# Chapter 43
# Cyber Command and Control: A Military Doctrinal Perspective on Collaborative Situation Awareness for Decision Making

**Michael E. Ruiz**
*Deloitte Consulting, USA*

**Richard Redmond**
*Virginia Commonwealth University, USA*

## ABSTRACT

*Cyber-space is emerging as the fifth domain of warfare and a crucial operational concern for commercial industry. As such, it requires a command and control system that enables defensive and operational capabilities within cyber-space. This chapter describes a research and development project aimed at discovering solutions for a Cyber Command and Control both for commercial and military environments. The chapter identifies challenges and provides solutions rooted in the body of knowledge composed of Command and Control and Situation Awareness Theory.*

## INTRODUCTION

Cyberspace is officially the fifth domain of warfare. On June 23, 2009, US Secretary of Defense, Robert Gates, in a memorandum to the Joint Chiefs of Staff and Military Service leadership, established the US Cyber Command (USCYBERCOM) (Jackson, 2009). This came as no surprise to those in the US military industrial complex, because the Air Force and the other military services were all competing for leadership of this new mission area (Clarke & Knake, 2010). The Gates Memo, for the first time, positioned cyber as the fifth domain of warfare along side of Air, Land, Maritime, and Space; giving the US military the authority and the duty to conduct defensive and offensive missions in cyberspace (Fry, 2010; Jackson, 2009; Staff Writer, 2010). Like the other four domains, cyber requires a command and control system that is able to integrate with existing command and control systems in an operational environment, while providing supporting capability to those operating in cyber space.

DOI: 10.4018/978-1-4666-5942-1.ch043

Prior to the official announcement many firms in the military industrial complex actively conducted research in this emerging domain. BearingPoint Public Service (now Deloitte Federal Services), performed research and development in the information sharing domain dating back to mid-2007; applying their efforts to the maritime domain awareness (MDA) problem. In mid-2008, the research team decided that the solutions created for MDA could be applied to the Cyber Command and Control (Cyber C2) problem.

In the early stages of this research it was important to understand how security operation centers (SOC) were conducting business. Visits to several security operations centers revealed similar results to those articulated in Visualizing Cyber Security: Usable Workspaces (Fink, North, Endert, & Rose, 2009). Many of the cyber analysts working in the SOC were former systems administrators, network engineers, and hardware technicians. The analysts' comfort with hands-on operations of the physical system coupled with their years of experience in dealing with systems at the system console level, created an environment where only a minimum set of automation and analytical tools existed. The sheer volume of information that the analysts were processing on any given day was of particular interest. It was on the order of three million alerts indicating possible threats every day.

This chapter articulates the outcomes associated with the Cyber C2 R&D effort and the lessons learned from that research endeavor. In order to provide the most complete analysis the chapter starts with the theoretical underpinning of command and control, as well as situation awareness. The chapter then progresses into a description of the technical solution and aligns that solution with its theoretical foundation.

## BACKGROUND

### The Challenge

Command and Control Systems today, have a limited perception as it pertains to Situation Awareness. Traditional C2 systems situational awareness elements are typically focused on a geospatial understanding of the battlefield. This can be seen, most notably, in red force/blue force tracking systems and many other command and control sub-systems. Capabilities, not on the battlefield, are considered in the context of readiness but are typically not an integrated part of the situation awareness picture (i.e. Common Operating Picture). While this separate tracking of human capital and other capabilities is effective in traditional three-dimensional warfare (land, air, and maritime), it is not effective in today's five-dimensional battlefield.

Superior communication and information systems once offered commanders a distinct advantage on the battlefield. Today, that advantage creates a more complex and vulnerable environment to manage and understand (Builder, Bankes, & Nordin, 1999; Krulak, 1996). Specifically, the operational problem faced by commanders in the field is to understand the real- time situation as it pertains to the current health and status of individual C2 resources (including sensors and actuators both on and off the battlefield). This understanding is required in order to dramatically reduce the iteration time for each OODA[1] loop associated with mission planning or re-planning based on detected failures or degraded operational states of the C2 systems (Joint Chiefs of Staff, 2006; 2007; 2008; 2010a; 2010b). Furthermore, commanders on the battlefield require greater accuracy as it relates both to situation assessment