2022年初，在大家以为疫情将要结束之时，新一轮疫情反扑。在传染力极强的奥密克戎病毒的影响下，高校陆续实施封闭管理，从生活到学习全面转移到线上。

与两年前相比，这一轮疫情对校园网的压力极大：两年前，学生们大都分散在家，这一次，学生基本在校内，网络需求集中在校内。校园网的稳定运行，成为高校抗疫的关键点，与抗疫的胜利紧密相连。

迅速响应，毅勇行动。面对疫情带来的巨大挑战，中国教育和科研计算机网CERNET与运营单位赛尔公司用技术全力守护着校园。

一项全力保障的任务

“为做好疫情防控期间的网络保障，提高在线教学体验，昨夜今晨，上海教育城域网和CERNET互联线路在徐汇校区机房已完成大幅度升级扩容。”3月14日一早，上海交通大学信息化推进办公室、网络信息中心副主任姜开达在社交平台说。

当时上海的疫情反扑开始严重，高校纷纷进入封闭管理模式，学校的活动大都转为线上进行。这使得上海节点带宽压力骤增，出口流量几乎跑满，必须紧急扩容。

3月12日，接到CERNET主干网扩容任务后，CERNET上海节点、赛尔上海分公司紧急调配资源，与上海教育城域网管理中心和上海市大数据中心教育信息化团队紧密配合，连续奋战，于14日凌晨2点，完成百G扩容。此次扩容行动最大程度保障了上海师生在校园封闭管理期间，高速访问互联网资源的需求。

因在线教学的巨大带宽压力，带宽的扩容、保障与优化，成为贯穿疫情期间的一项持续行动。

5月初，CERNET收到消息：同济大学与上海地区网互联带宽20G已经跑满，学校的线上教学活动受到极大影响。但基于上海前期多轮扩容，当下线路已满，再追扩容难度很大。

经过讨论，CERNET运行团队提出建议：用下一代互联网CERNET2线路开通IPv4 Over IPv6隧道，从而让学校可以通过CERNET2的设备来接入业务，实现用户带宽的增加。

但在尝试接入线路后，测试结果并不理想，流量始终无法超过1M，网站访问也不稳定。反复测试后，终于发现问题所在，并在第一时间妥善处理。再次测试后，流量成功跑至4G，此次扩容任务，切实保障了同济大学的用网需求。

一项全新的技术支持

如果说主干网保障是一项日常工作，那么协助高校防范与治理“挖矿”则是2022年CERNET面临的一项全新工作。

3月以来，CERNET网络中心接到不少高校治理“挖矿”的技术求助。

虚拟货币的生产过程被称为“挖矿”。因为比特币过去几年迅速增值，全球“挖矿”活动愈发严重。但“挖矿”本身对能源产生巨大消耗，同时影响着金融等各个领域，基于此，国家相关部门去年年底加大治理力度，要求各领域全面梳理排查虚拟货币“挖矿”活动。今年3月开始，我国对“挖矿”的治理进入攻坚期，其中，高校因本身特有的硬件基础和用户特点成为重点治理领域。

但如何治理挖矿？对于今年年初的高校来说还是一个难题。因为没有过往经验可以借鉴。在接到治理求助后，CERNET通过筛查数据、编写程序，对学校半年以来的流量记录进行比对，并结合威胁情报分析、态势感知、关联流量分析等技术，分析判断出可疑的矿池地址，筛查出几千个地址段，最终协助学校及时治理校内“挖矿”行为。

在治理的过程中，教育网“挖矿”监测平台起到了重要作用。这是CERNET专门为支持教育领域防范“挖矿”而开发的平台。平台将流量日志和矿池IP相互匹配，确认具有挖矿嫌疑的IP地址。经人工复核后，对可能存在挖矿活动的高校通知提醒，协助高校及时发现处理挖矿活动。

截至6月16日，平台共检测出400多所学校的4308个IP疑似存在“挖矿”行为，收集到9324个矿池地址，数据每天更新，他们还根据全国高校挖矿活动的密集程度形成治理地图，为相关领域提供数据支持。

授人以鱼，不如授人以渔。CERNET网络运行部门还和清华大学信息化技术中心联合发布《挖矿病毒自查和防护指南》，为广大高校处置挖矿提供了切实可行的实际操作方法。

在CERNET的助力下，教育领域防范“挖矿”工作进展取得初步成效，既保

障教育领域网络安全，也助力国家向碳达峰、碳中和目标的实现，体现了教育网服务教育和国家的大网担当。

一场与DDoS攻击的斗争

在“挖矿”的新挑战外，校园网还面临着一些传统的网络安全攻击，其中，DDoS拒绝服务攻击是典型代表。前不久北京健康宝系统在使用高峰期遭受境外攻击，采用的手段就是DDoS攻击。如何协助高校发现和处理DDoS攻击，也是CERNET一直以来的重点工作。

4月的一天，CERNET网络中心接到赛尔重庆分公司求助：“部分高校遭受DDoS攻击，导致用户无法正常访问网络资源。”

DDoS拒绝服务攻击是一种传统攻击手段，以破坏服务可用性为目的，会直接导致系统或网络无法提供正常服务。而在疫情期间，学校的各项工作对网络高度依赖，此时发生DDoS攻击，影响更严重。

接到报障后，CERNET网络运行部门紧急启动安全应急预案，抓取用户流量信息进行分析，发现这次攻击除了涉及面广，攻击手段还很多样，溯源后，追踪到了所有攻击的源地址，随后紧急分析出应对方案，及时帮助用户解决了攻击，恢复了业务。

随着当前国际政治经济环境复杂化，各种DDoS攻击事件也层出不穷。为更好地守护主干网和校园网，CERNET不断提升对DDoS攻击的溯源和取证能力，并开发了多个攻击行为分析系统，在多次实战中发挥了重大作用。

一个IPv6部署服务平台

疫情期间，CERNET对高校IPv6规模部署的技术支持工作仍在有条不紊地进行。

6月初，甘肃省教育厅对全省教育系统2022年第一季度门户网站IPv6支持度评测情况进行通报。“教育系统IPv6发展态势监测平台”测评数据显示，赛尔甘肃分公司承担的甘肃林业职业技术学院校园网IPv6建设项目，以IPv6支持度评分100分、甘肃省内高校IPv6支持度排名第一的成绩交付。

依托特有的技术，CERNET和遍布全国的赛尔技术人员正有力地支持着教育领域的IPv6规模部署行动。

2017年底，两办发布《推进互联网协议IPv6规模部署行动计划》，随后，教育部办公厅发布关于贯彻落实IPv6规模部署行动计划的通知，明确指出，“到2020年底，教育系统的各类网络、门户网站和重要应用系统完成升级改造，支持IPv6访问，基于IPv6的安全保障体系基本形成。”

在当时，对全国大多数高校来说，IPv6的部署是陌生的，充满了各种技术挑战。如何为教育领域推进IPv6规模部署提供技术、研究、数据的支持？基于此，在教育部科技司和CERNET网络中心的支持下，赛尔公司开发了“教育系统IPv6发展态势监测平台”。

平台通过监测、收集、分析及统计相关单位的IPv6网络建设、应用建设和运行数据，对教育系统IPv6发展情况进行动态监测和多维度实时分析。在平台上，学校的IPv6活跃用户，IPv6网络性能，网站IPv6支持率这几个重要因素一目了然。

这样，一方面可以形成一个整体的情况，帮助教育部门了解领域整体的IPv6部署情况，从而形成指导性政策。另一方面，对于每所高校来说，就可以获取到自己IPv6发展的多维度情况，从而形成一个定制化的IPv6部署地图，清楚自己的短板所在，及时追踪并补齐。平台开发到现在，支持着3000多个单位的IPv6规模部署工作。

CERNET是全球IPv6研究的先锋，最早建成全球第一个纯IPv6主干网CERNET2，并探索研发了下一代互联网真实源地址验证体系结构SAVA、两代网过渡技术IVI，对于引领全球互联网向下一代互联网IPv6平滑过渡具有重要意义。

新形势下，CERNET和赛尔又在承担着新的使命。在两办发文推动IPv6规模部署行动后，又责无旁贷承担着教育领域向IPv6过渡的技术服务支持。对于高校在IPv6规模部署中存在的任何技术细节问题，遍布全国的赛尔分公司技术人员都在及时跟进和解决。

用大网的技术资源和能力，用自己的技术经验和服务，疫情期间，CERNET人为千千万万的教育用户提供着高质及时的网络服务，支持着抗疫，守护着校园。