

March 11, 2009

Abstract for Consideration: Conference on Cyber Warfare - June 17-19, 2009

# Cyber Command and Control: A Current Concept for Future Doctrine

Submitted By:

Michael E. Ruiz  
BearingPoint, Inc.  
1676 International Dr.  
McLean, VA 22102 USA





## Abstract

Cyber Initiatives are best described in a continuum of solutions that range from Cyber Security to Cyber Operations. Additionally, Cyber Initiatives must be considered in the context of its supporting cyber domain. These cyber domains include Cyber Warfare, Cyber Homeland Security, and Cyber Law Enforcement. The specific instantiation of these solutions are dependent the underlying cyber domain.

This paper describes a concept for defining command and control, within a Cyber Warfare domain. The concept includes the basis for future doctrine, a definition for a proof of concept, and an implementation pattern for future cyber command and control systems. While this paper focuses on the domain of Cyber Warfare, many of the underlying constructs apply broadly across all cyber domains.

The DoD Dictionary of Military and Associated Terms defines Command and Control (C2) as “the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission...” This definition provides a general model for C2; however the C2 functional domain is a significantly richer body of knowledge that includes Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities (DOTMLPF) for operational domains (i.e. Air Operations, Ground Operation, etc). Integrating Cyber Warfare as an operational domain into the broader C2 functional domain is the key challenge addressed in this paper. This paper focuses on the following components of DOTMLPF.

- Doctrine –addresses the much needed Tactics, Techniques and Procedures (TTPs) for operating in a cyber realm.
- Organization – defines the organizational structures needed to successfully implement a cyber warfare organization, specifically the work BearingPoint is doing for the Army G2 for cyber operations.
- Materiel – describes a reference model / implementation pattern for implementing future cyber command and control systems.
- Facilities – illustrates the types of facilities (i.e. Network Operation Centers, Security Operation Centers, and Cyber Space Operation Centers) and the processes for federating across agency / organizational boundaries.

Additionally, the implementation pattern described in this paper depicts an open architecture / open standards approach to integrating existing network and security resource in order to ensure interoperability and collaboration. This implementation pattern focuses on the following:

- Cyber Situation Awareness – COP and UDOP
- Cyber Incident Detection and Response
- Cyber Collaboration incorporating Web 2.0 and Web 3.0 technology

1676 International Drive  
McLean, VA 22102-4828

T (703) 747-3000  
F (703) 747-8500  
[www.bearingpoint.com](http://www.bearingpoint.com)



## About the Author

Michael Ruiz is a Chief Technical Officer(CTO) for Net Enabled Operational Support (NEOS) group within BearingPoint's DoD segment. Mr. Ruiz aligns BearingPoint's global solution offerings in order to enable DoD and IC mission-related solutions. He leads several internal research and development projects geared towards Information Sharing, Enterprise Governance, and Cyber-Operations.

Mr. Ruiz has more than twenty years of IT experience spanning the U.S. military, private industry, and academia. Mr. Ruiz is a founding member of the OASIS Technical Committee for the SOA Reference Model, and he is a regular speaker at the Open Group Real-Time SOA Forum and SOA Forum, as well as a guest speaker at numerous industry conferences.