Applying Cybersecurity OT Lessons to Achieve Greater Cybersecurity of Future Defense Capabilities

Mr. Ryan Mayer
COMOPTEVFOR
Cybersecurity Test Design
March 2, 2016

Agenda

- Cybersecurity OT Observations
- Collaboration Opportunities
- Focusing DT Efforts
- Value of DT/OT Alignment
- Other Stakeholder Engagement
- Questions

Cybersecurity OT Observations

CS Domain

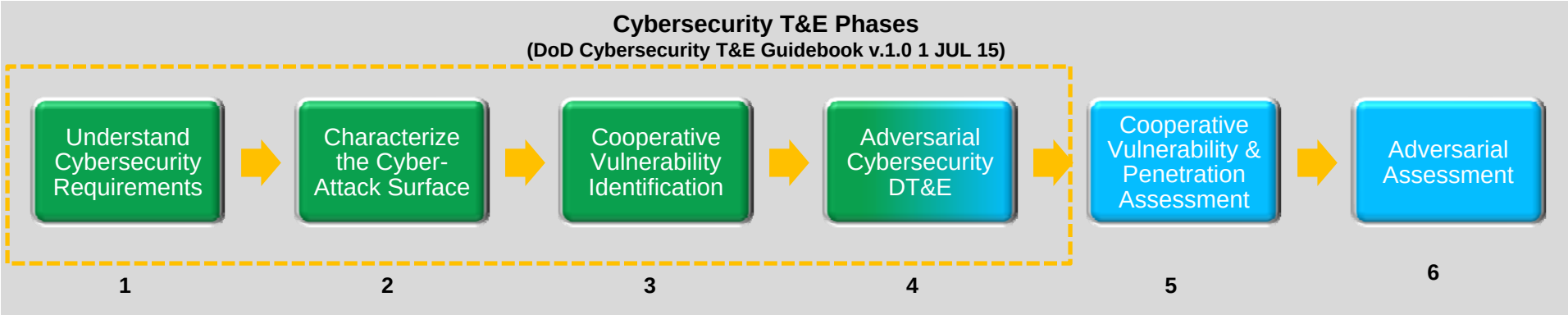
- Evolving/Dynamic
- DoD wide attention
  - Task Force Cyber Awakening
  - Cyber KPP efforts
  - Numerous new processes, instructions, guides
- Requirements documents
  - Vague or silent until recently
  - Rely upon Certification and Accreditation (C&A) process
  - ATO ≠ Cybersecure

CS OT Themes

- Results of CS OT shows significant discovery
  - Inexpensive but proven discovery tools discover a lot
- Common cyber-vulnerabilities
  - Authentication, password use and strength
  - Access control
  - Patch management
  - Outdated services, connections, OS
- Compliance matters
  - Serious mission effects likely stem from lack of compliance

DT is critical, collaboration a must

Collaboration Opportunities



- First 4 steps vital
  - Goal: Step 5 has minimal discovery
- Develop standard procedures, tools, and data requirements to carry into OT
  - Help fill resource gaps and mitigate test limitations
  - Better scoping of OT execution for TEMP inputs

Focusing DT Efforts

- DT should be more than C&A validation
  - Be adversarial against your own system
- Test, Analyze, Fix, Re-Test
  - Helps decrease attack surface
  - Helps build threat portrayal
  - Start small, end big
- Understand the OT methodology
  - Test differently, catch more deficiencies

Value of DT/OT Alignment

- Identify & remediate vulnerabilities prior to IOT&E
  - Cost less to fix vulnerabilities in DT vs OT
  - Reduces cyber-risks prior to Fleet release
- Effective use of available test resources
  - Reduce redundant testing through mutual data collection
  - Share limited experienced penetration testers
  - Share system subject matter experts
  - Share test tactics, techniques and procedures
- Supports PMO delivering cybersecure POR to the Fleet

Shift “Cyber-Discovery” to the Left

Other Stakeholder Engagement

- Stakeholders other than Program Office & OTA
  - SYSCOM, CND providers, engineering agents, PARMs
- Additional cybersecurity OT resources
  - NAVSEA “re-certification” process
- Post OT efforts can cause increase in resources
  - System restore
  - Operational verification post-restore
- Engage early, engage often
  - Manages expectations
  - Commanding Officers more at ease with OT

Questions

QUESTIONS?

Acronyms

- ATO: Authority To Operate
- C&A: certification and accreditation
- CND: Computer Network Defense
- CS: Cybersecurity
- DT: Developmental Testing
- IOT&E: Initial Operational Test & Evaluation
- KPP: Key Performance Parameter
- NAVSEA: Naval Sea Systems Command
- OS: Operating System
- OT: Operational Testing
- OTA: Operational Test Agency
- PARM: Program Acquisition Resource Manager

Acronyms (cont.)

- PIT: Platform Information IT
- PMO: Program Management Office
- POR: Program of Record
- PRA: PIT Risk Assessment
- SYSCOM: Systems Command
- TEMP: Test and Evaluation Master Plan