MAP05

Supply Chain Risk Management: When More Connectivity = More Risk

Ross Jackson[1], Barry Humphrey[2], Paul Hartman[3]

[1]RGBSI Aerospace & Defense Advanced Technologies Laboratory, Fairborn, Ohio, USA. [2]Defense Logistics Agency, Research & Development, Manasas, Virginia, USA. [3]RGBSI Aerospace & Defense, Fairborn, Ohio, USA

Abstract

The current vision of the U.S. Department of Defense (DoD) is to establish a globally connected, resilient, defense ecosystem to ensure the material readiness of the force in a contested logistics environment. This research addresses cybersecurity challenges in complex ecosystems, focusing on supply chain interactions and compliance. A simulation model revealed that breaches become inevitable with network connectivity over 22% or efficiency at 60%. The study emphasizes the need for resilient systems, advocating for optimized interconnectivity to balance benefits and risks. It highlights the limited impact of compliance without systemic changes and identifies conflicts with Tier-3 suppliers. Organizations are advised to shift strategies towards resilience, optimize interconnectivity, and design cost-effective cybersecurity policies aligned with mission objectives. This work contributes to cybersecurity decision-making by balancing security and efficiency.

Conference Track

Military Applications