Laboratories：高等教育网络安全实验室的模块化框架

作者：writer 来源：科学网

本文原地址：https://www.iikx.com/news/progress/37072.html

Laboratories：高等教育网络安全实验室的模块化框架。论文标题：A Modular Framework for Cybersecurity Laboratory Design in Higher Education

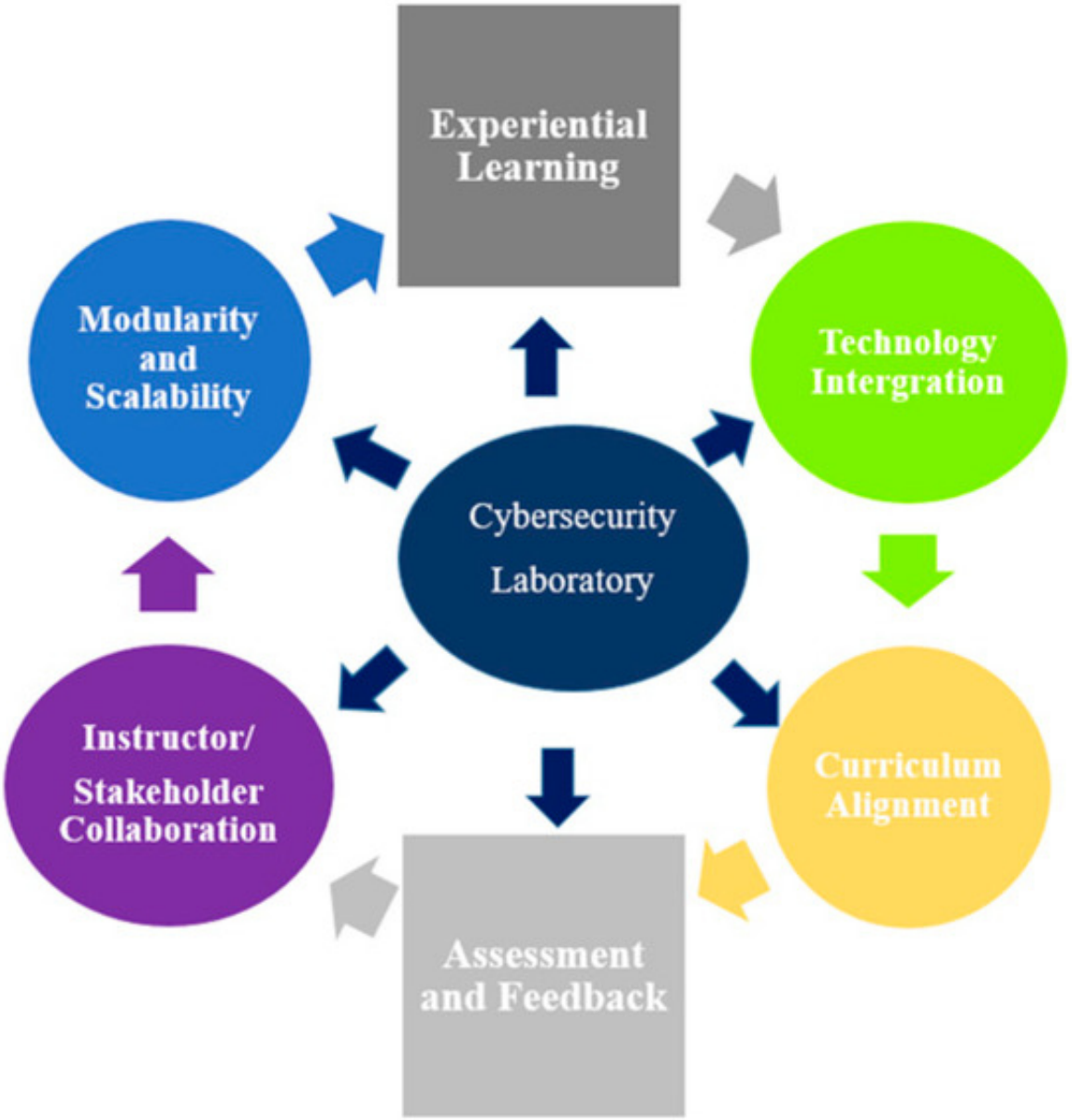
论文链接：https://www.mdpi.com/2813-8856/2/4/21

期刊名：Laboratories

期刊主页：https://www.mdpi.com/journal/laboratories

在数字技术全面渗透社会经济的今天，网络攻击的频次与复杂度呈指数级增长，网络安全已成为保障国家数字基础设施的核心支柱。高等教育作为网络安全人才输送的关键源头，却长期受困于理论与实践的严重脱节 —— 传统课程体系虽能传授密码学、网络协议等基础理论，却无法为学生提供应对真实攻防场景的实操训练，导致行业百万级人才缺口与毕业生 纸上谈兵 的矛盾愈发突出。针对这一结构性难题，近期发表于《Laboratories》期刊，由美国安柏瑞德航空大学 Sharon L. Burton 博士完成的研究《A Modular Framework for Cybersecurity Laboratory Design in Higher Education》提出了模块化网络安全实验室设计框架（MACLF），为高等教育机构构建实践教学体系提供了系统性解决方案。

本文核心创新为融合体验式学习理论与成人学习理念，通过多阶段案例研究（整合文献分析、实地观察、半结构化访谈及前后测评估）验证框架有效性。研究以5个六周试点、15-25名具备3年以上技术经验的成人学习者为对象，保障结果的实践代表性与普适性。MACLF框架以美国教育理论家和心理学家David A. Kolb1984年体验式学习周期理论为基础，将学习拆解为具体体验、反思观察、抽象概念化、主动实验四阶段，对应构建六大核心组件：体验式学习衔接理论与实操；模块化与技术整合保障功能灵活配置；可扩展性适配院校资源差异；协作模块促进教学相长；课程对齐组件匹配行业需求；评估反馈支撑教学优化。架构兼具系统性与灵活性，适配不同院校培养定位。



由 SL Burton 博士 (2025) 开发的模块化自适应网络安全实验室框架 (MACLF)

技术落地以虚拟化与沙箱（或虚拟练习环境）技术为核心，通过虚拟机与容器化技术，依托有限硬件模拟复杂网络拓扑，为学生提供隔离环境开展漏洞利用、攻击溯源等高危实操。沙箱环境既降低硬件成本，又实现训练实时追踪与动态评估，解决传统实验室场景更新慢、风险高、资源消耗大等痛点。

试点数据显示成效显著：参与者实操成绩平均提升20%以上，漏洞分析等核心能力突出；课堂参与度提升40%，协作与问题解决能力获行业认可。框架模块化特性可应对场地调整、系统停机等突发状况，实现教学零中断，验证了实践韧性。

该框架为院校带来多重价值：可扩展性支持随招生规模、技术迭代平滑升级；跨学科组件打破院系壁垒（如Ohio大学SecureAcademy项目培养复合型人才）；还可拓展为行业培训平台，强化院校产业联动。

针对预算约束、师资滞后、技术迭代等行业挑战，框架提出模块化渐进建设方案，降低落地门槛。Burton博士强调，其核心价值是构建自我迭代的教育生态，推广后可缩小人才缺口，推动网络安全专业向需求导向、实践为先转型。未来将探索AI与教学融合，追踪训练对职业发展的长期影响。

综上，MACLF框架为网络安全实践教学提供标准化方案，助力院校突破资源限制，提升办学质量，为数字安全输送专业人才。