Gaining Cyber Dominance

Software Engineering Institute
Carnegie Mellon University

NETCOM G3/5/7 TREX

January 2015
**1. REPORT DATE**  
15 JAN 2015

**2. REPORT TYPE**  
N/A

**3. DATES COVERED**

**4. TITLE AND SUBTITLE**  
Gaining Cyber Dominance

**5a. CONTRACT NUMBER**

**5b. GRANT NUMBER**

**5c. PROGRAM ELEMENT NUMBER**

**5d. PROJECT NUMBER**

**5e. TASK NUMBER**

**5f. WORK UNIT NUMBER**

**6. AUTHOR(S)**  
Longo / Gregory

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**  
Software Engineering Institute  
Carnegie Mellon University  
Pittsburgh, PA 15213

**8. PERFORMING ORGANIZATION REPORT NUMBER**

**9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**

**10. SPONSOR/MONITOR’S ACRONYM(S)**

**11. SPONSOR/MONITOR’S REPORT NUMBER(S)**

**12. DISTRIBUTION/AVAILABILITY STATEMENT**  
Approved for public release, distribution unlimited.

**13. SUPPLEMENTARY NOTES**  
The original document contains color images.

**14. ABSTRACT**

**15. SUBJECT TERMS**

**16. SECURITY CLASSIFICATION OF:**

<table>
<thead>
<tr>
<th>a. REPORT</th>
<th>b. ABSTRACT</th>
<th>c. THIS PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>unclassified</td>
<td>unclassified</td>
<td>unclassified</td>
</tr>
</tbody>
</table>

**17. LIMITATION OF ABSTRACT**  
SAR

**18. NUMBER OF PAGES**  
29

**19a. NAME OF RESPONSIBLE PERSON**
Cyber Force Development Challenges

Customizable and scalable training solutions for globally dispersed cyber operations forces

Establishment of CMF collective training program

“Our highest priority is developing and managing individual, collective, and sustainment training for our cyber mission forces.” CG, ARCYBER (2014)


FY15 Initiatives

Gaining Cyber Dominance Program

- Army topology development
- PCTC infrastructure refresh
- RCC training and exercises (unclassified)
- CPT training and exercises (unclassified/classified)

Classified training environment

- STEP infrastructure on JIOR
GCD Program Overview

- Improve Individual Operator Skills
- Improve RCC/CPT Team Skills
- Establish integration of RCC/ADOC/JFHQ-C/CPT
- Provide input to RCC of the Year Award

The Team!

END STATE:
Cyber training and exercise program that provides hands on training for RCCs and CMF teams to exercise and refine operational TTPs and mission command including alignment with joint training standards and the ability to evaluate mission ready status of forces.
CMF Training Approach

Gaining Cyber Dominance

US Army Regional Cyber Centers
Theater Signal Command

Individual Training (FedVTE)
Unit Lead Collective Training Sandbox
Facilitated Collective Exercises
ELITE MERCURY Culminating Training Exercise

CMF Training

ARCYBER CPT CONOPS
USCC CPT CONOPS
USCC CMF T&R Manual
USCC CFCOE
Program Objectives

1. Offer challenging training opportunities tailored to meet the needs of the RCCs and CPTs
2. Enlarge the RCC training audience to include the RCC director - exercising Mission Command
3. Build an enlarged/more complex virtual environment with a continued focus on realism
4. Within CPTs, focus on squads first, teams second
5. Work with NETCOM/ARCYBER/USCC leadership to prioritize effort to establish JIOR nodes in each RCC and the ADOC
6. Enhance program flexibility where possible in order to adjust vignettes based on RCC standardization decisions, doctrine and TTP development, force structure modifications, and short notice collective training preparation (ex. Pre-Cyber Guard train-up)
7. Build on relationship with 1st IO command that was initiated during GCD 14
Training Themes

Experience with new operational capabilities
Validation of existing TTPs/SOPs
Development of new TTPs/SOPs
Incident reporting
RCC/CPT/ADOC interaction
CPT squad operations
Exposure to emerging threats
Deployment/Exercise prep
GCD 15 Training Objectives

Demonstrate the ability to detect, respond to, and recover from a cyber attack
Support the intelligence cycle by performing cyber threat/event analysis
Develop procedures to coordinate with JFHQ-C during RCC and CPT operations
Demonstrate the ability to engage RCC leadership and perform critical decision making during cyber-kinetic operations
Assess emerging doctrine ISO RCC and CPT mission integration during operations
Demonstrate the ability to perform CPT squad level 3000 tasks
USCC T&R Manual

CPT identifies & protects assets critical to mission accomplishment
CPT defends Cyber Key Terrain & critical assets in larger/overlapping areas of operation
Operates across Service controlled terrain; Protects Service & CCDRs’ priorities ISO operational needs

“USCYBERCOM and CMF leaders and staffs shall use the CMF T&R Manual to develop their training and assessment plans for individual, staff, and collective levels. They will ensure that CMF exercise events incorporate CMF T&R Manual standards for assessment team readiness to perform our mission.” – ADM Rogers
CPT Training Resources

Individual skill building

• FedVTE/PCTC courses -- lectures, demonstrations, labs

Collective experience building

• Scenario vignette library focusing on squad operations
• Facilitated exercises
Vignette Library

CPT Operations

- Prepare Phase
- Execution Phase
  - Survey
  - Secure
  - Protect
  - Recover

Squads

- Mission Protect
- Cyber Readiness
- Cyber Support
- Discovery & Counter-Infiltration
- Cyber Threat Emulation
## Training Battle Rhythm

### RCC

<table>
<thead>
<tr>
<th>Month</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>December – February</td>
<td>TEXN Build (CMU-SEI)</td>
</tr>
<tr>
<td>March</td>
<td>Cyber Sandbox 1 (24x7)</td>
</tr>
<tr>
<td>April</td>
<td>Mercury Challenge 1 (4hr)</td>
</tr>
<tr>
<td>May</td>
<td>Cyber Sandbox 2 (24x7)</td>
</tr>
<tr>
<td>June</td>
<td>Mercury Challenge 2 (4hr)</td>
</tr>
<tr>
<td>July</td>
<td>Cyber Sandbox 3 (24x7)</td>
</tr>
<tr>
<td>August</td>
<td>Mercury Challenge 3 (4hr)</td>
</tr>
<tr>
<td>September</td>
<td>Elite Mercury CTE (8hr)</td>
</tr>
</tbody>
</table>

### CPT

<table>
<thead>
<tr>
<th>Month</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>December – February</td>
<td>TEXN Build (CMU-SEI)</td>
</tr>
<tr>
<td>March</td>
<td>RCC Configuration</td>
</tr>
<tr>
<td>April</td>
<td>PTE Go-Live</td>
</tr>
<tr>
<td>May</td>
<td>CPT Exercise 1 (4hr)</td>
</tr>
<tr>
<td>June</td>
<td>Squad Vignette Training</td>
</tr>
<tr>
<td>July</td>
<td>CPT Exercise 2 (4hr)</td>
</tr>
<tr>
<td>August</td>
<td>Squad Vignette Training</td>
</tr>
<tr>
<td>September</td>
<td>Squad Vignette Training</td>
</tr>
</tbody>
</table>
Training Partnership

Event Design

• RCC/CPT trusted agent
• Design review

Assessment Strategies

• Embedded Observers
• Training Coordinators
• Hotwash/Shot Validation
• White Cell
Virtual Training Environments

**Training enabler** - Focus on providing the capability for units to conduct small team collective training while addressing time and scale.

Environments based on training objectives
- Unclassified (NIPR)
- Classified (JIOR)

Platform and environment as a managed service
- Rapid prototyping based on training requirements (e.g. integrated JQR training database)
CERT ® Private Cyber Training Cloud

Intuitive Learning Management System
Thousands of hours of captured training
  • Lectures, Demos, Hands-on Labs
Robust team exercise and simulation
  • Air-gapped; isolation from production networks
  • “Train as you fight” scenarios
  • Advanced user and Internet Simulation
Training & Exercise Network (TEXN)

Build the most realistic representation of an Army enterprise yet for multi-mission element training

Incorporate Joint Regional Security Stack (JRSS) systems

Current design based on inputs from RCC

• Many enterprise variations in the real world meant a single environment could not represent every region

CPT Capability Integration

• Security Onion
• SIFT (Linux/Windows)
• Kali
• Rucksack
• Docker
• VTS
TEXN Architecture
Training Collaboration

NETCOM
• Integration of RCC, CPT, ADOC, and 1st IO

Cyber Protection Brigade
• Individual training proficiency tracking (JQR)
• CPT training requirements

Cyber Center of Excellence
• Training advancements for emerging missions
• TTP/SOP development and codification

CECOM
• Army cyber range working group

ARCYBER JFQH-C
• Training coordination
• CMF training alignment
Curriculum Development

Leverage PCTC beyond the exercise portal
Custom course development integrating LMS features, courses, and labs
Integration of Army training content
QUESTIONS
Contact Information

Bruce Madalinski, NETCOM G3/5/7 TREX
bruce.a.madalinski.civ@mail.mil
520-538-8439

Greg Longo, CMU/SEI
ggl@cert.org
412-268-8330
CWDi Approach to Training

- Knowledge Building: *lectures and demos*
- Skill building: *hands-on labs*
- Experience building: *team-based exercises*
- Evaluation
**ART 5.9.1.2 Conduct Defensive Cyberspace Operations**

Units conduct and coordinate, as required, defensive cyberspace operations to effectively detect, identify, and respond to enemy and adversary actions against friendly networks and information resident in these networks. (FM 3-38) (USAMCCoE)

<table>
<thead>
<tr>
<th>No.</th>
<th>Scale</th>
<th>Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>Yes/No</td>
<td>Unit employed tactics, techniques, and procedures to detect intrusions and cyber attacks into the Army’s portion of the Department of Defense information networks called LandWarNet.</td>
</tr>
<tr>
<td>02</td>
<td>Yes/No</td>
<td>Unit coordinated, deconflicted, and conducted defensive cyberspace operation response actions outside the LandWarNet.</td>
</tr>
<tr>
<td>03</td>
<td>Yes/No</td>
<td>Unit coordinated, deconflicted, and employed internal defensive measures inside the LandWarNet.</td>
</tr>
<tr>
<td>04</td>
<td>Yes/No</td>
<td>Unit conducted rehearsals to react to enemy cyber attacks on friendly networks and per operation order, battle drills, and standard operating procedures.</td>
</tr>
<tr>
<td>05</td>
<td>Yes/No</td>
<td>Unit coordinated and conducted cyberspace information collection to support defensive cyberspace operations.</td>
</tr>
<tr>
<td>06</td>
<td>Yes/No</td>
<td>Unit developed and submitted cyber effects request formats as required in support of defensive cyberspace operations.</td>
</tr>
</tbody>
</table>

**Condition**

- Using network resources while under cyber attack
- Operate through degraded network conditions
AUTL

ART 5.9.1.3 COORDINATE NETWORK OPERATIONS

Units that perform this task coordinate, integrate, and synchronize network operations within Department of Defense information networks and the LandWarNet to support cyberspace operations. (FM 3-38) (USAMCCoE)

<table>
<thead>
<tr>
<th>No.</th>
<th>Scale</th>
<th>Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>Yes/No</td>
<td>Unit enabled and facilitated cyberspace operations inside friendly force networks.</td>
</tr>
<tr>
<td>02</td>
<td>Yes/No</td>
<td>Unit enabled and facilitated cyberspace operations outside friendly force networks.</td>
</tr>
<tr>
<td>03</td>
<td>Yes/No</td>
<td>Unit enforced cyber electromagnetic policies and standards that guided the development, deployment, and management of personnel, products, and processes.</td>
</tr>
</tbody>
</table>

**CONDITION**

- Using network resources while under cyber attack
- Operate through degraded network conditions
ART 5.9.1.4 CONDUCT CYBERSPACE SUPPORT

Units conduct cyberspace support actions to enable cyberspace operations and the accomplishment of the mission. (FM 3-38) (USAMCCoE)

<table>
<thead>
<tr>
<th>No.</th>
<th>Scale</th>
<th>Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>Yes/No</td>
<td>Unit performed development, engineering, and analysis to enable the enterprise network.</td>
</tr>
<tr>
<td>02</td>
<td>Yes/No</td>
<td>Unit conducted legal, regulatory, and policy analysis and coordination.</td>
</tr>
<tr>
<td>03</td>
<td>Yes/No</td>
<td>Unit performed vulnerability assessments.</td>
</tr>
<tr>
<td>04</td>
<td>Yes/No</td>
<td>Unit performed forensics.</td>
</tr>
<tr>
<td>05</td>
<td>Yes/No</td>
<td>Unit performed remediation in response to unauthorized intrusions or attacks.</td>
</tr>
</tbody>
</table>

**CONDITION**

- Using network resources while under cyber attack
- Operate through degraded network conditions
ART 5.9.1.5 DEVELOP CYBERSPACE SITUATIONAL AWARENESS

Units develop and provide cyberspace situational awareness to gather, process, and communicate relevant information to enable cyberspace operations. (FM 3-38) (USAMCCoE)

<table>
<thead>
<tr>
<th>No.</th>
<th>Scale</th>
<th>Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>Yes/No</td>
<td>Unit developed, disseminated, and maintained relevant information enabling the commander and staff to achieve situational understanding of friendly and adversary use of cyberspace.</td>
</tr>
<tr>
<td>02</td>
<td>Yes/No</td>
<td>Unit conducted cyberspace information collection contributing to the common operational picture and answering the commander’s critical information requirements.</td>
</tr>
<tr>
<td>03</td>
<td>Yes/No</td>
<td>Unit coordinated with host nation to develop situational awareness of critical infrastructure and key resources.</td>
</tr>
<tr>
<td>04</td>
<td>Yes/No</td>
<td>Unit identified and applied the legal considerations, intelligence gains or losses, and associated risks supporting the commander’s decisions within the operations process.</td>
</tr>
</tbody>
</table>

**CONDITION**
- Using network resources while under cyber attack
- Operate through degraded network conditions
Joint Training Manual (CJCSM 3500.03D)

**Joint Learning Continuum**

- **Learning**
  - Education
  - Individual Training
  - Self Development
  - Experience

- **Performing**
  - Certification
  - Execution

**Integrated and disciplined preparation to defined performance standards**

- **Indoctrination**
- **Qualification**
- **Validation**

**Time**

- Joint Duty
- Mission Ready
- Joint Operations