National Cyber Range Complex (NCRC)

Paul K. Ketrick
NCRC Event Director
pketrick@ida.org

Nov 2018
The TRMC “Blueprint”: Putting Test Capabilities on the DoD Map

Defense Strategic Guidance

Acquisition Process

Service T&E Needs and Solutions Process

Annual T&E Budget Certification

Strategic Plan for DoD T&E Resources

Risk mitigation needs
Technology shortfalls

Risk mitigation solutions
Advanced development

Requirements
Capabilities

Transition

Service Modernization and Improvement Programs
 Acquisition Programs and Advanced Concept Technology Demonstrations
 T&E Multi-Service/Agency Capabilities
 DoD Corporate Distributed Test Capability
 DoD Corporate Cyber Range Capability

TRMC Joint Investment Programs

(6.3 Funding)

(6.4 Activity)

(6.6 Funding)

(6.6 Funding)

DISTRIBUTION A. Approved for public release: distribution unlimited.
What is a “Cyber Range”?

Traditional Open Air Ranges
- Physical Environment
  - Weapon Testing
  - Mission Rehearsal
  - TTP Development

Cyber Ranges
- Virtual Environment
  - Cyber Capabilities Testing
  - Mission Rehearsal
  - TTP Development

The NCRC provides virtualized, high-fidelity representations of cyber-contested environments
Cyber Range Key Capabilities

• **Rapid emulation of complex, operationally representative network environments**
  • Red/Blue/Gray networked environments
  • Operational systems (e.g., weapon, C2, business, etc.)
  • Realistic traffic types, flows, and scale
  • Customized instrumentation

• **Automation provides significant efficiencies that enables high OPTEMPO**
  • Time to deploy environments on the order of hours
  • Minimizes potential for human error and ensures capability to replicate scenarios and phenomena

• **Sanitization to restore all exposed systems to a known, clean state**
  • Allows assets to be reused even when they are exposed to the most malicious and sophisticated uncharacterized code (i.e., “non-destructive” cyber events)

• **Support multiple concurrent tests at varying classification levels**
  • Events, users and data are isolated

• **Secure connectivity**
  • Integration of distributed capabilities (e.g., other cyber ranges, HWIL, SILs, etc.)
  • Remote user access
NCRC Integrated Solution

Distributed Infrastructure

Computing Environment

Tools and Services

Technical Support Team
Customer Defined Level of Support

Testing & Training as a Service
Event design & execution, customized instrumentation & traffic generation, OPFOR, data analysis, reports & briefings,

Platform as a Service (Upper Tier)
Complex network enclaves, enterprise/internet level services, complex networking and routing

Platform as a Service (Lower Tier)
OS, end-point services and applications, simple networking

Secure Infrastructure as a Service
Computing, networking, storage, security architecture

Tailored Services
- Sophisticated services (e.g., anonymization)
- Threat representative environments
- Customized traffic generation
- Customized instrumentation
- Large scale, hi-fidelity, heterogeneous environments

Commodity Services
- Deploy VM images
- Scale testing
- Canonical event design
- Bare metal compute and storage
- Event data storage
- Guaranteed HW performance
- Basic services (e.g., DNS)
Increase in demand signal is only expected to accelerate

As of July 2018

Cyber Events Supported

DISTRIBUTION A. Approved for public release: distribution unlimited.
Typical Use Cases

• **Vulnerability Assessment**
  • How resilient is a System or a Systems-of-Systems (SoS) to a given set of threats?
  • What are the external system dependencies that can impact overall cybersecurity posture?
  • What is the impact to mission effectiveness?

• **Cyber Mission Force (CMF) Training**
  • Create realistic mission tailored, unconstrained environments (at scale) to support training, certification and exercises
  • Provide the most realistic training possible from classroom to force-on-force
  • Enable cyber operators to train from home station

• **Product/Solution Evaluations**
  • Does adding a new product increase or decrease your security posture?
  • How well does the product perform in different scenarios?

• **Architecture Evaluations**
  • Remove lab constraints and evaluate system architectures at scale
Control Systems (ICS)
Typical BMS Control Systems (GAO)
## Event Samples

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Attacks Executed</th>
<th>Attacks Blocked</th>
<th>Technology Evaluated</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>15</td>
<td>4</td>
<td>Solution comprised of appliances and monitoring software that provide protection of OT and IT endpoints through network isolation. The protected devices are continuously monitored and managed.</td>
</tr>
<tr>
<td>2</td>
<td>14</td>
<td>6</td>
<td>Hardened PLC solution comprised of a backplane with pin-less sockets for I/O modules. Communication with no I/O pins enables strong anti-snoop protection while sealed all-metal modules keep cyber predators at bay.</td>
</tr>
<tr>
<td>3</td>
<td>14</td>
<td>6</td>
<td>Power controller solution that allows the end user to monitor, control, automate and optimize their plug-in electronic and electrical devices.</td>
</tr>
<tr>
<td>4</td>
<td>15</td>
<td>9</td>
<td>Agentless and infrastructure vendor agnostic cybersecurity platform that continuously discovers, classifies, assesses, and monitors physical endpoints, IoT and OT devices, and virtual instances connected to a network.</td>
</tr>
<tr>
<td>5</td>
<td>7</td>
<td>1</td>
<td>Solution that detects potential malware by periodically scanning user identified folders in a file system and creates logs of findings for a user to review.</td>
</tr>
<tr>
<td>6</td>
<td>10</td>
<td>7</td>
<td>Stand-alone LED lighting systems with integrated control, occupancy sensing and daylight harvesting. Automated dimming behaviors are activated after installation using a remote control or an Android app to create groups and connect wireless switches.</td>
</tr>
</tbody>
</table>

*It is important to note that the number of attacks blocked does not necessarily indicate the quality of the product. The event analysis document for each evaluation should be reviewed to understand the findings.*
## Example Test Outputs

Every Cybersecurity Evaluation Team Attack will be described in the following format:

<table>
<thead>
<tr>
<th>Description:</th>
<th>Describe test case</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expected Outcome:</td>
<td>Expected outcome of the test</td>
</tr>
<tr>
<td>Attack type:</td>
<td>SYN flood, UDP flood, malformed packets, web, fuzz etc. etc.</td>
</tr>
<tr>
<td>Tools used:</td>
<td>List the tools being used</td>
</tr>
<tr>
<td>Command/Syntax:</td>
<td>Include sample command/syntax used if possible</td>
</tr>
<tr>
<td>Target(s):</td>
<td>List the target to be attacked, ports, protocols etc.</td>
</tr>
<tr>
<td>Attack source(s):</td>
<td>List attacking device source IP/hostname</td>
</tr>
<tr>
<td>Attack time/date:</td>
<td>List date/time attack was launched</td>
</tr>
<tr>
<td>Attack side effect:</td>
<td>List any observed side effects if any, ex. none of FW crashed or froze</td>
</tr>
<tr>
<td>Test result observation:</td>
<td>Ex. an average of 8756 SYN-ACK/sec were received at the attack laptop over the 30 second attack period; NCR plots of traffic shows degradation of all flow performance during time 5s – 40s after which time they recovered.</td>
</tr>
<tr>
<td>Test result rationale:</td>
<td>Ex. the router configuration did not configure rate limiting for SYN packets</td>
</tr>
<tr>
<td>Final Test result</td>
<td>SUCCESS/FAIL/etc.</td>
</tr>
<tr>
<td>Mitigation:</td>
<td>Configure xyz, implement xyz etc. etc...</td>
</tr>
<tr>
<td>Mitigation timeframe:</td>
<td>Immediate, short(30d), mid(60d), long(90d)</td>
</tr>
<tr>
<td>Supporting Data Collected:</td>
<td>List of screenshots, device configurations, packet captures etc.</td>
</tr>
</tbody>
</table>
Several Potential COAs for Future

• COA 1: Continue on the current path
• COA 2: DoD reform/awareness
• COA 3: Training environments
• COA 4: Exercises
• COA 5: More Situational Awareness for Industrial Control Systems (MOSAICS)
• COA 6: Environmental Security Technology Certification Process (ESTCP)
Summary

• The demand for cyber range resources continues to increase
  • The DoD is placing increased emphasis on the need to consistently incorporate realistic cybersecurity testing and training at all levels and phases
  • Early identification of system vulnerabilities can make them easier and cheaper to fix

• NCRC provides customers with a unique set of cybersecurity Test and Training skills and capabilities
  • Enable the acquisition community to conduct system or System-of-Systems (SoS) cybersecurity test and evaluation events that are tailored to meet program requirements throughout the its acquisition lifecycle
  • Enable the training community to conduct realistic cybersecurity training in environments that closely replicate the real world

• NCRC capabilities have successfully supported a wide variety of cyber events including
  • Developmental/Operational/Compliance/Risk Reduction Testing
  • Architecture/Forensic/Malware/Product Assessments
  • Training/Exercise/TTP Development

• NCRC is institutionally funded by the DoD Test Resource Management Center
  • Cyber range users only pay for their own personnel, travel, systems under test, special equipment, etc.
  • Network users only pay for the underlying transport
Primary NCRC
Points of Contact

AJ Pathmanathan
Director, NCRC
arjuna.pathmanathan.civ@mail.mil
571-372-2702

Robert Tamburello
Deputy Director, NCRC
robert.n.tamburello.civ@mail.mil
571-372-2753

Doug Troester
Chief Engineer, NCRC
douglas.c.troester.ctr@mail.mil
703-463-7350

Lizann Messerschmidt
Lead Event Director, NCRC
lizann@mitre.org
571-451-4295
Support Across the Acquisition Lifecycle

NCRC Event
- Cybersecurity Architecture Evaluation
- Cybersecurity Verification and Validation
- Mission Thread Testing with Blue Team
- Mission Thread Testing with Red Team in a Contested Environment
- Large-scale Simulation to Train Cyber Mission Forces and Evaluate Cyber Defensive and Offensive Operations

Pre MS A/B
- Requirements and Systems Security Engineering Analysis
- Evaluate Software and Systems Security Architecture
- Verify Baseline Cybersecurity Requirements and Vulnerability Assessment
- Evaluate Mission Capabilities and Interoperability in a Contested Environment
- Evaluate TTPs in a Contested Environment

SE/DT&E
- Evaluate Software and Systems Security Architecture
- Verify Baseline Cybersecurity Requirements and Vulnerability Assessment
- Evaluate Mission Capabilities and Interoperability in a Contested Environment
- Evaluate TTPs in a Contested Environment

RMF/DT&E
- Verify Baseline Cybersecurity Requirements and Vulnerability Assessment
- Evaluate Mission Capabilities and Interoperability in a Contested Environment
- Evaluate TTPs in a Contested Environment

DT&E/OT&E
- Evaluate Mission Capabilities and Interoperability in a Contested Environment
- Evaluate TTPs in a Contested Environment

Training & Exercises
- Evaluate TTPs in a Contested Environment

POR
- Requirements and Systems Security Engineering Analysis
- Evaluate Software and Systems Security Architecture
- Verify Baseline Cybersecurity Requirements and Vulnerability Assessment
- Evaluate Mission Capabilities and Interoperability in a Contested Environment
- Evaluate TTPs in a Contested Environment

Operations and Sustainment

O&S
JMETC MILS Network (JMN)

- Provides **secure distributed testbeds** to support unconstrained cyber activities at **multiple classifications**
  - Provides users access to NCRC enterprise resources
  - Connect remote facilities and capabilities

- Employs **Multiple Independent Levels of Security** (MILS) architecture
  - Allows for segregation of data streams by protocol, system, event, COI, etc.
    - Capable of supporting multiple simultaneous events at multiple classifications concurrently
    - Ability to create isolated, distributed “sandboxes”
JMETC MILS Network (JMN)

• **Defense Research Engineering Network (DREN) for unclassified transport**
• **JMN NOSC**
  • Manage, optimize and troubleshoot network connectivity
  • Help Desk
  • Provide pre-event checkouts as requested
  • Local infrastructure assistance as requested
  • 10x5 with after hours support as necessary
• **Inter-Site Collaboration**
  • VoIP
  • Chat Server
  • Secure File Transfer Protocol (SFTP) Server

Continue to expand tools & services offered based on user requirements
## Threat Library

<table>
<thead>
<tr>
<th>ID</th>
<th>Attack</th>
<th>Phase/Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Network-based port scan against SUT devices</td>
<td>Recon</td>
</tr>
<tr>
<td>1.2</td>
<td>Bypass detection of port scan against ICS devices</td>
<td>Exploit</td>
</tr>
<tr>
<td>2.1</td>
<td>Whitebox network service inspection against SUT devices</td>
<td>Recon</td>
</tr>
<tr>
<td>3.1</td>
<td>Passive network packet sniffing</td>
<td>Recon and research</td>
</tr>
<tr>
<td>4.1</td>
<td>SUT Protocol analysis – standard use cases</td>
<td>Recon and research</td>
</tr>
<tr>
<td>5.1</td>
<td>SUT Software reconnaissance – determine and replicate capabilities</td>
<td>Recon and research</td>
</tr>
<tr>
<td>6.1</td>
<td>Check SUT for default or hard-coded credentials</td>
<td>Recon and Exploit</td>
</tr>
<tr>
<td>6.2</td>
<td>Check SUT for anonymous access to control interfaces</td>
<td>Recon and Exploit</td>
</tr>
<tr>
<td>6.3</td>
<td>Password Strength Analysis of SUT</td>
<td>Recon and Exploit</td>
</tr>
<tr>
<td>7.1</td>
<td>Identify clear text protocols being transmitted on the wire and determine relevance to attack scenario</td>
<td>Recon and Exploit</td>
</tr>
<tr>
<td>8.1</td>
<td>Common web attacks on SUT-device-hosted web services</td>
<td>Recon and Exploit</td>
</tr>
<tr>
<td>9.1</td>
<td>Perform Man in the Middle attacks to intercept data and/or tamper with data in transit</td>
<td>Exploit</td>
</tr>
<tr>
<td>10.1</td>
<td>ICS protocol data tampering</td>
<td>Research and Exploit</td>
</tr>
<tr>
<td>11.1</td>
<td>Spoof ICS sensor data</td>
<td>Recon and Exploit</td>
</tr>
<tr>
<td>12.1</td>
<td>Spoof ICS controller data</td>
<td>Recon and Exploit</td>
</tr>
<tr>
<td>12.2</td>
<td>Spoof ICS controller identity</td>
<td>Recon and Exploit</td>
</tr>
<tr>
<td>13.1</td>
<td>Denial of Service attack – flood listening service</td>
<td>Exploit</td>
</tr>
<tr>
<td>13.2</td>
<td>Denial of Service attack – flood closed ports</td>
<td>Exploit</td>
</tr>
<tr>
<td>13.3</td>
<td>Denial of Service attack – blacklisting</td>
<td>Exploit</td>
</tr>
<tr>
<td>13.4</td>
<td>Denial of Service attack – WiFi Controller DeAuthentication</td>
<td>Exploit</td>
</tr>
</tbody>
</table>
## Threat Library

<table>
<thead>
<tr>
<th>ID</th>
<th>Attack</th>
<th>Phase/Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.5</td>
<td>Denial of Service attack – Fuzzing SUT Interfaces</td>
<td>Exploit</td>
</tr>
<tr>
<td>14.1</td>
<td>Investigate physical access to SUT via manufacturer ports</td>
<td>Recon and Exploit</td>
</tr>
<tr>
<td>15.1</td>
<td>Investigate physical access to SUT via bus controller</td>
<td>Recon and Exploit</td>
</tr>
<tr>
<td>16.1</td>
<td>Investigate diagnostic mode to bypass authentication or other restrictions</td>
<td>Recon and Exploit</td>
</tr>
<tr>
<td>16.2</td>
<td>Investigate alerts on security configuration changes of the SUT</td>
<td>Recon and Exploit</td>
</tr>
<tr>
<td>17.1</td>
<td>Laterally move and pivot from inside the ICS controlled building environment to the enterprise segment of the network</td>
<td>Exploit/Egress</td>
</tr>
<tr>
<td>17.2</td>
<td>Laterally move across protected ICS segments of the network</td>
<td>Exploit/Egress</td>
</tr>
<tr>
<td>18.1</td>
<td>Perform privilege escalation on the SUT’s command/control application server</td>
<td>Exploit</td>
</tr>
<tr>
<td>18.2</td>
<td>Perform privilege escalation on the SUT’s operator client station</td>
<td>Exploit</td>
</tr>
<tr>
<td>19.1</td>
<td>Perform reconnaissance against ZigBee installation within the environment – standard use case</td>
<td>Recon</td>
</tr>
<tr>
<td>19.2</td>
<td>Perform exploitation against ZigBee installation within the environment – instance specific use case</td>
<td>Exploit</td>
</tr>
<tr>
<td>20.1</td>
<td>Investigate current and/or outdated firmware running on SUT devices for known vulnerabilities and attempt recovery of useful data from firmware</td>
<td>Recon and Exploit</td>
</tr>
<tr>
<td>21.1</td>
<td>Perform attacks leveraging removable media (i.e. USB)</td>
<td>Exploit</td>
</tr>
<tr>
<td>22.1</td>
<td>Scan WiFi network leveraging controller access point capabilities</td>
<td>Recon and Exploit</td>
</tr>
<tr>
<td>23.1</td>
<td>Rogue WiFi Access Point Attack</td>
<td>Recon and Exploit</td>
</tr>
<tr>
<td>24.1</td>
<td>Physical device review</td>
<td>Recon - Physical Exploit</td>
</tr>
<tr>
<td>25.1</td>
<td>Investigate attacks from quarantine against security appliance</td>
<td>Recon and Exploit</td>
</tr>
</tbody>
</table>