

CYBER-INFORMED ENGINEERING: ENGINEERING OUT THE CONSEQUENCES OF CYBERATTACKS



September 28 at 4:30 - 6 p.m.
DMC Theater, LSU Digital Media Center



RSVP HERE

Benjamin Lampe

IDAHO NATIONAL
LABORATORY

ABSTRACT

Modern engineered systems—from industrial machinery to transportation networks to critical infrastructure—increasingly depend on digital technology to coordinate, control, and optimize how they function. That dependence delivers real gains in efficiency, visibility, and performance, but it also introduces a risk most engineering disciplines were never designed to handle: the possibility that the very digital components a system relies on could be manipulated or compromised by an adversary. This talk introduces Cyber-Informed Engineering (CIE), a framework developed by Idaho National Laboratory and the U.S. Department of Energy that reframes digital risk as an engineering problem, not just an IT problem. Rather than treating cybersecurity as something wrapped around a finished design, CIE asks engineers to build resilience into the system itself, at the design, operational, and maintenance stages, so that core functions keep working safely, reliably, and performantly even when the digital layer can't be fully trusted. We'll walk through the central question CIE poses to engineers: if an adversary successfully manipulates the digital technology inside your system, what still has to hold true? And we'll look at how CIE's twelve principles, including engineered controls, secure information architecture, consequence-focused design, and planned resilience, give engineers concrete ways to answer that question, independent of what cybersecurity operations are doing elsewhere. The talk's central argument: cyber-against-cyber defense is necessary, but it's good only until it isn't. Zero-days, misconfigurations, and abuse of implicit trust eventually get through. Real resilience comes from pairing strong digital defenses with engineered, physical or logical backstops that don't depend on the digital layer behaving correctly.

SPEAKER BIO

I am an engineer and researcher at the Idaho National Laboratory (INL), specializing in Cyber-Informed Engineering since September 2023. Previously, I held a position as a faculty member in the ICS Cybersecurity program at Idaho State University, where I was a joint appointee with the INL. My professional journey includes significant roles at the Naval Nuclear Laboratory (NNL), where I served as an Operational Technology (OT) Enterprise Architect, Systems Analyst, and a Controls Engineer. In these roles, I formulated the OT technical strategy and implemented a nation-wide OT infrastructure between the NNL's process systems. As a control engineer, I maintained a myriad of process and monitoring systems within power distribution, water and wastewater management, building automation, and radiological monitoring. I have a Bachelor of Science in Electrical Engineering from the University of Wyoming, and a Master of Science in Computer Science from the University of Idaho.