Panel Presentation:

How Cyber Ranges are Enabling Effective OT

25 January 2017

Scott M. Lewandowski

Chief Cyber Scientist, National Cyber Range

Current Cyber Testing Infrastructure

- **Three types of cyber testing infrastructure in the DoD:**
  - Computing assets
  - Flexible-purpose cyber ranges
  - Specific-purpose cyber ranges

- **All have significant advantages and disadvantages**

- **It is usually easy to determine which is most appropriate for a given test requirement (e.g., by looking at required environment scale, fidelity, diversity, etc.)**

- **Multiple infrastructure types can be used in concert to improve test quality while decreasing costs**

Flexible-Purpose Cyber Ranges

- **Each range offers different capabilities and services, but as an example, NCR offerings include:**
  - Virtualized computing infrastructure
  - Physical computing infrastructure
  - Virtualized networking infrastructure
  - Physical networking infrastructure
  - Integrated hardware in the loop (HWITL)
  - Traffic generation
  - OPFOR and cyber security evaluation services
  - Data analysis and visualization
  - Interoperable content libraries
  - Test design services
  - Comprehensive results analysis and reporting

Flexible cyber ranges need to provide more than just infrastructure to meet the critical objectives of effective OT!

Virtualization, Hardware in the Loop, and Open-Air Testing

- **Used appropriately, virtualization, real hardware, and emulated links *all* have roles in effective operational tests**
  - There are many misconceptions about the relative merits and drawbacks of these approaches
- **Key observations:**
  - Virtualization is often the operational platform (means virtualization provides high-fidelity, but cannot be used as test infrastructure)
  - Real hardware is not typically required unless the specific behavior of the hardware (e.g., performance, sensor sensitivity, etc.) is relevant to the test or specific hardware changes the relevant portions of the software stack (e.g., drivers, kernel versions, etc.)
  - Open-air testing that allows for wireless physical layers is similarly not usually required unless complicated link characteristics (e.g., atmospheric effects, reflections, signal purity) are relevant to the test or the use of actual wireless connectivity changes the relevant portions of the software stack (e.g., drivers, kernel versions, etc.)
- **Connectivity between ranges via JMN, JIOR, etc. can allow each portion of an environment to be instantiated on the right type of infrastructure and seamless operate as an integrated unit**

DoD Cyber Testing Capabilities Today

- **A good test requires operationally representative systems (including supporting infrastructure), threats, and (often) users**
- **Some domains are fairly well addressed by current capability:**
  - US commercial and government enterprise IT environments
  - Foreign commercial and government enterprise IT environments
- **Other US and foreign systems still pose significant challenges:**
  - Specialized commercial systems (e.g., carrier-grade routing)
  - Industrial control systems (ICS)
  - Wireless assets (especially long-range systems)
  - Specialized military systems
  - “National assets”
  - Complex systems-of-systems
  - Large-scale systems (e.g., nation-scale telecommunications networks)

Rapidly emerging requirements for OT involving complex, costly, and poorly understood systems pose challenges in the coming years

Addressing Challenges Providing Representative Systems

- **Platform (SUT) shortages**
  - Develop sanitization techniques to enable reuse of high-value or unique assets without fear of cross-contamination
- **Configuration issues**
  - Develop strategies to vary systems configurations and tools to implement those changes to test the full scope of reasonable final configurations
- **Environmental/architectural issues**
  - Continue to refine techniques for precisely identifying and emulating interfaces between systems and the other components of the environment
  - Leverage existing range capabilities to replicate the rest of the environment
- **Intelligence gaps**
  - Enhance automated discovery tools for both cooperative and uncooperative network environments
  - Automate import of data from various sources (e.g., open source intel, CM systems, etc.)

Addressing Challenges Providing Threats

- **Shortage of Red/Blue teams that use cyber ranges**
  - Codify past OPFOR campaigns into automated test cases
  - Develop truly robust automated OPFOR capabilities
  - Techniques can be grown to provide automated users
- **Intelligence and enumeration**
  - Develop converters and visualizers to convey configuration information to OPFOR teams
- **Execution issues**
  - Moving tests to cyber range environments greatly minimizes permission and safety issues
  - Using cyber ranges will become possible in more and more cases as cyber range capabilities are enhanced and community confidence in results improves

The Future

- **Cyber range capabilities are growing exponentially, in large part due to a self-perpetuating cycle**
  - Catalogs of reusable content are growing
  - Well-codified, repeatable processes lower the cost of and increase the effectiveness of testing
  - Finite test budgets can be used for refinement of critical test details
  - Confidence in results is growing

- **As programs emphasize cyber testing in their TEMPs, ranges will need to focus more on specialty infrastructure to meet the requirements**
  - These costs will need to be amortized across multiple programs

- **DoD S&T budgets are increasingly being allocated to cyber, which will address some of the key challenges discussed earlier**

- **As capabilities grow, cyber ranges will be appropriate for testing an increased set of systems**