Proposing the Integrated Virtual Learning Environment for Cybersecurity Education (IVLE4C)

Jeff Greer
greerj@uncw.edu

Geoff Stoker
stokerg@uncw.edu

Ulku Clark
clarku@uncw.edu

Congdon School
University of North Carolina Wilmington
Wilmington, NC 28403, USA

Abstract

Current U.S. military theory views warfare at three levels: strategic, operational, and tactical. This model allows commanders to better visualize linkage from national objectives to tactical actions. We borrow from this model and suggest that cybersecurity understanding, expertise, and education can be similarly oriented around three perspective levels we currently call: Government (GV), Enterprise Leadership (EL), and Enterprise Employee (EE). Informal observation of the current cybersecurity education landscape reveals tremendous educational effort at the EE level supported by a plethora of virtual environments. Often called cyber ranges, these environments offer operator and first-level supervisor skill development delivered from a computer network-centric perspective. At the GV and EL levels, educational opportunities are sparser, come late in the formal education process, and lack supporting virtual learning environments. This paper proposes creating an Integrated Virtual Learning Environment for Cybersecurity Education (IVLE4C) to help bolster cybersecurity education at the EL level. IVLE4C is a conceptual learning model based on six interrelated knowledge domains which, when aggregated, define a modern digital enterprise and its cybersecurity posture. IVLE4C can be used to train *inter*-functional skills at the EL level or *intra*-functional skills at the EE level. We contend that IVLE4C will provide three key benefits: improve cybersecurity pedagogy, enhance cross-enterprise EL training, and advance cybersecurity technology development.

Keywords: Cybersecurity, Education, Virtual Learning Environment, Model, Paradigm

An updated version of this manuscript may be found at https://cppj.info