INFORMATION ASSURANCE ASSESSMENTS
FOR FIELDED SYSTEMS DURING COMBATANT COMMAND EXERCISES

Dr. Shawn C. Whetstone

The Problem

Ground rules guiding combatant command exercises frequently discourage introduction of elements that distract from training objectives. This has inhibited the ability to insinuate cyber disruptions into gaming scenarios, thus masking the effects of cyber attacks on exercises, potentially slowing awareness of problems and corrective actions.

Increasing operational realism during training exercises by allowing cyber warfare to disrupt operations is needed to understand the potential operational effects of cyber activities.

To help monitor DoD efforts to improve its information assurance posture, the National Defense Authorization Act (NDAA) of October 2002 tasked the operational test community and information warfare centers to conduct annual operational information assurance assessments during major Combatant Command and Service training exercises. The Director, Operational Test and Evaluation (DOT&E) leads the efforts. To help accomplish this task, DOT&E draws upon IDA's expertise with operational and information technology assessments and familiarity with assessments performed during large-scale exercises.

Learning About Adversaries' Goals

IDA's role is to provide: (1) analytical support to DOT&E's oversight of the assessments and (2) analyses of data to identify issues and trends from multiple exercises, such as the relationships between cybersecurity and other security functions including physical access and disposal of information. Our work has confirmed an increased emphasis by attackers on gaining entry to secure areas for placing unauthorized devices, accessing unattended workstations, seeking improperly secured papers, and searching through trash for passwords or personal information to establish initial entry points into networks.

Exploitations during training exercises are increasingly focused on intelligence gathering rather than on disrupting information systems and networks – an observation that mirrors experiences in the commercial sector. Factors contributing to these trends include restrictions on permitted attacker activities and the realization that intelligence gathering is valuable for adversaries and the opposing forces in the exercise environment. Network defenders are countering

adversaries' intelligence gathering activities with increased protection of critical operational information and deception operations that provide false information to known compromises.

Red team focus on intelligence-gathering highlights the interplay between interoperability and security. Operators are increasingly using chat tools and web portals to communicate and exchange critical operational information. The assessments are helping establish an appropriate balance between an operator's desire for accessibility through improved interoperability and the need to protect operational information.

Areas of Continuing Research

IDA's analysis confirms that improvements continue to be needed in network defenders' abilities to detect and respond to malicious activity. Improvements can include network sensors, analysis tools, and methodologies for analyzing data.

The DoD has emphasized compliance control measures for monitoring information assurance preparedness. The current measures are necessary but insufficient for predicting performance during exercises. IDA's assessments have helped to identify additional operationally relevant controls, but research is needed to improve and identify measures to better capture those aspects of defensive posture that affect performance.

Increasing operational realism during training exercises by allowing cyber warfare to disrupt operations is needed to understand the potential operational effects of cyber activities. Exercise ground rules have typically prevented such disruptions deemed to potentially distract from training objectives. However, an increasing awareness of the importance of cyber warfare is opening the door for venues that permit cyber attacks to disrupt systems and for retaliatory cyber strikes against the adversary. More research is needed to increase the rigor of information assurance testing to the levels enjoyed by weapon system testing.

Dr. Whetstone is a research staff member in IDA's Operational Evaluation Division. He holds a doctorate in nuclear engineering from the University of Michigan.