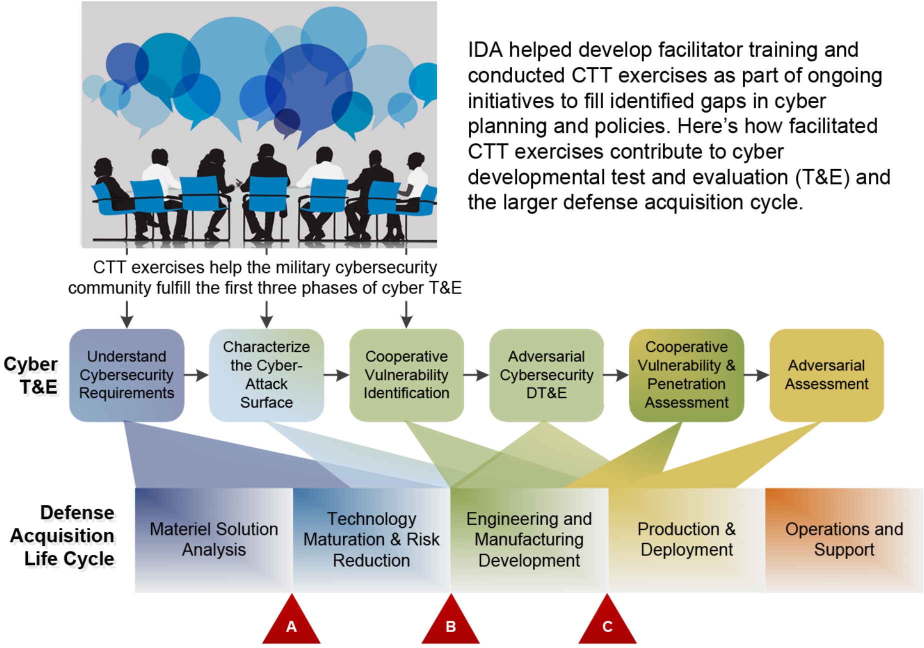
IDA | Research Insights

November 2017

Closing Gaps in Cybersecurity Developmental Test and Evaluation

Michael A. Ambroso, mambroso@ida.org

Following a 2016 IDA survey of organizations involved in cybersecurity developmental test and evaluation, staff from several divisions of IDA's Systems and Analyses Center have been collaborating with sponsors, test teams, and others to begin to fill some of the gaps the survey identified. The focus of these collaborations has been on research to inform policy and guidance, technical analysis in support of programs, and support to cybersecurity test teams. One of several initiatives that have evolved from these efforts is advancing the practice of cyber tabletop (CTT) exercises.


CTT exercises help the military cybersecurity community fulfill the first three phases of cyber T&E
Cyber T&E
Understand Cybersecurity Requirements
Characterize the Cyber-Attack Surface
Cooperative Vulnerability Identification
Adversarial Cybersecurity DT&E
Cooperative Vulnerability & Penetration Assessment
Adversarial Assessment
Defense Acquisition Life Cycle
Materiel Solution Analysis
Technology Maturation & Risk Reduction
Engineering and Manufacturing Development
Production & Deployment
Operations and Support
A
B
C

IDA helped develop facilitator training and conducted CTT exercises as part of ongoing initiatives to fill identified gaps in cyber planning and policies. Here's how facilitated CTT exercises contribute to cyber developmental test and evaluation (T&E) and the larger defense acquisition cycle.

Corresponding phases of the defense acquisition life cycle include two milestone decisions (labeled A and B) to confirm that requirements to that point have been met

Table top exercises involve the informal exchange of ideas about potential responses to a specific scenario. Such exercises have long been used to assess plans, policies, and procedures of emergency response teams, crisis management personnel, and the like. But applying the tabletop concept to cybersecurity is a relatively new idea that has been executed inconsistently until now.

Training CTT facilitators: IDA researchers have been working alongside the Deputy Assistant Secretary of Defense for Developmental Test and Evaluation (DASD[DT&E]) and his staff to develop a formal process for building a cadre of practitioners in the Department of Defense (DoD) with the knowledge, skills, and abilities to effectively facilitate CTT exercises. Through both practice and training, these practitioners learn how to successfully construct, coordinate, organize, and execute a CTT exercise on their own.

So far in 2017, over 480 people have received training during 22 sessions that IDA researchers and collaborators from DASD(DT&E) and MITRE delivered at military facilities throughout the United States, and more have been planned. Over 60 of those trained are now fully certified to run a CTT exercise alone. CTT facilitator training is contributing to a growing awareness of cyber issues and increasing the workforce available to plan and host CTT events.

Executing CTT exercises: DASD(DT&E) and IDA efforts to train and equip DoD have led to the execution of 16 CTT exercises so far in 2017, and at least that many more are planned. These low-cost, intellectually intensive wargames use informal dialogue to explore the effects that potential cyber offensive operations would have on the capabilities of warfare systems. The insight participants gain contribute to the first three phases of cyber test and evaluation (see figure). Participants leave these exercises with useful information about high-priority/high-mission-impact cyber threats. Such information clarifies cybersecurity concepts to program managers and system operators and bridges gaps between systems engineering, testing, and operations.

Based on research sponsored by the Deputy Assistant Secretary of Defense for Developmental Test and Evaluation.

NS D-8816

4850 Mark Center Drive
Alexandria, VA 22311-1882
www.ida.org