#4 - Cybersecurity Risks in Overseas Military Construction: Practical Measures to Protect Infrastructure in EUCOM & AFRICOM

Summary

Overseas construction faces growing cyber threats that can affect cost, schedule, and mission readiness. This session shows how to identify vulnerabilities in design and construction processes and apply simple, effective cybersecurity controls. Attendees will learn how to strengthen infrastructure resilience across EUCOM and AFRICOM through better planning and contractor collaboration.

Full Description

Military construction and infrastructure projects across Europe and Africa now face a rapidly evolving set of cyber risks that directly impact cost, schedule, safety, and mission assurance. From Building Management Systems and power distribution controls to cloud-connected design tools and automated construction equipment, modern MILCON projects rely on digital systems that adversaries can disrupt long before concrete is poured or equipment is energized. These challenges are amplified in EUCOM and AFRICOM, where Host Nation standards vary widely, supply chains cross multiple jurisdictions, and units often operate with reduced on-site cybersecurity capacity.

This session provides a practical, non-technical framework for military engineers, planners, contracting officers, and industry partners to identify and mitigate the most common cyber vulnerabilities encountered during planning, design, and construction of overseas facilities. Drawing from real assessment experience supporting the Missile Defense Agency, NATO-connected programs, NAVFAC, and multiple industrial control system hardening projects, the presentation explains how cyber weaknesses emerge during design reviews, material selection, vendor engagement, and installation—and how simple process improvements can substantially reduce exposure.

Attendees will learn how to apply basic cybersecurity requirements early in project development; evaluate Host Nation contractor risk; manage digital submittals and remote

access; integrate cybersecurity into quality control; and ensure operational technology (OT) systems—HVAC, water, microgrids, sensors, access control, and monitoring—are delivered in a secure and resilient state.

This session is designed to strengthen collaboration between government and industry, reduce rework caused by late-identified cyber issues, and help the Tri-Service engineering community deliver safer, more resilient infrastructure across EUCOM and AFRICOM.

Learning Objectives

- Identify the most common cyber vulnerabilities that arise during design, planning, and construction of overseas military facilities.
- Apply practical cybersecurity controls to Host Nation contractors, digital submittals, OT/ICS equipment, and vendor-provided systems.
- Integrate cybersecurity into quality management, reducing rework and preventing cyber issues from emerging during commissioning.
- Strengthen collaboration between government and industry to deliver more resilient, secure infrastructure in resource-constrained environments across EUCOM and AFRICOM.

Speakers

Jonathan Hard is the CEO and Founder of H2L Solutions, Inc., a Service-Disabled Veteran-Owned Small Business specializing in cybersecurity engineering, cyber readiness assessments, and secure system integration for the Department of Defense. A U.S. Army Reserve Major and Signal Officer with more than 17 years of service, he has led cyber efforts for the Missile Defense Agency, NAVFAC, the U.S. Navy's HM&E modernization programs, GVSC, USACE, and international defense partners. Hard's teams have executed ICS/OT hardening, facility cybersecurity reviews, and mission-assurance assessments across multiple theaters. He is recognized for delivering practical, mission-focused cybersecurity solutions that improve resilience and reduce risk in complex environments.