



OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

NOV 15 2013

MEMORANDUM FOR CHIEFS OF THE MILITARY SERVICES
COMMANDERS OF THE COMBATANT COMMANDS

SUBJECT: Improving Department of Defense (DoD) Training and Operational Assessments of Cybersecurity

The DoD relies on a defense-in-depth approach for cybersecurity support to operational missions and tasks. The tasks required to protect systems, detect adversarial activity, and respond to threats in an effective manner are executed by organizations across all three tiers of the DoD Computer Network Defense (CND) hierarchy, with Tier 2 and Tier 1 CND Service Providers (CNDSPs) performing the majority of the detect and respond functions. Therefore, the ability to effectively "train as we fight" depends on the active participation of all three tiers during exercises.

During Congressionally-directed cybersecurity assessments conducted during exercises over the last two to three years, we have seen decreasing participation by Tier 2 CNDSPs and minimal participation by the Tier 1 (national level) CNDSPs. Only one of all the exercises in Fiscal Year 2013 included significant CNDSP participation, and most exercises over the last two years had limited or very constrained CNDSP involvement as participation was routinely limited to only local network personnel. The attached depiction of CND actions summarizes our analysis which shows that exempting these CNDSP tiers from performing their normal CND functions during major exercises results in unrealistic training and an incomplete assessment of DoD's CND capability. As discussed in our last two annual reports to Congress, the Department is missing valuable opportunities to develop and assess the necessary skills, tactics and processes to execute effective CND at all levels.

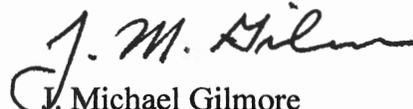
Improving participation of all tiers of CND during exercises is essential to provide realistic and consistent training necessary to develop operational and cyber responses to cyber adversaries and to assess the cybersecurity capability supporting operational forces and missions. I request your support in two specific areas to improve that participation:

1. Require that exercises include as a training objective the defense of all networks, systems, and data necessary to conduct key missions in the face of an aggressive cyber adversary, specifically exercising all tiers of network defense-in-depth. We also need to adjust exercise training objectives, Red Team ground rules, and the scope of exercise training events to properly reflect the new distribution of CND roles across the various Tiers
2. Formally request exercise participation and support from the key Tier 2 and Tier 1 CND activities (including CNDSPs for both headquarters and Services) via the Joint Training Information Management System. A formal request will allow



validation by the Joint Staff and subsequent sourcing by the appropriate force providers for key exercise participants, ensuring the necessary demonstration and development of CND skills critical to executing warfighting missions.

I consider this effort of vital importance and look forward to partnering with you to enhance training and assessments with realistic participation of DoD cyber warfighting capabilities in an operationally realistic, contested cyber environment. My point of contact is Mr. Dave Aland, who may be reached at 571-372-3882 or david.j.aland.civ@mail.mil.


J. Michael Gilmore
Director

Attachment:
As stated

cc:
CJCS
DoD(CIO)
Commander, USCYBERCOM
Director, NSA
Director, DISA



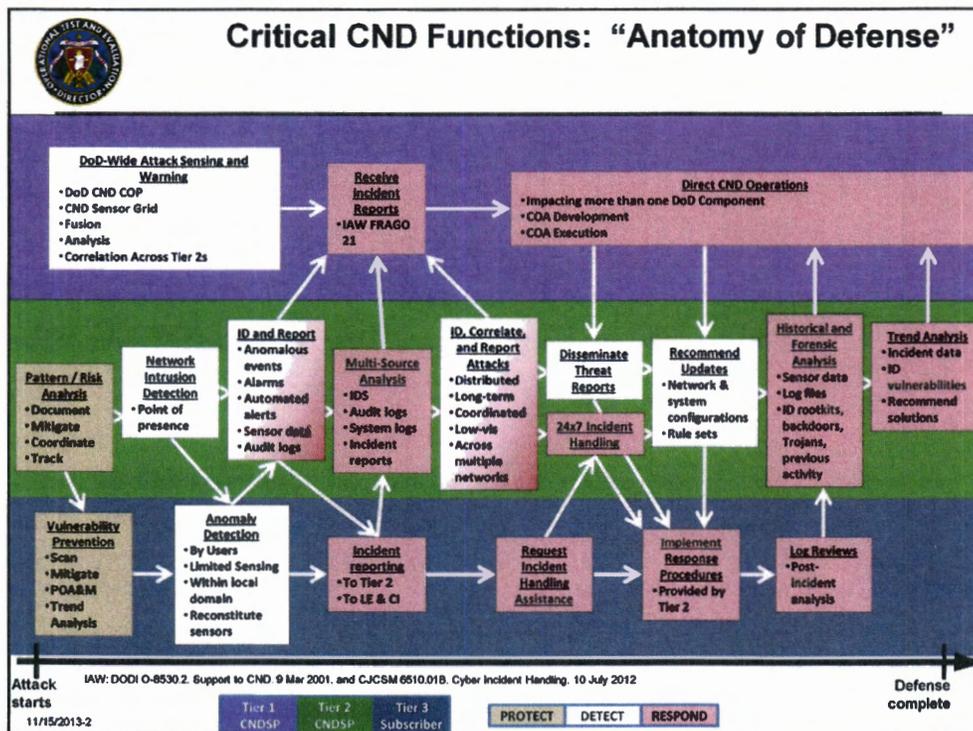
Background

- **DOT&E conducts Information Assurance and Interoperability assessments during Combatant Command and Service exercises, as directed by Congress in 2002.**
- **Exercise objectives and ground rules govern the scope and nature of cyberspace exercise events, including**
 - Impact of training events
 - Cyber Red Team actions and limits
 - Computer Network Defense Service Providers (CNDSPs) participation
- **Assessment teams have observed a trend towards decreasing participation by Tier 2 CNDSPs in exercises despite the continuing consolidation of CND responsibilities at that level**
- **DOT&E has reviewed the impact of decreased upper tier CND participation**
 - Reviewed current distribution of network defense responsibilities
 - Determined implications to assessments from decreasing CNDSP participation
 - Identified actions to attain needed levels of participation

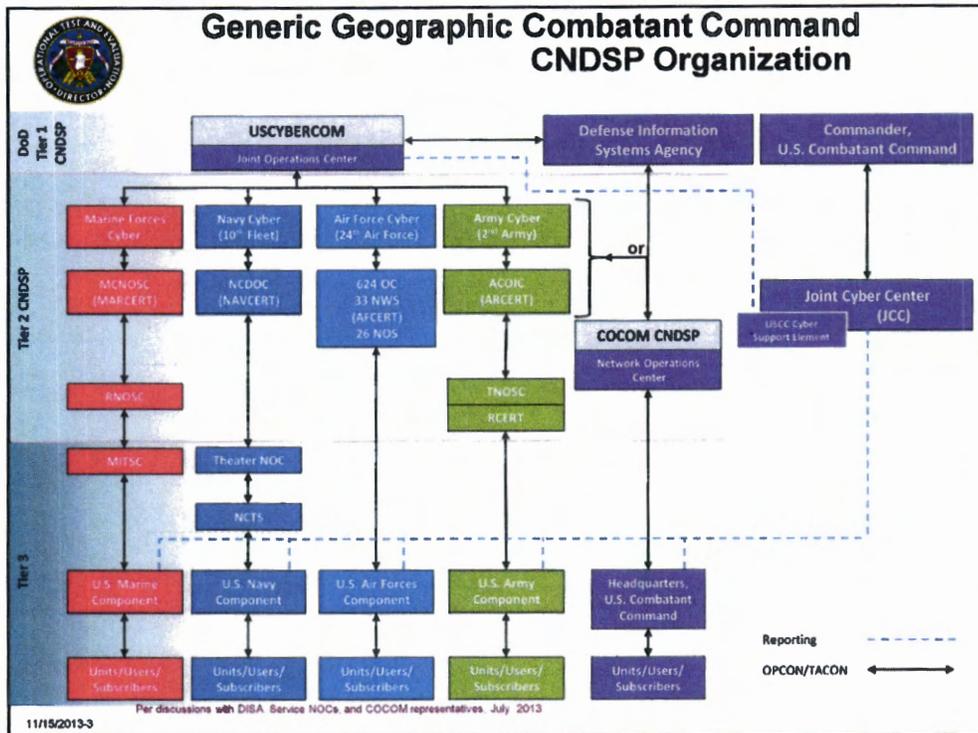
11/15/2013-1

In the course of the Congressionally-mandated Information Assurance and Interoperability assessments, exercise assessors from the Service Operational Test Agencies have noted an increasing trend towards decreasing participation by upper tier CND organizations. For years, during major exercises supporting both Services and Combatant Commanders, the exercise cyber training audience has been limited to local network personnel. In the last 2-3 years, however, a large share of cyber defense responsibilities have been consolidated at the Tier 2 and even Tier 1 CND Service Providers – yet the exercise training objectives, Red Team ground rules, and scope of exercise training events have not been adjusted to reflect this redistribution of CND roles. As a result, the scope of CND training (as well as assessments of performance) has narrowed, and no longer includes key actors and capabilities.

DOT&E undertook a brief study to understand what elements of CND were not being adequately assessed during exercise events. This required an in-depth review of DoD and Service documentation pertaining to CND and CND Service Providers, visits with DISA, the Services, and several Combatant Commands. At the same time, an ongoing Joint Test and Evaluation effort sponsored by DOT&E has been reviewing CNDSP performance metrics. Based on this information, DOT&E reviewed the varying levels of CND responsibility now practiced at all three tiers of the CNDSP model as well as the lost opportunities for training and performance assessment resulting from limited participation by key players.



- This diagram is illustrative and consolidated/simplified – and is not inclusive of all functions and relationships. The distribution of these functions varies to some degree from Service to Service. The figure shows the three tiers of network defense in ascending order (blue = Tier 3; green = Tier 2, purple = Tier 1)
- Without Tier 2 and Tier 1 participation, the training and assessment events lose visibility to the assigned functional responsibilities “above the line” as well as the interactions, UPWARDS (reporting) and DOWNWARDS (notification, direction for response).
 - Note: Some of the responsibilities may have been partially shared to Tier 3 units, so some of this may be present in some exercises, but not uniformly.
- In general, DOT&E has observed minimal Tier 2 participation over the past two years while the Tier 2 responsibilities have continued to grow/expand.
 - As a result, DOT&E has not been able to accurately assess Tier 2 participation and effectiveness because of lack of data.



- A Combatant Command typically receives support from all four Service Tier 2 CNDSPs.
- A Combatant Command also receives support for its Headquarters separately.
 - Support could be provided by one of the four Service CNDSPs, or from a fifth (i.e., DISA).
- The JCC does not have OPCON or TACON of any of the CNDSPs, and reporting of cyber incidents to the JCC has been observed by OTAs in several exercises to be inconsistent.
- As a result, an exercise assessment at a Combatant Command HQ may now only encompass a limited scope of Tier 3 responsibilities carried out by the immediate CCMD staff and does not exercise or permit assessment of the full range of cyber defense activities.



CNDSP Participation Needed In Cyber Exercise Assessments

- **Tier 2 CNDSPs are responsible for the majority of Detect and Respond (React) functions**
 - Includes detection at the asset level (i.e., Host-Based Security System)
 - Tier 3 functionality typically limited to reporting observed anomalous behavior
 - Allocation of responsibilities between Tier 2 and Tier 3 varies across Services
- **Assessment of Cyberspace Defense-in-Depth requires end-to-end incident handling**
 - Detection, Reporting, Analysis/Forensics, Response Actions, Dissemination of Intelligence and Orders
 - Reporting between Tier 3, Tier 2, and Tier 1
 - Across the full range of emulated attacks, target systems and networks, and cyber effects
- **Characterization of Cyberspace Defense performance is required to understand the risk to operational warfighting missions**
 - Fundamentally different criteria than DISA-conducted Tier 2 Certification and Accreditation inspections,
 - Ability to support execution of dynamic, phased missions in a degraded, manipulated, or contested cyber environment throughout the duration of an exercise

11/15/2013-4

To improve training as well as assessment of capabilities, the level of participation should be improved. All tiers involved in cybersecurity and CND should participate so that the full range of activities can be both exercised and evaluated for effectiveness -- defense-in-depth should ideally be practiced end-to-end to ensure realism. Although there are differences in how the Service allocate responsibilities, it is clear that the organizations that have the most to do with cyber defense are the least often represented in training events and assessments for the Combatant Commanders.