校科研攻关与在线教学，在 CERNET 网络中心统一部署下，北京大学等承担单位加快 CARSI 资源覆盖工作的同时，也积极向高校拓展服务。

疫情发生一个月以来，CARSI 接入共享教育科研资源高校数量已达 400 余所，比疫情初期增长了 300 多所，其中湖北疫区已经有包括武汉大学、华中科技大学、中南民族大学、武汉纺织大学等多所高校服务正式上线。签约的学术资源服务机构也大幅增长，在国外学术资源基础上，目前已签约专项服务中国的 13 家学术数据服务商，其中包括科睿唯安、爱思唯尔等 11 家境外著名数据库厂商以及知网、万方两家国内主要中文学术资源库，涵盖 14 万种中外期刊、超万种实验和教学视频。据悉，自新型冠状病毒肺炎爆发以来，全国通过 CARSI 访问学术资源的人数快速增长，已经从疫情初期的 1 万余人次/日，快速增长至 16 万人次/日。

疫情期间，CARSI 已帮助生物、化学和医学等领域专家，通过使用资源目录中的高性能计算资源和多方线上协作，为我国针对新型冠状病毒疫苗、特效药研制和国际合作提供了有效助力。

CARSI 的推出，不仅有效支撑了当下针对疫情的科研攻关，也可以有效简化我国高校与其他国家教育科研网共享应用资源的流程，积极促进我国教育科研的创新发展。

（来源：中国教育和科研计算机网）



5G+VR 已来 看萌科如何打造新课堂

随着 5G 商用落地，带动了新一轮科技革命和产业的变革，各行各业将搭载 5G 这趟“高铁复兴号”迎接新风口，其中 VR 将吸引更多的用户及院校关注，在教育领域带来颠覆性的技术革新。

2020 年年初，一场突如其来的新冠肺炎疫情肆虐，让我们的世界嘎然“停摆”。但有些行业得到了更多的关注和发展，例如：视频会议，和虚拟技术。2019 年 5G 的到来将给 VR 带来了强大的网络支持，打开了 VR 发展的时代之门，带来了广阔无边的 VR 创业机会，尤其是基于 VR 的下一代 5G 多人互动教育系统的发展，更是得到了更多院校的关注。

我们大家都知道，在教育多元化发展的今天，教育应当是尊重差异、可供选择、满足需求，让学生生动活泼的发展，让学生在特色化、多样化、可选择的学习过程中产生满足感、成就感和幸福感。而当前教育方式主要以视频为主，通过直播视频、MOOC、微课、SPOC 等方式传达，这种单向缺乏互动、枯燥、无法进行实验实训，使用平面形象无法营造真实授课感受。VR 技术的出现恰好解决了传统课堂无法实现的沉浸式学习体验，互动性的教学资源充分激发了学生的学习兴趣和学习的积极性。



在 5G 进入大规模商用的前夕，5G+VR 教育开始成为热门的话题。萌科立足 VR 教育，专注于虚拟现实、自然交互技术的研发多年，在结合 AI、网络直播等技术，构建了 VR 全景虚拟课堂，使异地多人从不同的设备上像真实面对面授课一样汇聚在一起，进行沉浸式的实时互动教学。

萌科 VR 可以有力支持理论及实验教学，现在已经进入虚拟空间中多人互动的时代。不论身在教室还是异地远程，所有师生都能通过 5G 或高速互联网进入线上虚拟教室，让教室随时穿越到任何时空，完成沉浸式的互动教学，互动实验，为学生提供高效率、低延迟、全自动的个性化学习。

每一轮技术进步都会催生新的内容表现形式，以前是文本、图片、视频等，当 5G 时代到来之时，VR 等科技将通过虚拟物品、虚拟人物、增强性情境信息等方式给人们带来连接媒体的全新方式，产生新的媒介，信息传播方式的变化会对社会造成重大影响，因此 VR 教育将得到重点关注。

尤其是在疫情过后，在线教育将在 5G、VR、AI 的辅助下，实现更好的跨空间、跨领域的共享教学资源，学生们将在远程课堂上感受真实的师生互动，从而有效的提高教学质量。

（来源：萌科 MK）

强安全 2020
Security

1月-3月，发现网络安全事件9起；发送正式整改通知9份。大连市网警通报了其中的两起网络安全事件，并要求责任单位限时整改。获得网警的整改通知书后，网络安全部第一时间与两个系统的负责人及厂商取得联系，详细说明了事件情况。厂商完成漏洞修复后，又及时对修复情况进行了确认，并陪同系统负责人向网警支队及时递交了整改情况说明与处置单。

1月-3月，发布网络安全预警公告11个。其中包括操作系统、服务器组件、浏览器等漏洞的安全公告，及恶意邮件的安全公告等。

2月，对数据中心部署 Apache Tomcat 的服务器进行了存在文件包含高危漏洞（CVE-2020-1938）排查。排查共发现四十余台服务器存在该高危安全漏洞，网络安全部逐一通知系统负责人对漏洞进行修复。3月初对漏洞修复情况进行复检，确认均已修复完毕。

（来源：郑维 网络与信息化中心）