Extending Command and Control Infrastructures to Cyber Warfare Assets

Robert F. Erbacher
Department of Computer Science, UMC 4205
Utah State University
Logan, UT 84322, USA
Robert.Erbacher@usu.edu

Abstract – *the goal of this work is to identify a framework for the integration of cyber command and control within the classical command and control infrastructure. The advent of cyber resources and military capabilities, as well as additional cyber information, requires that command and control infrastructures be updated to incorporate such cyber infrastructures. While much of these infrastructures will operate in isolation from the physical resources, there are needs for cross-over between the two disciplines. Such crossovers require far more flexibility than traditional command and control hierarchies allow.*

Keywords: Cyber Command and Control Infrastructures

1 Introduction

Military command and control infrastructures have traditionally revolved around material assets and reconnaissance. These command and control infrastructures must adapt to incorporate cyber command and control tasks, resources, and requirements. This integration of cyber command and control activities into military infrastructures can be associated with two activities:

- The application of cyber capabilities to enhance information awareness and dissemination.
- The integration of cyber offensive and defensive capabilities as military resources.

The focus of this research is the latter. Thus, the goal of this research is to examine the place for such capabilities in a traditional command and control infrastructure and the changes needed to the typical command and control hierarchy and the chain of command in order to accommodate such changes.

Cyber warfare capabilities have the potential to enormously enhance the capabilities of the military and in essence are becoming critical components of the military. This is due to the extensive use of networked technologies to link squads with the command infrastructure. This allows command personnel to continuous monitor assets. By attacking a military network infrastructure a unit can be isolated just as well as they could be through a physical attack but through far less expenditure of resources. Additionally, information as to the status or location of units could be gained. Thus, the wiring of units, personnel, and resources requires that the network infrastructure be protected through network defensive capabilities, i.e., cyber-defense.

Additionally, as the motto goes, a strong offense makes for a good defense. Thus, military organizations must incorporate cyber-offense based capabilities, i.e. attacks of enemy networks. This aids defense of friendly networks but also has the ability to disrupt enemy physical operations. Methods for conducting cyber or information warfare have been discussed.

Thus, it is critical that cyber infrastructures and resources be incorporated into the command and control hierarchy. However, the significant differences in such a hierarchy require a distinct hierarchy, separate from the physical hierarchy. These two hierarchies must provide mechanisms for coordination due to their ability to impact one another. For example, anomalous network activity in select units can identify the location of a jammer or some other form of attack or interference. This cyber activity can result in a physical response to disable such activity.

Given the need for such a cyber command and control hierarchy, we begin be examining what the cyber command and control hierarchy is and is not. We then examine typical types of activities to be associated with the command and control hierarchy. These results are then used to formulate a model which is described in following sections. Finally, we consider local versus global confrontations and their impact on the hierarchy and challenges of the hierarchy development.

2 Cyber Command and Control

The proposed model is exemplified by Figure 1. The goal of the model is to identify the principal components of a cyber command and control hierarchy and show the needed linkages with the physical command and control hierarchy. As the diagram exhibits, network defenses take priority and must be provided against all network accesses, both inbound and outbound.

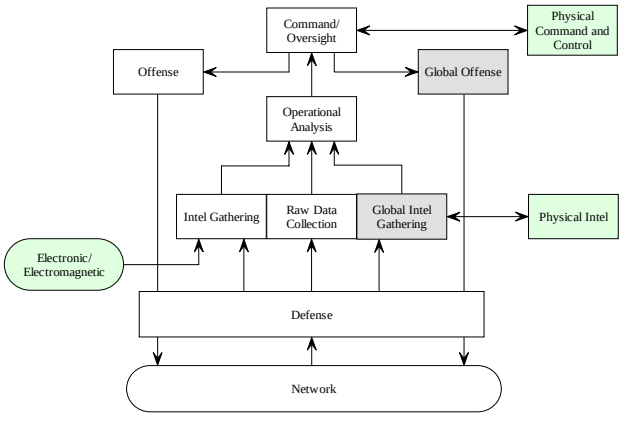

Figure 1: Cyber command and control model representational diagram. Green boxes identify physical units and responses. Grey boxes identify actions related to the global battle sphere, in contrast to the local battle space.

In considering the auspices of cyber command and control, we must consider its goals, requirements, and set of domains (i.e., what it encompasses). This will greatly aid in determining its function within the military hierarchy. Fundamentally, cyber command and control is the command hierarchy responsible for networks and hosts in the operational theater. This would include aspects of sensor networks, communication networks, informational networks, etc. Any computer or informational network which is susceptible to attack and can be used to attack must be considered part of the cyber command and control infrastructure. This is due to the need for additional and separate operational monitoring and management of such networks.

We argue that the additions must be made to the command and control hierarchy due to the level of expertise and the deviation in tasks required by cyber warfare. Thus, we are proposing the cyber command and control infrastructure is instantiated concurrently with the traditional command and control hierarchy.

The fundamental mission objective of the cyber command and control infrastructure is to relate the monitoring and analysis of the integrity of the network and associated hosts within the theater. This is of particularly importance in conjunction with aspects of cyber warfare. Cyber warfare refers to:

- **Offense** - attacking enemy networks with the goal of disrupting their offensive capability, information gathering capability, and defensive capability.
- **Defense** - protecting local networks, protecting communication with soldiers in the field, protecting information gathering capabilities, and identification of enemy activities.
- **Information gathering** – friendly asset positioning and enemy asset positioning through the application of GPS and trilateration as appropriate. Collection of Intel as to enemy activities and goals.
- **Network hot-zone and anomaly detection** – identification and localization of areas of high error rates, loss of communication, or other activity inhibiting to the normal operation of networked infrastructures.

The cyber command and control chain of command must identify what cyber resources are available, where they should be allocated, what tasks they should focus on, the risks to friendly cyber resources, the threats from enemy cyber resources, and both tactical and strategical application of friendly cyber resources based on acquired reconnaissance. In essence, the cyber command and control hierarchy must plan a cyber warfare campaign.

While cyber command and control will have a hierarchy all its own, with its own separate tasks and resources, it will also impact the physical theater and soldiers. The identification of how they are integrated, the chain of command, and how information critical to the physical theater is passed to the appropriate command structure is critical. We can easily see the need for a separate command structure and the need for close linkages with the physical command and control structure, i.e., something akin to troops in the field calling in air strikes. In this fashion, we can envision deployed units calling in a cyber attack to disorient enemy combatants or disable enemy informational awareness capabilities.

2.1 Information Awareness

The goal of cyber command and control is to provide an infrastructure aware of the current status of friendly network resources and to the extent possible that of enemy network resources, allocations, and usages. A pre-requisite of cyber command and control is essentially information awareness, or situational awareness, as it relates to the associated networks. The information available must be conveyed visually, as with typical battle maps; e.g., through visualization techniques. The cyber war map would therefore identify positions and vectors of friendly units, last position of units out of touch, the status of units (ok, casualties, ammo, MIA, rations, etc), connection status (last message time, error rate, transmission rate, bandwidth), accumulated error rates for all units generating a cyber effectiveness rating for each zone, locations of received enemy transmissions, known locations of enemy positions, trilateration of enemy positions with estimated percentage of accuracy, identified zones of poor receptions, possible jamming (flagged).

2.2 Local vs. Global Confrontations

The cyber command and control infrastructure requires information awareness of networked resources, their allocation, and their effectiveness. Additionally, it requires information awareness of enemy network resources to the extent possible. The idea is to consider the network infrastructure to be another type of theater of operation. This theater needs to be related to the physical operational theater due to impacts between the two, such as with the jamming of units in the theater. Thus, there are in essence two scopes of operational theaters, the local theater (war zone) and the global theater (propaganda zone). The command infrastructure needs to deal with both and assign appropriate resources to each as needed by present conditions.

When considering the global theater, consider that in a physical scenario they would be considered completely different levels in the chain of command due to their scale and deviation in scope and level in the hierarchy. However, in this scenario we are considering enemy units in the local theater using the Internet to initiate propaganda. Thus, we have a local action applying to a global scale. We must initiate local cyber counter measures but also physical countermeasures when deemed appropriate. Through cyber counter measures we may be constantly chasing after the individual. Can we identify a physical location from which the propaganda is being created and initiate a physical counter measure? This requires local physical Intel as well as cyber Intel. This requires direct communication between the different command and control structures to be effective. Due to the immediacy of cyber activity, the delay in a full chain of command pass over would be detrimental. Thus, while a separate command and controls structure is needed there must be close ties to the physical command and control structure.

3 Acknowledgements

Much of this work was performed at AFRL, Rome Labs, under their summer faculty research program.