



12th ITEA Test Technology Review

“Back to Basics” Panel

George Rumford

Deputy Director, Technology Development

Program Manager, Test & Evaluation / Science & Technology Program

Test Resource Management Center



Interoperability and Cyber Test Drivers

Shift from Stand Alone to Net Centric Systems Operating in Cyberspace

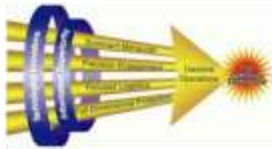


2005
GIG 2.0
Net Centric Enterprise Services

2007
Net Centric Operating Environment

2008
Cyberspace Declared Operating Domain

2012
FLAMES
Cyber War



2000
Joint Vision 2020
GIG 1.0

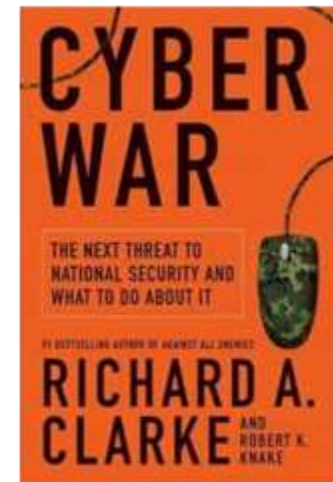
2010
Advanced Persistent Threat Insiders
STUXNET



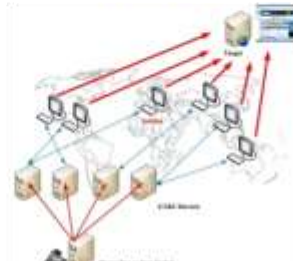
1990
C4I for the Warrior

1996
Joint Vision 2010
GCCS

2005
BOT Nets
Data Leakage Prevention (DLP) Security
Information Management (SIM) Application-Aware Firewalls



2000
Worms
Intrusion Detection Prevention



1990
Viruses
Anti Viruses



Degree of Threat/ Damage to US Forces

Expanding Interoperability Also Results in Increasing the Cyber Attack Surface



The Vision: One Integrated Test Environment

Interoperability Test Vision

Test & Evaluation that accurately and affordably measures mission effectiveness and interoperability of DoD warfighting systems and information systems, to verify the warfighter's capability to achieve mission success while operating in the Joint Operational Environment

Cyber Test Vision

Test & Evaluation that accurately and affordably measures cyberspace effectiveness and vulnerabilities of DoD warfighting systems and information systems, to verify the warfighter's capability to achieve mission success while operating in cyberspace

TRMC Test Infrastructure Vision

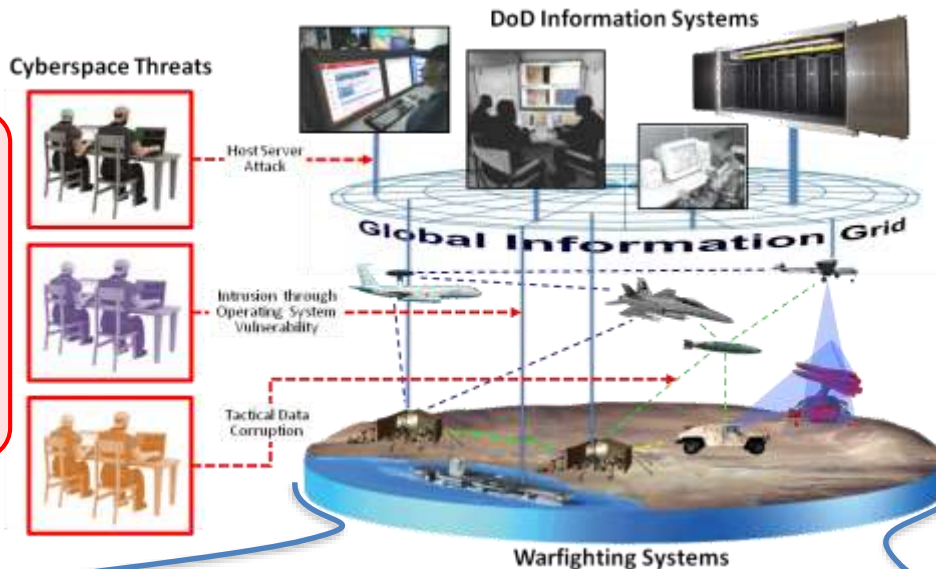
A technically robust, co-located or geographically distributed, access-controlled capability operating over a network architecture capable of supporting multiple mission test environments with integrated LVC capabilities, allowing for mission effects testing, interoperability certification, and cyber vulnerability assessments in an operationally realistic environment



Cyberspace T&E Strategy

Cyberspace T&E Vision

Test & Evaluation that accurately and affordably measures cyberspace effectiveness and vulnerabilities of warfighting systems and DoD information systems, to verify the warfighter's capability to achieve mission success while operating in cyberspace



Four Major Thrusts

1. Cyberspace T&E Policy

- Defined guidance to test cyberspace during the acquisition process

2. Cyberspace T&E Methodology

- Test approach to adequately assess cyberspace capabilities/limitations

3. Cyberspace T&E Workforce

- Training to enable T&E professionals to conduct enhanced cyberspace testing

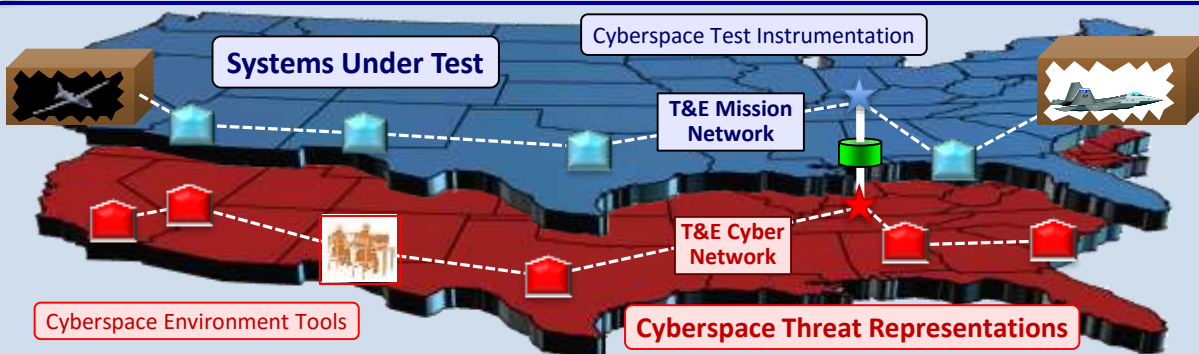
4. Cyberspace T&E Infrastructure

- Existing DoD Labs & Ranges
 - Live system(s) under test
 - Validated threat representations
- Existing DoD Test Networks
 - Continuous (24/7) monitoring
 - Can isolate or "quarantine" systems
- Cross Domain Solutions to bridge across multiple security domains
 - TS/SCI
 - Secret
 - Coalition (NATO, Four Eyes, etc.)
- Common Test Framework with:
 - Cyberspace Environment Tools
 - Cyberspace Test Instrumentation
 - Cyberspace Test Analysis Tools

Cyberspace Attack Effects and Impacts:

- Unauthorized Access
- Unauthorized Use
- Disruption of Ops
- Loss of Control
- Data Corruption
- Data Fabrication
- Target Spoofing

Federated Cyberspace T&E Capability



An integrated T&E enterprise capable of creating a realistic cyberspace test environment at all required security levels, collecting performance & vulnerability test data, and assessing effects



T&E/S&T Program

Cyberspace Test Technology Area



- **Develop advanced technologies and methodologies to test and evaluate DoD capabilities and information networks to defend and conduct full-spectrum military operations across cyberspace**

Current Domain Areas

- 1. Cyberspace Test Planning:** Test technologies to address the unique challenges in designing and planning testing of cyberspace systems
- 2. Cyberspace Test Environments:** Test technologies to improve the representations of cyberspace environments and threats to an adequate degree to support testing
- 3. Cyberspace Test Execution:** Test technologies to address the unique challenges in executing cyberspace tests
- 4. Cyberspace Test Analysis and Evaluation:** Test technologies that address post-test analysis of data, formulating conclusions, and evaluating the quality of those conclusions and the overall test sufficiency, accuracy, and validity

