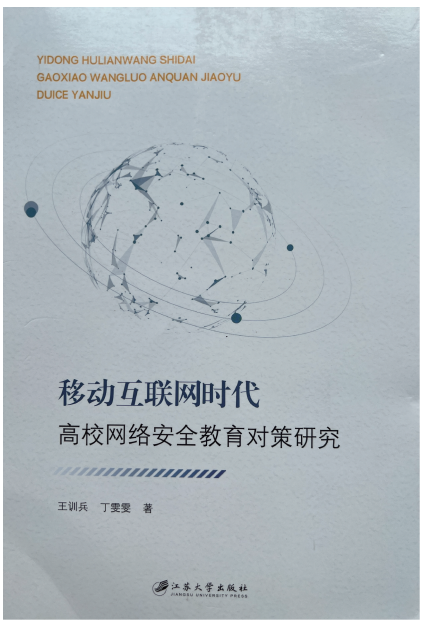
数智时代高校网络安全教育策略
——评《移动互联网时代高校网络安全教育对策研究》

数智技术的浪潮已彻底重塑了象牙塔的肌理。智慧校园不再是简单的数字化堆砌,而是演变为一个物理空间与数字空间深度孪生的复杂生态。从“一网通办”的便捷到人工智能(Artificial Intelligence,AI)助教的普及,数据如血液般在校园的每一根血管中奔涌。然而,光影相生,阴霾随行。多数高校曾遭遇网络安全事件,数据泄露、勒索软件、钓鱼攻击如同隐形的达摩克利斯之剑,高悬于学术殿堂之上。面对这一严峻局势,传统的“防火墙+杀毒软件”式教育已难以为继,必须以雷霆之势,构建一套涵盖认知重塑、技术赋能与生态共治的立体化防御教育体系,将网络安全教育从枯燥的说教转化为深入骨髓的生存本能。



书名:移动互联网时代高校网络安全教育对策研究
作者:王训兵,丁雯雯
出版社:江苏大学出版社
ISBN:9787568420693
出版时间:2024年10月
定价:58元

当“5G+工业互联网”项目遍地开花,网民规模突破10亿大关时,高校作为人才培养的摇篮,其网络安全教育却正面临着前所未有的至暗时刻与破局机遇。笔者在开展2023年辽宁省教育厅基本科研项目青年项目(文科类)(JYTQN2023226)研究过程中,认真阅读了《移动互联网时代高校网络安全教育对策研究》一书,该书为笔者提供了思考与对策。全书共6章,第1章概述解读了研究背景与意义,梳理国内外现状,并厘清思路方法;第2章搭建理论骨架,界定移动互联网与网络安全教育概念,引入国家总体安全观理念下的关于网络安全重要论述;第3章聚焦机遇,指出移动互联网在丰富内容、整合资源、拓宽平台及创新载体方面的积极作用;第4章直面挑战,分析威胁多样化、意识形态冲击、校园风险增加及教育体系缺陷等现实问题;第5章基于实证调查,揭示大学生网络安全素养不足及教育体系不健全等短板,并从市场环境、网络特性、学生自身及教育合力等维度剖析成因;第6章提出对策,明确目标原则,借鉴国外经验,强调提升自我教育能力,通过完善课程设置、推进生活场景导向的实践教学等路径创新,形成“理论-问题-实证-对策”的完整闭环。

该书作者指出,网络安全意识与素养是最基础,也是最重要的防线,其可通过安全教育方式形成,因此,高校应推动网络安全教育从被动合规向主动防御的观念跃迁,重塑学校全体师生网络素养的“精神防线”。高校师生群体庞大、IT技能参差不齐、设备类型繁杂,从教授的科研数据、学校的管理数据,以及新生的奖学金助学金信息,无一不是黑客眼中的“金矿”,具有非常高的数据价值。现实中,不少高校曾遭遇网络安全事件,轻则系统瘫痪,重则敏感数据泄露,甚至引发意识形态危机。要摒弃“网络安全只是信息中心的事”这种荒谬的甩锅思维,必须建立“人人都是安全官”的全员防线。这种防线不是靠几场讲座就能建立的,而是要将安全意识植入每位师生的骨髓。首先,要击碎“侥幸心理”的泡沫。看看那些触目惊心的案例,如某高校学生因设置弱密码,导致电脑沦为黑客跳板,瘫痪了整个校园网;某毕业生盗取全校学生信息搭建“颜值打分”网站,最终身陷囹圄;还有学生为了兼职蝇头小利,缺乏信息安全意识,在申请兼职和实习过程中没有保护好个人的信息隐私,最终泄露人脸识别数据,最终导致出现一些无法预控的信息风险,损失惨重。作为大学生要深刻意识到,现实生活中的每一次弱密码设置、每一次随意扫码、每一次违规翻墙,都可能成为攻破校园堡垒的“蚁穴”。其次,要将网络素养教育纳入“大思政”课堂,实现从知识灌输到价值引领的升华。网络空间是意识形态斗争的主阵地。要旗帜鲜明地反对历史虚无主义,抵制网络暴力与低俗内容。要利用国家网络安全宣传周等节点,通过情景剧、短视频、沉浸式体验等鲜活形式,让学生在震撼中学会辨别真伪,在思辨中坚定“四个自信”。当学生在面对境外势力策反、网络间谍勾连时,能具备敏锐的政治鉴别力,敢于亮剑,这才是最高级的网络安全——政治安全与思

想安全。最后,要培养“洁癖式”的用网习惯。在公共 WiFi 下不办公、不乱插陌生 U 盘、不随意转借账号,这些看似琐碎的细节,实则是数字公民的基本操守。要让“保护隐私如保护生命,守护数据如守护黄金”成为校园文化的一部分,让安全用网成为一种无需提醒的自觉。

笔者认为,数字化转型的核心是数据,而数据的流动性决定了安全风险的无孔不入。长期以来,高校信息化建设存在“重建设、轻安全”“数据孤岛林立”“权责不清”的顽疾。教务处管成绩,学工部管学籍,财务处管经费,数据像碎片一样散落在各个角落,一旦某个环节失守,全盘皆输。构建现代化的安全体系,必须依靠严密的制度闭环和责任链条,彻底告别“打补丁”式的被动防御。①必须确立“数据分级分类”的治理基石。不是所有数据都要用核武器级别的防护,要集中力量保卫核心资产。对于涉及国家安全的科研数据、师生个人隐私、学校核心机密,必须实行“绝密级”管理,采用数据库防水坝、高强度加密、细粒度访问控制等技术,确保“核心数据不出域,敏感信息不落地”。对于一般性行政数据,则要在保证效率的前提下规范流转。宁波大学、西安电子科技大学等高校的实践证明,通过建立数据目录、明确责任主体、实施脱敏展示,可有效平衡数据共享与安全保护的矛盾。②必须压实“党政同责、一岗双责”的政治责任。网络安全不再是技术部门的“独角戏”,而是全校上下的“大合唱”。要成立由党政一把手牵头的网络安全领导小组,将安全指标纳入各部门考核,实行“谁主管谁负责、谁使用谁负责”。对于因管理疏漏导致数据泄露的,必须启动问责机制,绝不姑息。要建立“网格化”管理体系,将安全触角延伸到每一个课题组、每一个实验室、每一个宿舍,打破信息孤岛,形成全校“一盘棋”的协同治理格局。③必须构建“全流程、全链条”的运维体系。安全不是一次性的工程,而是动态的过程。从系统上线前的安全评估,到运行中的实时监测,再到废旧系统的数据销毁,每一个环节都要有章可循。要引入专业的第三方力量,建立“校企协同”的联合运维模式,利用企业的前沿技术和专家资源,弥补高校专业人才短缺的短板。通过部署态势感知平台、高级持续性威胁攻击检测系统,实现对威胁的“秒级发现、分钟级处置”,让安全运维从人工救火转向智能御敌。

在网络安全的战场上,只有被攻破或守住 2 种状态,没有中间地带。网络安全的本质在对抗,对抗的本质在攻防两端能力较量。如果防御手段还停留在 10 年前的水平,面对有组织、有预谋的高级持续性威胁,无异于以卵击石。高校网络安全教育的终极目标,是培养一支“拉得出、打得赢”的实战化队伍,构建“云、边、端”协同的纵深防御体系。一方面,要打造“实战化”的人才培养模式。不能再让学生在虚拟机里玩过家家,必须建设高仿真的网络靶场和攻防实验室。要引入真实的攻击场景,开展红蓝对抗演练,让学生在模拟的 DDoS 攻击、SQL 注入、社会工程学陷阱中,真切感受系统被撕裂的痛感,从而学会如何修补漏洞、如何追踪溯源、如何进行应急响应。要鼓励学生参加 CTF 夺旗赛、漏洞挖掘比赛,以赛代练,在真刀真枪的较量中磨砺技艺。正如长安大学利用 OSM 平台实现运维自动化一样,要用最先进的工具武装学生,让他们在走出校门前就具备企业级的安全防护能力。另一方面,要构建“智能化”的技术防御体系。面对海量的告警信息和复杂的攻击手段,单纯靠人力已无法应对。必须大力推进“智慧防御”,利用 AI、大数据分析技术,构建校园网络安全态势感知中心。这不仅是一个大屏幕,更是一个“超级大脑”,它能从海量日志中抽丝剥茧,发现异常行为;能自动识别未知威胁,阻断攻击链条;能预测风险趋势,提前发布预警。

总之,“皮之不存,毛将焉附?”网络安全是高校发展的底座,也是师生幸福的保障。在数智时代,这场没有硝烟的战争每天都在进行。对于网络信息安全,不能掉以轻心,必须时刻保持“箭在弦上”的紧迫感。通过重塑全员觉醒的精神防线、织密制度铁网的治理体系、打造实战对抗的硬核战力,不仅是在保护几台服务器、几行代码,更是在守护国家的科技命脉,守护民族的未来希望。让我们以坚定的决心、雷霆的手段、智慧的策略,共同筑牢校园网络安全的铜墙铁壁,让数字技术真正成为赋能教育强国的“翅膀”,而非悬在头顶的“达摩克利斯之剑”。这不仅是教育的使命,更是对国家、对民族必须交出的合格答卷!

(李典/辽宁工业大学马克思主义学院/讲师)