

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. This paper discusses available cyber resources, typical goals of such resources, the reasoning behind such crossover activity, and a developed model for providing such a hierarchy.*

Keywords: Cyber Command and Control, Network Infrastructures, Information Awareness

1 Introduction

Military command and control infrastructures have traditionally revolved around physical and 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 one of 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 continuously monitor assets. These informational networks, i.e., sensor networks, provide an additional avenue of attack. 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 [7].

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 capabilities.

Given the need for such a cyber command and control hierarchy, we begin by 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

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 be 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 particular 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 strategic application of friendly cyber resources based on acquired reconnaissance. In essence, the cyber command and control hierarchy must plan a cyber warfare campaign [5].

We must also consider how aspects of cyber reconnaissance affect physical unit and resource deployment and movement. If there is a network jammer in a building that impacts friendly troops then this should impact the deployment strategy, i.e., avoid this area until the jammer can be taken out or deploy units *to* take out this resource.

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 [3], as it relates to the associated networks. The information available must be conveyed visually, as with typical battle maps; e.g., through visualization techniques [2]. 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).

The goal is to generate a map overlaid onto the landscape showing the impact of the cyber infrastructure from both sides. Much information can be derived from the raw data, such as possible positions of enemy jammers/units. This information must be collated by the cyber command and control infrastructure and passed to the physical command and control infrastructure as needed. While the cyber command and control infrastructure will be focusing on the

network aspects of the battlefield, the fact that soldiers are generally wired in today's military greatly blurs the line between the two command structures. There must be a separate command structure to the extent of additional functionality.

The visualization capabilities have primary concern with the operational theater. However, visualizations can be applied to provide analysis of cyber warfare on a more global scale. For example, such representations would provide detail as to the number and location of propaganda sites by each side, the activity undergoing to discredit or disable each enemy propaganda site, as well as the status of networked infrastructures such as power and communications. This allows the chain of command to identify targets accessible through networked attacks and suitable for reducing the ability of the enemy to continue the confrontation. In essence, available data and informational sources must be fused into a single visual presentation for command and control analysis [1].

Ultimately, visualization tools are needed for the total integration of cyber assets. Both network infrastructure organization and their relationship to physical topology must be represented in a clearly comprehensible and intuitive fashion. There are several difficulties here which must be resolved. First, the volume and dimensionality of the data to be represented results in a significant obstacle to the ease of representation of said data. Second, the need to correlate said data with a terrain map with associated error rates for correct information awareness presentation is critical but also challenging.

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 [4]. 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.

One possible strategy would be to entice enemy units to put effort into attacking rather than defending, or vice versa. Do they have the resources to do both effectively? If they are defending then they can't attack. If enemy units have nothing to defend, as is the case with insurgencies, then force them to attack something less desirable (e.g., honeypots). In other words, give them something that needs to be attacked such that they either cannot defend or they cannot apply more effective attacks. Rather than distributing propaganda or attacking our main systems entice them to attack our propaganda machine or hardened units in the field that are prepared for it. The command and control personnel must be concerned with friendly resources and allocations in addition to enemy resources and allocations. Can we control enemy resource allocations in cyber space? Doing so can force enemy units to perform actions we are interested in them doing rather than truly harmful actions.

3 Cyber Command and Control Model

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 also 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. Given the likelihood of attack, this is critical.

Network data is collected and stored for operational analysis according to a variety of rules. First, raw network data is collected to aid in local defensive and offensive operations within the local battle space. Additionally, network-based Intel is collected for use by operational analysis personnel to aid in identification of local troop movements, particularly enemy troops. This can then be compared with known information from other sources, e.g., GPS coordinates of friendly troops; thus the need for data from the electromagnetic spectrum, i.e., for trilateration purposes. Intel is also collected from the global battle space. This will include the Intel relating to the location of

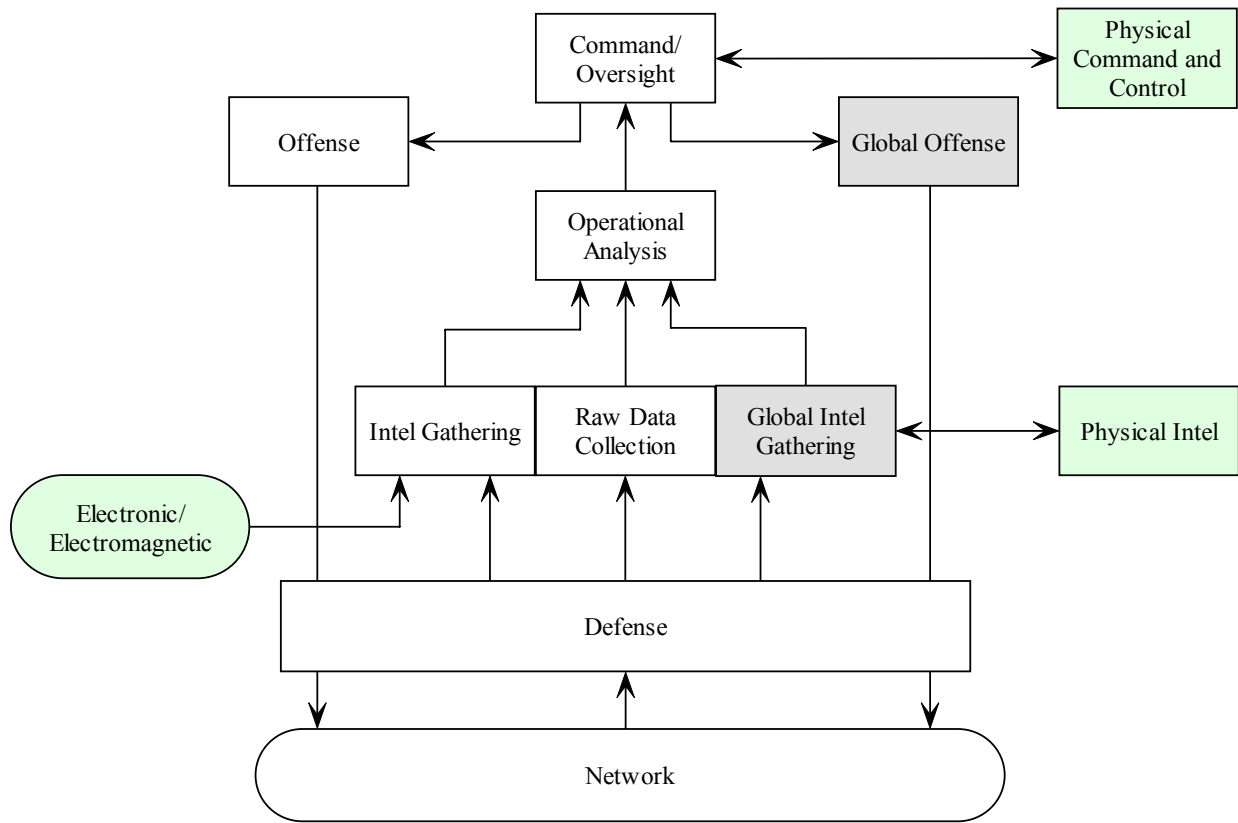


Figure 1: Cyber command and control model representational diagram. Green boxes identify physical units and responses. Grey boxes identify actions related to the global battle sphere, in contrast to the local battle space.

enemy propagandists and command oversight located in third party countries or elsewhere outside of the immediate battle space.

All three of these forms of data gathering benefit from and provide benefit to the physical Intel and oversight. This is due to the ability to validate unit positions, identify threats to friendly units, particularly jamming or other anomalous interference to communications.

This information is provided to operations analysis personnel such that an analysis can be provided to command and oversight personnel. It is this command level that will determine the needed offensive response and issue such orders directly, assuming a cyber response is to be initiated. Additionally, this command level will also be responsible for communicating with the physical command and control personnel if a physical response is deemed to be warranted. This may occur if the cyber Intel identifies the location of enemy units or potential jammers that can not be acted against through cyberspace. Thus, a physical response may be needed to take these units out or disable the jamming device.

The collected data will also be provided to the physical Intel community. This will aid in validation and

improvement of information awareness. It would be a grave mistake to completely isolate the information available to each of the command hierarchies. Errors due occur in current Intel gathering paradigms and disagreeing information must be remedied.

Finally, our model provides for the segregation of global versus local offensive actions, as is discussed in section 2.2. Local actions would result in offensive actions against units, assets, or resources within the local theater of operation. Such actions would have direct impact on local units, both friendly and hostile. Global actions are applied against non-local resources or assets. This would deal with propaganda being distributed from a non-local source or command oversight being provided from outside of the local theater. Disabling such non-local capabilities can have enormous impact on the effectiveness of enemy capabilities.

4 Challenges

While we have begun to lay out the foundations for a cyber command and control hierarchy to work in collaboration with the physical command and control hierarchy, there remain many challenges yet to be resolved. These challenges cover both technical aspects as well as

organizational aspects of the cyber infrastructure. These challenges persist due to the young and changing face of cyber capabilities and characteristics. Such challenges include:

How can the signals generated by units be trilaterated to identify their positions [6]? This is particularly important when GPS values aren't available, such as for enemy units. Trilateration is essentially a type of triangulation algorithm applied to a series of three signals generated by some device. GPS applies trilateration to the available GPS satellite signals. This trilateration must take buildings and other sources of interference and signal degradation into account for accuracy. Current trilateration approaches do not take such things into consideration. Locations inside of buildings will thus be inaccurate. This trilateration can be done from the wireless signals generated by enemy units, either from signal strength or signal receipt time. Both techniques can generate incorrect results due to signal bouncing but signal receipt time is less subject to artificial degradation due to interference from structures or terrain.

How can the sharing of operational information and Intel with the physical command and control infrastructure be supported by the segregated hierarchies? Additionally, this sharing must be performed rapidly in combat situations with minimal oversight. Such lack of oversight and approval can cause tension between the two chains of command. Determining how to formalize such information exchange between segregated command hierarchies will remain a challenge but is critical to success, as has been seen with the formation of the department of homeland security [8].

How can command personnel be made to comprehend the extent of cyber capabilities, their effectiveness, and their application? This is important such that the command and control hierarchy comprehends the meaning and limits of the presented information. With the rapid changing and advancement of technology it is necessary to maintain a small amount of doubt with respect to the effectiveness of defensive techniques. Additionally, the cyber command and control hierarchy must be very adaptable and able to integrate new techniques and technologies in short order. Rather than getting a new tank every thirty years, new cyber technology, that could offer significant advances, will be available every thirty days, perhaps even more rapidly in some scenarios.

How much information should be shared between defensive and offensive components of the cyber warfare capabilities? What are the legal issues with offensive technology as it relates to cyber warfare? This becomes particularly problematic with the involvement of civilians distributing propaganda and with global activities by individuals. What happens if enemy units staged in a third party country are distributing propaganda or providing

command oversight? What options are available for combating such capabilities?

To what extent should the infrastructure allow direct communication between units? With the wiring of the military and individual units it is quite feasible for units to share information with one another without approval of the chain of command. What extent of collaboration should be incorporated and allowed? Extensive communication and collaboration is useful but can lead to issues with the chain of command and inappropriate use of the resources, i.e., internal misuse. The sharing of information without approval could aid enemy misinformation objectives but failure to share information can prevent units from having a timely and complete assessment of status within the battlefield.

How can unit effectiveness be measured when the unit's activities take place in cyberspace? This is essentially a measurement issue. Generally, military units will undergo an after action review assessment of their performance. This after action review determines what the unit did right and wrong and provides both an opportunity for learning and a way of determining the effectiveness of a given unit. How can we perform such an after action review of cyber battles and identify the effectiveness of cyber-based units? How can we identify what went wrong? Will we even know, especially for offense?

Finally, how can we associate value with cyber or virtual resources? One critical aspect of resource allocation is the association of value with assets. The identified value can then be used to determine the extent to which the asset should be defended or attacked, in the case of enemy assets. However, cyber assets currently do not have the same association with value and this can lead to misallocation of resources during critical times. This again leads to the need for the separate command hierarchy as the separate command hierarchy will be better positioned to comprehend the value of cyber-based resources and will not overlook their value in light of physical assets.

5 Conclusions and Future Work

The goal of this work was to begin developing a framework for the integration of cyber capabilities into the day to day operations of military command and control infrastructures. The proposed solution provides a distinct and separate but integrated command hierarchy for cyber-based resources. This is necessary due to the completely distinct set of capabilities available within the cyber domain as well as the completely disjoint theater of operation, i.e., cyberspace. Thus, we propose following the paradigm entrenched in the familiar divisions of the armed forces, i.e., air force, army, navy, etc.

The proposed model is designed to incorporate the needed cyber capabilities at a high level while also identifying the needed integration with the physical command and control infrastructure. This integration will be difficult but is not unheard of, as current deployed units can call in air strikes or bombardment.

Given that this is a novel analysis there remain enormous numbers of technical, educational, and logistical challenges yet to be resolved. These challenges derive from the fact that this aspect of military command and control has previously not been examined. This initial examination of such challenges will aid determination of what directions should be pursued to make such a command and control infrastructure a reality. By no means is the listed discussion complete.

Additionally, in order to aid identification of tasks associated with such cyber units and identify the capabilities this command hierarchy must be capable of handling we have developed an initial set of tasks to be associated with such a command and control hierarchy. This task list is presented in Appendix A.

6 Acknowledgements

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

7 References

- [1] Airforce AFOSR PRET: Information Fusion for Command and Control (IFC2): The Translation of Raw Data To Actionable Knowledge and Decision http://www-2.cs.cmu.edu/~softagents/project_grants_afosr.html.
- [2] Stuart K. Card, Jock D. Mackinlay, and Ben Schneiderman, *Readings in Information Visualization: Using Vision to Think*, Morgan Kaufmann Publishers, 1999.
- [3] Steve Jameson, "Architectures for Distributed Information Fusion to Support Situation Awareness on the Digital Battlefield," *Proceedings of the 4th International Conference on Data Fusion*, August 2001.
- [4] James Chee Khan, David Vi-Keng, Daniel Soo Sim, Tee Huu, Nicholas Boon Hwee, Gregory Kheng Lee, Tiat Leng, and Karen Burke, Information Assurance Plan for the Protection of the Sea Base Information Systems, Naval Postgraduate School, 2003.
- [5] Fredrick Okello, Richard Ayres, Patrice Bullock, Brahim Erhili, Bruce Harding, and Allan Perdigao, "Information Warfare: Planning The Campaign," Research Paper: ACSC/DEC/124/96-04, <http://citeseer.csail.mit.edu/okello96information.html>
- [6] H. Staras and S. N. Honickman, "The Accuracy of Vehicle Location by Trilateration in a Dense Urban Environment," *IEEE Transactions on Vehicular Technology*, Vol. VT-21, No. 1, pp. 38 - 44, February 1972.
- [7] Claw Wilson, Information Warfare and Cyberwar: Capabilities and Related Policy Issues, CRS Report for Congress RL31787, <http://www.fas.org/irp/crs/RL31787.pdf>, 2004.
- [8] Homeland Security, Securing Our Homeland: U.S. Department of Homeland Security Strategic Plan, http://www.dhs.gov/interweb/assetlibrary/DHS_StratPlan_FINAL_spread.pdf, 2004.

8 Appendix A : Task List for Cyber Command and Control

This appendix is geared towards providing an initial set of capabilities and tasks to be set forth by the proposed cyber command and control hierarchy. Units within this hierarchy would be responsible for one or more of the identified capabilities. These tasks are divided into six categories.

- Deploy network infrastructure in the theater of operation
- Allocate network resources
 - Ensure quality of service measures are met
 - Data from soldiers in the field must meet bandwidth and delay constraints
 - Ensure priority of service measures are met
 - Soldiers in the field have priority over those off duty
- Monitor network for appropriate effectiveness
 - Identify and defend against attacks to the network
 - Identify impacts of attacks and intrusions on the physical operation of units
 - Notify impacts up the chain of command
- Identify and maintain status of units
 - Position
 - Movement
 - Deviations from expected action
 - Information is based on electronic information
- Allocate available resources to disrupt enemy network usage
- Identify and prioritize targets and modes of operation
 - Possible modes of operation include:
 - Propaganda warfare
 - Distribution of information only

- Distribution of information and disruption of enemy propaganda
- Information gathering
 - Attack enemy capabilities for information gathering
 - Identify location of enemy units
 - Identify targets/plans of enemy units
 - Identify detection of Intel gathering
- Cyber warfare
 - Attack enemy combatants ability to communicate
 - Attack enemy general infrastructure
 - Pass incorrect information to enemy combatants
- Operational functionality
 - Identify impacts on operational functionality
 - Monitor error rates
 - Identify causes and sources of error rates
 - Flag and notify chain of command of areas with poor communication
 - Possible causes include infrastructural interference, enemy jamming, environmental, terrain formations
 - Monitor probing rates. Identify possible passive monitoring (How?)
 - Flag and identify possible trilateration, enemy Intel gathering, attacks in progress
 - Apply trilateration for location identification of enemy activity

- Network hubs, routers, switches
- Jammers
- Sniffers

o Possible targets include:

- Enemy websites
 - Identify location of web sites
 - Continuously monitor for new appearances of web sites
 - Monitor web site content
 - Disable distribution of propaganda
 - Replace enemy propaganda with friendly propaganda
 - Disable web sites entirely
- Enemy mobile devices
 - Laptops
 - Combatant communication devices
 - Cell phones
- Enemy fixed devices
 - Command and control systems
 - Targeting systems
- Enemy e-mail based services
 - Disable all ability to communicate propaganda
 - Prevent ability for “civilians” to identify friendly troop positions and movements
- Enemy streaming video services
- Enemy television services
- Enemy network infrastructure