Air Force Institute of Technology

AFIT Scholar

Theses and Dissertations

Student Graduate Works

3-2008

Identification of Command and Control Information Requirements for the Cyberspace Domain

Brian D. Aschenbrenner

IDENTIFICATION OF COMMAND AND CONTROL INFORMATION REQUIREMENTS FOR THE CYBERSPACE DOMAIN

THESIS

Brian Aschenbrenner, Captain, USAF

AFIT/GIR/ENG/08-01

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government.

AFIT/GIR/ENG/08-01

IDENTIFICATION OF COMMAND AND CONTROL INFORMATION REQUIREMENTS FOR THE CYBERSPACE DOMAIN

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Information Resource Management

Brian Aschenbrenner

Captain, USAF

March 2008

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

AFIT/GIR/ENG/08-01

IDENTIFICATION OF COMMAND AND CONTROL INFORMATION REQUIREMENTS FOR THE CYBERSPACE DOMAIN

Brian D. Aschenbrenner, BS
Captain, USAF

Approved:

_______________/signed__________________ ________________
Robert F. Mills, PhD (Chairman) Date

_______________/signed__________________ ________________
Michael R. Grimaila, PhD (Member) Date

_______________/signed__________________ ________________
Paul D. Williams, Maj, USAF (Member) Date

AFIT/GIR/ENG/08-01

Abstract

The purpose of this research was to develop an information requirements analysis method that would provide the Director of Cyberspace Forces with the information required to support effective command and control of cyberspace. This research investigates the role of information in command and control, information in the traditional war fighting domains, cyberspace as a war fighting domain, and various methods of determining information requirements of organizations. This research produced an information requirements analysis method that is suitable for identifying the command and control information requirements of the Director of Cyberspace Forces.

Acknowledgements

I would like to thank my faculty advisor, Dr. Robert Mills for his guidance throughout the course of this research effort.

Brian D. Aschenbrenner

Table of Contents

Page

Page

List of Figures

Figure Page

List of Tables

Table Page

IDENTIFICATION OF COMMAND AND CONTROL INFORMATION REQUIREMENTS FOR THE CYBERSPACE DOMAIN

I. Introduction

Cyberspace is a dynamic environment that is becoming increasingly important to civilizations around the world. Industries and governments are exploiting a variety of cyberspace capabilities to gain a strategic advantage over their competition. The United States, along with many other countries and industries have been exploiting cyberspace capabilities without employing measures to thoroughly protect and control their cyber interests. America's adversaries recognize our dependence on the un-controlled cyberspace domain and see it as a soft target for attack that could disrupt our national center of gravity and further their agendas (9:1). The focus of this research is to identify the information requirements that are required to enable a cyber commander to visualize the cyber-battlespace and effectively Command and Control (C2) offensive and defensive cyber operations.

The purpose of this chapter is to provide an overview of research efforts that are applicable to the identification of C2 information requirements for a cyberspace commander. The concept of cyberspace is defined first to establish the scope of the problem area. Military C2 is introduced next to establish a general understanding of C2 theory and information requirements. The nature of the various warfighting domains is also discussed to establish and understanding of basic domain characteristics. Finally, Air Force initiatives in cyberspace are overviewed to complete the framing of the conceptual problem area. The research problem to be investigated, methodology applied, and a preview of subsequent chapters follows the overview of research efforts.

Background

The term “cyberspace” was created by William Gibson in a 1982 science fiction short story titled “Burning Chrome” (17:1). Gibson used the term to reference a state of computer-simulated reality. The Merriam-Webster dictionary defines cyberspace as “the online world of computer networks and especially the internet” (19). In September 2006, the Joint Chiefs of Staff recognized cyberspace as a distinct warfighting domain “characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange data via networked systems and associated physical infrastructures” (8:1). This radical expansion of the definition extends the traditional definition of cyberspace well beyond the concept of networked computers to encompass all electronic devices that transmit, receive, or emit electronic signals throughout the electromagnetic spectrum (18:62).

Timely and accurate information is essential for effective C2 of every warfighting domain. Joint Publication 3-0, *Joint Operations*, defines C2 as the exercise of authority by a military commander over assigned troops to accomplish a mission (5:III-1). Communicating critical information with assigned forces and assessing the status of the operational environment are two key functions of C2 (5:III-1). Commanders depend on C2 information to visualize the battlespace within a volume of time and space and support effective decision-making (5:III-1). The information requirements depicted in

Figure 1 typically include priority intelligence information focused on the enemy and the operational environment and friendly forces information that details coalition force activities and mission capabilities (5:III-11).

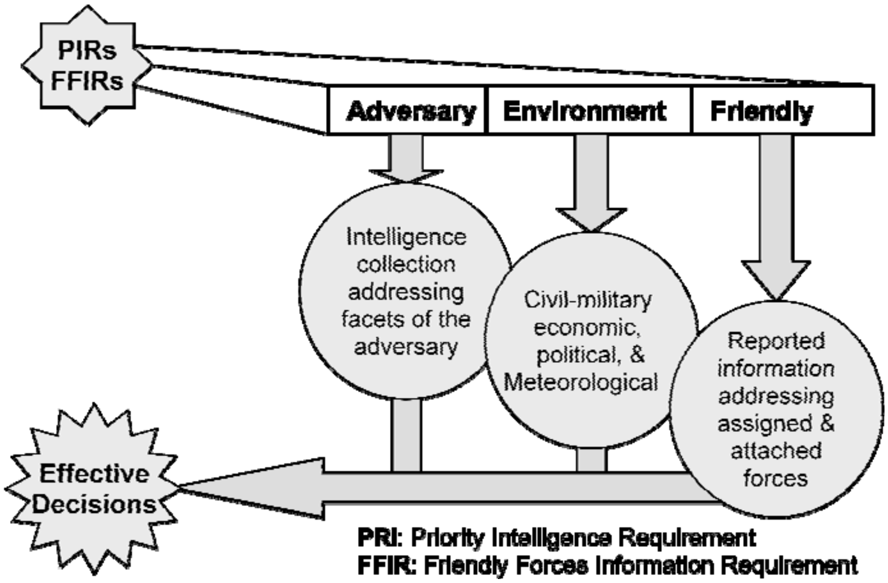

PIRs
FFIRs
Adversary
Environment
Friendly
Intelligence collection addressing facets of the adversary
Civil-military economic, political, & Meteorological
Reported information addressing assigned & attached forces
Effective Decisions
PRI: Priority Intelligence Requirement
FFIR: Friendly Forces Information Requirement

Figure 1. Information Requirement Categories (5:III-11)

The traditional warfighting domains of air, land, sea, and space can each be characterized by their physical nature. Assets in the traditional domains can be visualized and physically manipulated by the commanders to achieve the desired effects culminating in domain superiority. Commanders in the traditional domains rely on operational experience within their physical domain to designate the majority of their own C2 information requirements and his or her staff collects and organizes the information to support effective decision making (5:III-11). Cyberspace has become a force enabler for the traditional warfighting domains (9:2). The traditional domains rely on cyberspace capabilities to attain situational awareness, tailor an appropriate course of action, and execute that course of action to achieve desired effects throughout the battlespace (9:2).

Figure 2 illustrates how cyber domain is used to achieve cross-domain effects (8:6). Thus, freedom to operate in cyberspace is considered a prerequisite to effective operations in the traditional warfighting domains because the majority of their C2 networks reside in cyberspace (9:2).

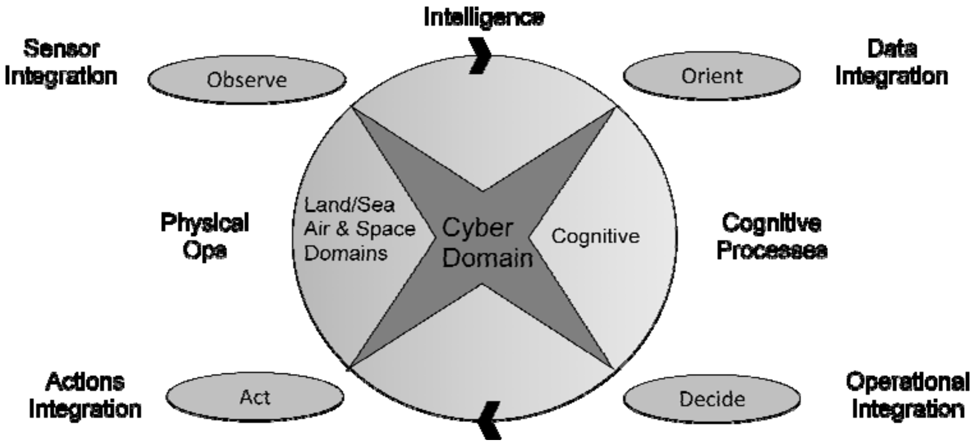


Figure 2. Cross Domain Effects (8:6)

The recognition of cyberspace as a distinct warfighting domain is the result of the United States' increasing dependence on cyberspace capabilities for military and civilian purposes (8:1). In November 2006, Air Force Cyber Command was established and is currently developing doctrine for integrating cyber effects into the Air Force's global strike capability and conducting offensive and defensive cyber combat operations in support of national objectives (8:1). The virtual nature of the cyberspace along with evolutions in information technologies has increased the volume of available information to a point of information overload (14:1). Situational awareness in cyberspace will therefore require finding, sorting, and integrating data into decision quality information (14:1).

Problem to be Investigated

The purpose of this research is to identify the information requirements that will enable a cyberspace commander to visualize the cyber-battlespace and effectively C2 military operations throughout the cyberspace domain. The recognition of cyberspace as a warfighting domain necessitates the development of tactics, techniques, and procedures for C2 that are uniquely suited for military operations in cyberspace to ensure our continued ability to operate freely in the domain. Identification of C2 information requirements will support cyberspace commanders by providing key cyber leverage points for inclusion in the cyber decision cycle. The C2 information requirements will also allow cyberspace commanders to effectively employ cyber forces and capabilities to conduct offensive, defensive, and support cyber operations. Identifying C2 information requirements for cyberspace is a fundamental aspect of achieving cyberspace superiority which will enable our freedom to operate in the domain while denying that same freedom to our adversaries (8:5).

A series of investigative questions will be asked to facilitate solving this research problem. First, what is the role of information in C2? The answer to this question will indicate whether the basic purpose of this research is necessary or not. Second, how do the traditional warfighting domains identify C2 information requirements? Solving this question may identify a method for determining the C2 information requirements for cyberspace commanders. Third, is there an existing method or, can a method be developed for identifying information requirements for military C2 of cyberspace? Answering this question will indicate if the identification of C2 information requirements for cyberspace commanders is possible and if the information requirements identification process is reproducible.

Scope/Methodology

A content analysis will be conducted to systematically examine the study of C2, information requirements analysis, and military doctrine to identify patterns or themes that relate to the identification of C2 information requirements. Academic research in the fields of situational awareness, decision support, and information requirements analysis will be included in the body of research and evaluated based on their applicability to military C2. Characteristics and qualities of factors contributing to the identification of C2 information requirements will be examined and defined in concise terms to provide a consistent conceptual framework for the remainder of the research effort. The data resulting from this content analysis will be used to interpret the role of information in C2, the identification of C2 information in the traditional domains and methods for identifying C2 information requirements.

Preview

This research is organized into five chapters with the first chapter being the introduction. Chapter II provides the literary review of pertinent background material related to the identification of C2 information requirements. Chapter III proposes a methodology for the identification of C2 information requirements for a cyberspace commander. Chapter IV will determine if the C2 information requirements method proposed in Chapter III is producible or not. Chapter V will provide a conclusion of the research effort and offer potential areas for future study.

II. Literature Review

Overview

This chapter provides background information that will enable the reader to understand key research concepts related to the complexity of identifying the C2 information requirements for a cyberspace commander. The background begins with an overview of the role of information in C2 to demonstrate how commanders depend on information to support effective decision-making. Then, information in the traditional warfighting domains is analyzed to highlight various natures of C2 information and methods for determining information requirements. Air Force Cyber Command is then discussed to frame the complex operating environment in which C2 information will be identified and used. The final section of the chapter discusses information requirements analysis methods that could be used to identify the C2 information requirements of cyberspace commanders.

The Role of Information in Command and Control

Information plays a critical role in all decision making and control settings. The military is one unique context. Drucker suggested that information that provides a foundation for knowledge is the principal means to create wealth and power in the post-capitalist society (12:8). This idea is clearly salient to the military where timely and accurate information is the foundation for the commander's visualization of the operational environment enabling them to make effective decisions (5:III-3). Figure 3 illustrates how a commander uses quality C2 information to visualize his operational environment (6:II-33). A force with a superior ability to gather, understand, control, and use information has a strategic advantage on the battlefield (10:ii). Military history is full of examples demonstrating that having the right information at the right time is often the decisive factor of a battle (10:ii).

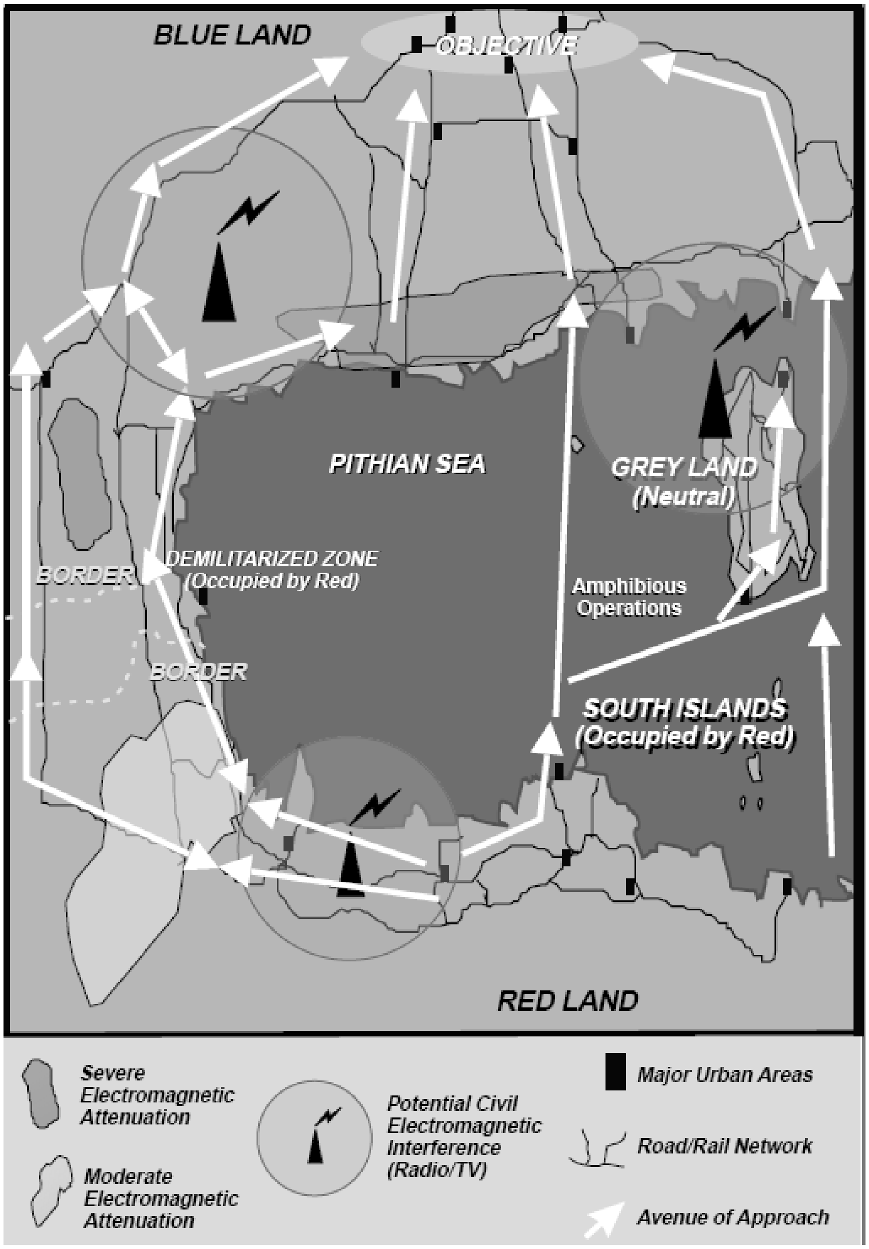
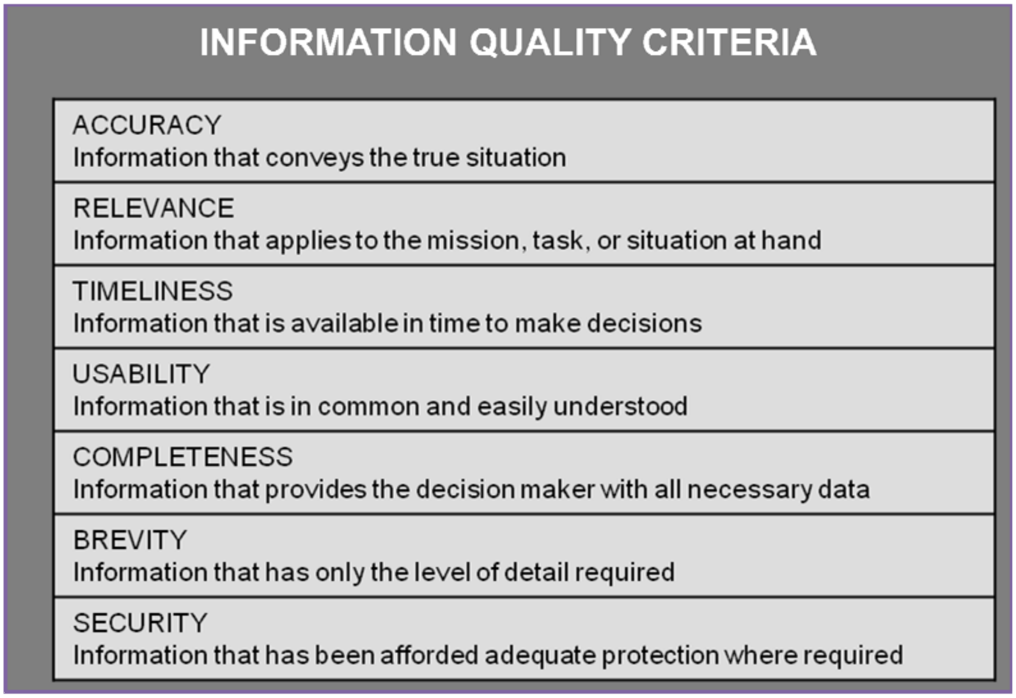

BLUE LAND
OBJECTIVE
PITHIAN SEA
GREY LAND (Neutral)
DEMILITARIZED ZONE (Occupied by Red)
BORDER
BORDER
Amphibious Operations
SOUTH ISLANDS (Occupied by Red)
RED LAND
Severe Electromagnetic Attenuation
Moderate Electromagnetic Attenuation
Potential Civil Electromagnetic Interference (Radio/TV)
Major Urban Areas
Road/Rail Network
Avenue of Approach

Figure 3. Visualization of the Operational Environment (6:II-33)

Information that is provided to the war fighting decision maker must be appropriate for the level of war they are making decisions in. Joint Publication 3-0, *Joint Operations* identifies three levels of war. The three levels of war are: strategic, operational, and tactical (5:II-1). The strategic level of war represents a level in which a nation or a group of nations determine a strategic objective they wish to achieve such as, expel the Iraqi army from Kuwait (5:II-1). The operational level of war links the tactical employment of forces to national and military strategic objectives such as, use fighter aircraft to destroy Iraqi air defenses (5:II-1). The tactical level of war is focused on the planning and execution of battles, engagement, and activities assigned to individual units or task forces such as, destroy the anti-aircraft artillery located at Baghdad International Airport (5:II-1). The characteristics of information required to support effective C2 are different for each level of war.

Joint Publication 3-13, *Information Operations* characterizes the quality of information required to support effective decision making in Figure 4 (4:I-3). Providing decision makers with information meeting the information quality criteria postures him to make the best decision possible for a given situation. Information that complies with this criterion enables the decision maker to focus on the decision at hand and not be distracted by information items that are not directly associated with the decision that is being made at that point in time.



INFORMATION QUALITY CRITERIA

ACCURACY
Information that conveys the true situation

RELEVANCE
Information that applies to the mission, task, or situation at hand

TIMELINESS
Information that is available in time to make decisions

USABILITY
Information that is in common and easily understood

COMPLETENESS
Information that provides the decision maker with all necessary data

BREVITY
Information that has only the level of detail required

SECURITY
Information that has been afforded adequate protection where required

Figure 4. Information Quality Criteria (4:I-3)

The Observe, Orient, Decide, and Act (OODA) loop was proposed by John Boyd in the 1950s to represent the decision cycles of Air Force pilots and is still used in military doctrine to represent the C2 decision cycle (3:1). The OODA loop presented in Figure 1 represents the decision cycle in which decision makers observe, orient, decide, and act (2, 3:1). Decision makers must have timely and accurate information to gain a situational awareness (observe and orient) of the operational environment and achieve decision superiority. Decision superiority (C2 superiority) is achieved by maintaining an ongoing situational awareness that allows decision makers to accurately execute their decision cycles faster than their adversary can react (10:1, 3:1).

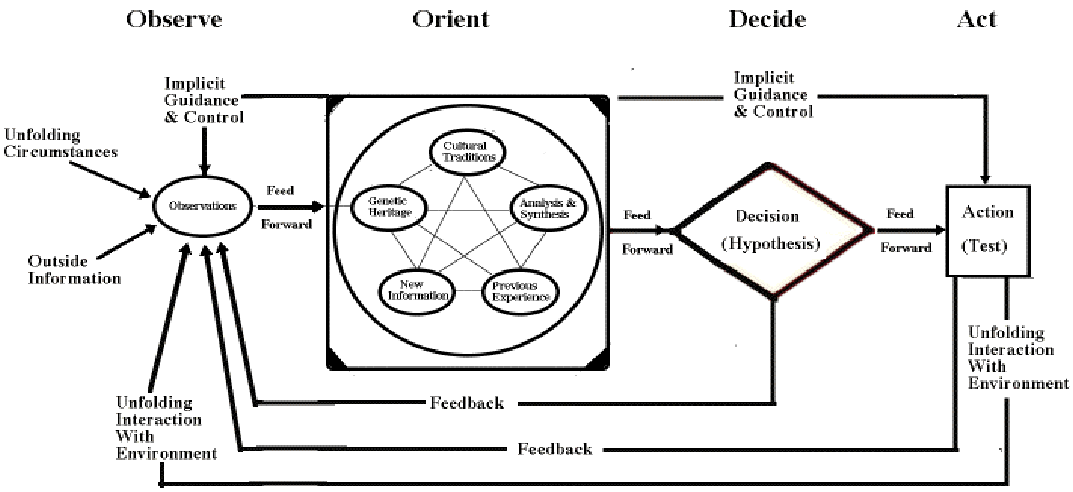


Figure 5. John Boyd's OODA Loop (2)

Decision makers must be able to assign meaning to information before they can achieve a situational awareness of the domain (16:150). Failing to identify meaningful C2 information or focusing on the wrong goal will confuse the decision maker and corrupt the C2 process. The information must represent the battlespace in a way that allows decision makers to understand various situations, focus on the most salient of those situations, and make the best possible decisions (1:THB 1/26). These situations, especially within the context of a battle are dynamic and the decision maker’s situational awareness must change along with the situation to remain effective (15:4).

Goals provide a framework for the identification of C2 information requirements. To be most effective, goals must be clearly stated to ensure accurate C2 information is gathered to support goal achievement (13:14). Relating C2 information to specific goals provides a litmus test to determine the “so what” of the information (13:14). Moreover, decision makers typically have multiple goals that may shift in importance as time passes (15:14). Therefore, any information used to achieve situational awareness must align with several goals simultaneously and be sufficiently flexible to support shifting requirements that may arise (14:2).

Information in the Traditional Warfighting Domains

The traditional warfighting domains are functionally divided between the military services. The Air Force has traditionally had primary responsibility for the air and space domains. The Army has primary responsibility for the land domain and the Navy has primary responsibility for the sea domain. The goal of the military services in each domain is to achieve domain superiority thus ensuring friendly forces access and use of the domain and denying the same access and use to the adversary. Information plays a critical role in each of the traditional warfighting domains. Achieving information superiority which is a degree of information advantage over the adversary is an integral part of achieving superiority in the traditional war fighting domains (10:7)

Each of the traditional domains conducts offensive, defensive, and support operations to achieve domain dominance. Military services in the traditional domains (i.e., air, land, sea, and space) operate in well defined physical environments with proven tactics, techniques, and procedures for achieving domain superiority. For example, an offensive air mission against an enemy would necessitate gathering information about possible targets, the enemy's defense capabilities, threats to friendly forces aircraft, and the position of friendly forces as well as civilians in relation to targets. The commander also needs to know the availability of support crews, aircrews, aircraft, and munitions available for the mission and their operational capabilities. This example is provided to highlight the fact that C2 information represents the physical characteristics of the traditional domains. The procedures for identifying C2 information requirements in the traditional warfighting domains must be modified to be useful for identifying C2 information requirements for cyberspace because of extensive differences between the domains.

There are various functions conducted in the traditional domains such as counter air, air interdiction, and close air support that are not representative of the types of functions that will be conducted in the cyber domain. The majority of these functions are representative to the physical nature of the domains however, a few traditional domain operations, such as counter information operations represent a non-physical environment. The non-physical information environment depicted in Figure 6 that is used to connect the physical and cognitive dimensions (4:I-2). Information operations is a mission area of counter information that is conducted within and across the traditional domains and relates closely to the functions that will be conducted in the cyberspace domain.

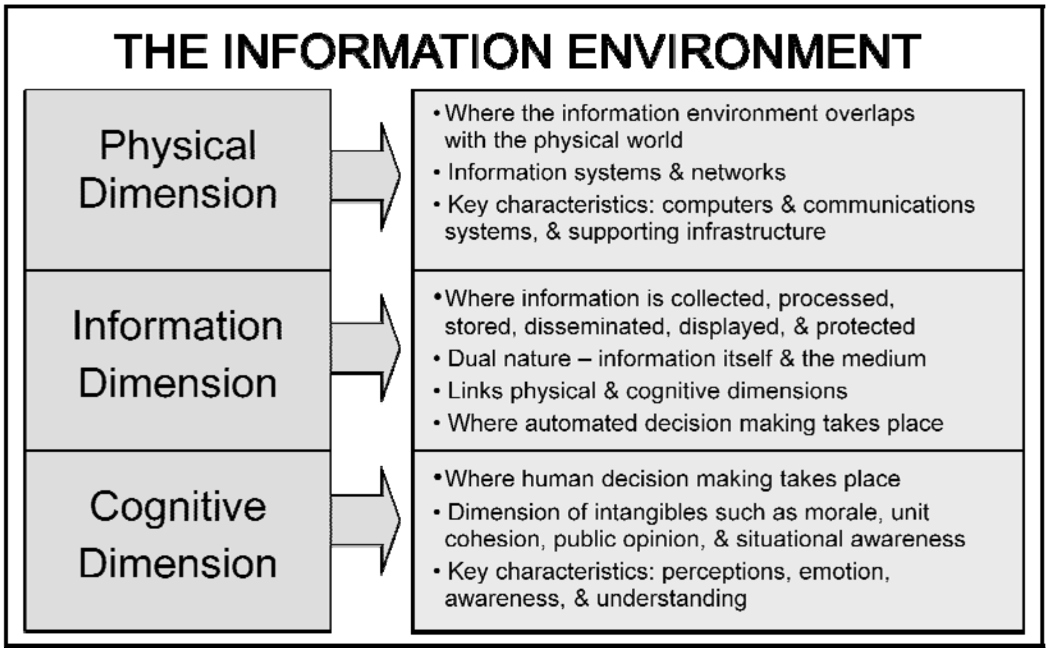

THE INFORMATION ENVIRONMENT
Physical Dimension
• Where the information environment overlaps with the physical world
• Information systems & networks
• Key characteristics: computers & communications systems, & supporting infrastructure
Information Dimension
• Where information is collected, processed, stored, disseminated, displayed, & protected
• Dual nature – information itself & the medium
• Links physical & cognitive dimensions
• Where automated decision making takes place
Cognitive Dimension
• Where human decision making takes place
• Dimension of intangibles such as morale, unit cohesion, public opinion, & situational awareness
• Key characteristics: perceptions, emotion, awareness, & understanding

Figure 6. The Information Environment (4:I-2)

The assigned mission of Air Force Information Operations is to integrate the employment of capabilities of influence operations, electronic warfare operations, and network warfare operations, in concert with specified integrated control enablers, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own (10:1). The primary goal associated with the Air Force's mission in information operations is to achieve information superiority. Information superiority is a degree of dominance in the information domain which allows friendly forces the ability to collect, control, exploit and defend information without effective opposition (10:1). Information superiority enables decision makers across the traditional warfighting domains to observe, orient, decide, and act faster and more effectively than the adversary (10:1). Figure 7 illustrates the central role that the information domain and information superiority play in a commander's decision cycle (10:3).

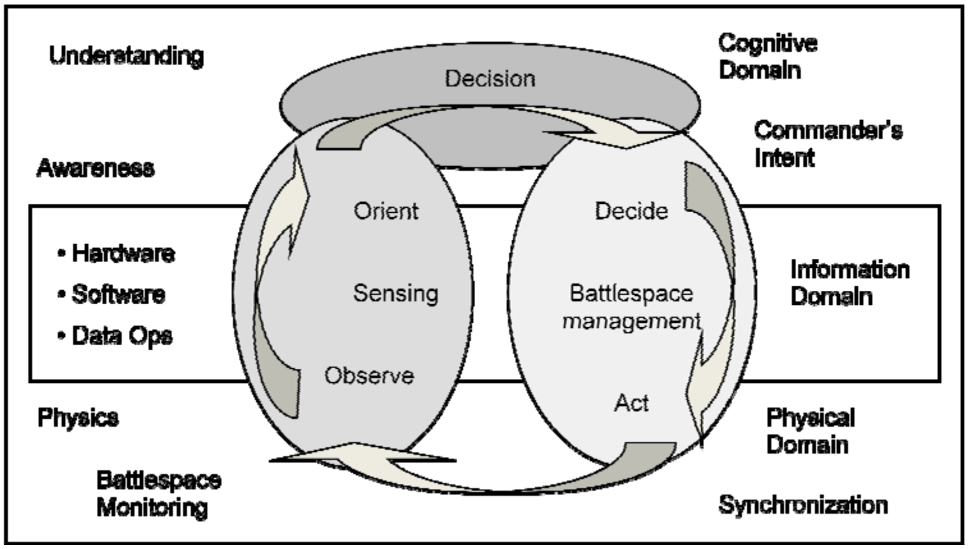


Figure 7. The Information Domain's Role in the Decision Cycle (10:3)

Information operations include influence operations, electronic warfare operations, network warfare operations, and integrated control enablers (10:1). Information operations are very similar to cyber warfare operations as they are conducted to create effects across and throughout the traditional domains in all levels of conflict (10:1). Identifying the missions, goals, and operations areas associated with information operations will facilitate the identification of the missions, goals, operations areas, and capabilities associated with cyber warfare.

Influence operations are conducted to affect the perceptions and behaviors of leaders, groups, and entire populations to ultimately change the adversary's decision cycle (10:1). Influence operations include psychological operations, military deception, operations security, counterintelligence operations, counterpropaganda operations, and public affairs operations. Influence operations are conducted across the traditional domains as well as in and through the cyber domain.

Network warfare operations are "the integrated planning, employment, and assessment of military capabilities to achieve desired effects across the interconnected analog and digital network portion of the battlespace" (10:5). These networks are an interconnected and interrelated assortment of electronic systems which are used to store or transmit information (10:19). Networks associated with network warfare operations include: radio networks, satellite links, tactical digital information links, telemetry, digital track files, telecommunications, and wireless communications networks (10:5). Network warfare operations include offensive (network attack), defensive (network defense) and support (network warfare support) missions (10:19).

Network attack operations employ network capabilities to destroy, disrupt, corrupt, deny, degrade, or usurp information that is either stored in or transmitted through networks (10:20). Network defense operations employ network based capabilities to defend friendly information that is either stored in or transmitted on networks from the adversary’s attempts to destroy, disrupt, corrupt, or usurp it (10:20). Network warfare support operations involve the collection and production of network related data that supports effective network operations decision making (10:21). Network warfare support enables network attack and network defense actions to find, fix, track, and assess both adversary and friendly sources of access and vulnerability of networks (10:21). Network warfare support personnel are responsible for producing: the network order of battle, profiling, event analysis, open source review, and pattern analysis in support of network warfare defense and countermeasure development, nodal and system analysis to identify vulnerabilities in adversary networks, and full spectrum and cryptological planning and de-conflictions (10:21).

Electronic warfare is military action involving use of the EMS or directed energy to manipulate the EMS or attack and adversary (10:23). Electronic warfare operations are “the integrated planning, employment, and assessment of military capabilities to achieve desired effects across the electromagnetic domain in support of operational objectives” (10:23). Electronic warfare operations are conducted to control and coordinate friendly use of the EMS and attack or deny enemy use of the EMS (10:5). Electronic warfare operations include offensive (electronic warfare attack), defensive (electronic warfare protection), and support (electronic warfare support) missions (10:5).

Electronic warfare attack operations utilize electromagnetic, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment (10:23). The goals associated with electronic warfare attack are to deceive, disrupt, deny, or destroy the adversary's combat capabilities that utilize the EMS (10:23). Electronic warfare protection operations are conducted to enhance the use of the EMS for friendly forces (10:24). Electronic warfare protection is primarily a defensive function focused on protecting personnel, facilities, and equipment from negative effects caused by either friendly or adversary electronic warfare actions that degrade, neutralize, or destroy friendly combat capabilities that utilize the EMS (10:24). Electronic warfare support involves the collection of EMS data for immediate tactical applications such as, threat avoidance, route selection, targeting or homing (10:24). The collected data supports effective electronic warfare operations decision making (10:24). Electronic warfare support personnel are responsible for producing: the electronic order of battle, parametric data reflecting the electronic characteristics of electronic warfare threat systems to aid detection and countermeasure employment (10:24).

Integrated control enablers are critical capabilities required to execute successful operations and produce integrated effects throughout all war fighting domains (10:39). Integrated control enabler capabilities are used to gain, exploit, and disseminate quality information and support effective C2 (10:39). Integrated control enablers support the commander's ability to find, fix, track, target, engage, and assess adversary and friendly activities throughout the battlespace thus supporting effective decision making (10:39). Integrated control enablers (see Figure 8.) include: intelligence, surveillance, and reconnaissance, network operations, predictive battlespace awareness, and precision navigation and timing (10:39).

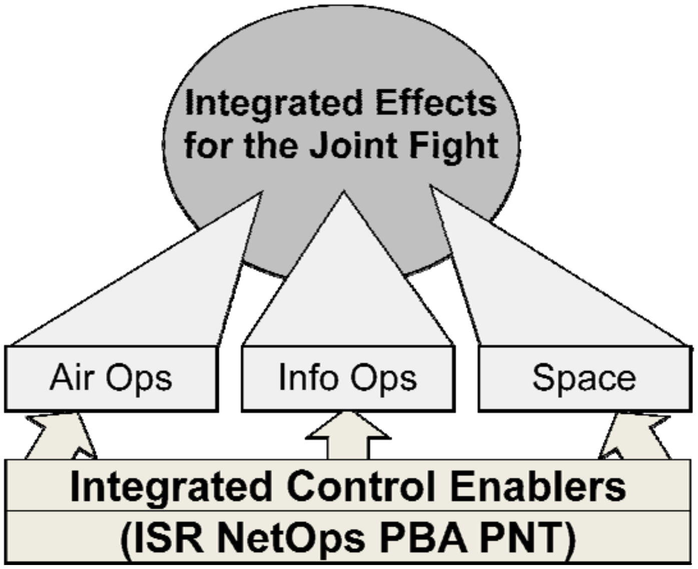

Integrated Effects for the Joint Fight
Air Ops
Info Ops
Space
Integrated Control Enablers
(ISR NetOps PBA PNT)

Figure 8. Integrated Control Enablers (10:40)

Intelligence, surveillance, and reconnaissance activities enable decision makers to accurately conceptualize the battlespace and exploit adversary vulnerabilities (10:40). Intelligence, surveillance, and reconnaissance operations include the integrated capabilities to task, collect, process, exploit, and disseminate quality intelligence information (10:40). Network operations are conducted to ensure all warfighting domain operations are unimpeded by friendly or adversary network activities (10:39).

Network operations consists of organizations, procedure, and functionalities required to plan, administer, and monitor networks in support of operations and to respond to threats, vulnerabilities, and outages that effect operational network capabilities (10:39).

Predictive battlespace awareness operations provide a knowledge of the operational environment that allows commander's to effectively execute C2 in the various war fighting domains (10:40). Predictive battlespace awareness provides a methodology that enables commanders to integrate all available intelligence, surveillance, and reconnaissance assets in order to maximize their ability to predict enemy courses of action and select friendly course of action (10:40). Developing a predictive battlespace environment requires the development and integration of: intelligence preparation of the battlespace, target development, intelligence, surveillance, and reconnaissance strategy and planning, intelligence, surveillance and reconnaissance employment, and assessment (10:40).

Precision navigation and timing are utilized to synchronize the integration of military capabilities (10:40). The precision navigation and timing provided by space-based assets are essential to enabling the ability to integrate and coordinate war fighting capabilities to create effects across the various war fighting domains (10:40).

Air Force Cyber Command

The United States' must develop the capability to protect and dominate cyberspace because the majority of the nation's neural networks reside in the cyber domain (9:2). The increasing dependence on communications capabilities and electronics used throughout the electromagnetic spectrum has led to the Joint Chiefs of Staff's recognition of cyberspace as a warfighting domain that is of equal importance to national security as the traditional domains and the addition of cyberspace into the Air Force mission statement (8:ii, 7:1). The mission of the Air Force is currently "to deliver sovereign options for the defense of the United States of America and its global interests - to fly and fight in air, space, and cyberspace" (8:ii). Air Force Cyber Command was established to meet this mission requirement and develop offensive and defensive cyber capabilities that would redefine airpower by extending the Air Force's global vigilance, reach, and power into cyberspace (8:ii).

The mission of the Air Force Cyber Command is to provide combat ready forces trained and equipped to conduct offensive and defensive cyber operations in support of national objectives (8:ii). Warfighting concepts must be developed for forces to operate in the cyberspace domain and conduct combat operations (8:1). Capabilities in the cyberspace domain will advance the airpower concepts of global reach and global power into cyberspace (8:1).

As previously noted, goals play a critical role in the identification C2 information requirements. Accordingly, the Air Force has stated explicit goals for a commander operating in cyberspace (8:4). Specifically leaders should achieve cyberspace superiority where superiority is defined as "the freedom to operate in the cyberspace domain while denying that same freedom to an adversary" (8:5). Achieving superiority in cyberspace is critical to maintaining the American military's unique advantages in precision engagement, situational awareness, and operational reach (8:5). The Air Force identified the following end states for cyberspace superiority (8:4):

- Deter and prevent cyberspace attacks against vital US interests (i.e., counter cyber operations)
- Rapidly respond to attacks and reconstitute networks
- Integrate cyber power into the full range of global and theater effects
- Defeat adversaries operating through cyberspace
- Freedom of action in cyberspace for US & Allied commanders
- Persistent cyberspace situational awareness

To achieve these end states the Air Force must: develop doctrine, organize, train, and equip cyber forces to enable successful cyber operations across the full spectrum of conflict (8:4).

Counter cyber operations must be effectively conducted to achieve cyber superiority (8:6). Counter cyber operations consist of offensive counter cyber and, defensive counter cyber missions (8:6). Offensive and defensive counter cyber missions are conducted to achieve specific military effects in the cyber domain resulting in cyber superiority by protecting friendly cyber capabilities and destroying, degrading, or disrupting the enemy's cyber capability (8:6).

Offensive counter cyber operations are conducted to deny, degrade, disrupt, destroy, or deceive the enemy's cyber capability (8:6). Offensive counter cyber operations can produce effects that directly impact our adversary's ability to wage war (8:6). Attacking and destroying an enemy's communications network is an example of an offensive counter cyber operation. Defensive counter cyber operations are conducted to protect friendly forces and vital national interests from cyber attacks (8:6). Defensive counter cyber operations preserve, protect, recover, and restore friendly cyber capabilities before, during, and after an attack (8:6). Protecting communications channels with intrusion detection systems is an example of defensive counter cyber operations.

For the purpose of this research, C2 of cyberspace is considered to be in a deployed operational environment. The Air Force operates an Air Operations Center (AOC) to perform C2 of deployed regional operations (11:105). The AOC is "the operations command center for the Joint Forces Air Component Commander (JFACC) and provides the capability to plan, task, execute, monitor, and assess the activities of assigned or attached forces" (11:105). The AOC integrates numerous disciplines in a cross-functional team to plan and execute a full range of joint air and space capabilities (11:105). Each capability represented in the AOC has an individual who serves as the principle advisor to the JFACC and the highest level of C2 for the military capability they represent. The Director of Cyberspace Forces will serves as the senior advisor to the JFACC within an operational war fighting environment for issues associated with the cyberspace domain. The Director of Cyberspace Forces is the highest level of C2 for Air Force operations in cyberspace and is responsible for tailoring cyber operations, effects, and coalition support (8:15).

The effectiveness of the Director of Cyberspace Forces is highly dependent on having detailed knowledge of the ever-changing cyber environment and adversary's C2 capabilities (8:9). The Director of Cyberspace Forces must have an extensive understanding of cyber-related constraints, capabilities, and activities to accurately target and assess cyberspace. The Director of Cyberspace Forces must also be able to operate throughout the cyber domain and be able to integrate cyber capabilities with traditional domain operations to deliver global effects (8:11). The complex and rapidly evolving operational environment of cyberspace will have a wider variety of C2 information requirements than the traditional warfighting domains. Warfare in the cyber domain is a new concept and there are currently no methodologies for identifying the critical information requirements that will enable the Director of Cyberspace Forces to effectively C2 the domain.

Exercising C2 over the cyberspace domain is going to be a daunting task because of the myriad of cyber data streams and information that is available. Every electronic device throughout the electromagnetic spectrum is a potential source of C2 information. The Director of Cyberspace Forces will need to maintain situational awareness of a complex variety of operational elements in the cyberspace domain to effectively exercise C2. The Director of Cyberspace Forces situational awareness requirements will need to enable effective C2 of the following areas (8:3):

- Internet protocol based terrestrial
- Wireless networks
- Airborne transmission systems
- Space transmission networks
- Non-internet protocol based networks
- Data links
- Telephone networks
- Control systems
- Electronic attack
- Directed energy
- Electronic protection

Information Requirements Analysis

Information requirements analysis is a process of determining the essential elements of information that will support effective C2 decision making and not overwhelm the decision maker (21:1). Conducting an information requirements analysis is an essential function for each warfighting domain that enables the commander's visualization of the battlespace and conception of an operations strategy (5:3). The information requirements must include information that identifies both threats and opportunities effecting national interests (5:3). Methods for identifying information requirements must be tailored for each domain to provide commanders with situational awareness of their unique warfighting domain.

Information requirements analysis methods generally fall into two categories. The first category determines the information requirements of the organization (warfighting domain) and the second category determines the information requirements for an information system (21:1). Studies have shown that methods for determining the information requirements for an information system are not suitable for determining the information requirements of an organization. The information requirements analysis methods for an information system do not identify decision quality information that is required for effective decision-making. The remainder of this research effort will focus on methodologies for determining the information requirements for C2 of a warfighting domain.

Organizational information requirements analysis methods identify information that is precise, purposeful, and beneficial to give the largest degree on information awareness to decision makers (1:THB 1/27). Several methods have been outlined. First, the Bayesian decision-making method, called "extending the discussion," can lead to the identification of information requirements (20:73-106). The method breaks a situation down into sub-cases until the decision maker is able to interpret the situation and make an informed decision (1:THB: 1/29). Extending the discussion leads to the discovery of information requirements that are required to support decision making for each of the sub-cases (1:THB 1/29). Second, Endsley proposed a method that employs goal-directed task analysis to identify information requirements for organizational decision-making. This requires identification of the major goals of an activity, along with pertinent sub goals needed to meet each goal. The steps of Endsley's goal-directed task analysis method for determining C2 information requirements are identified in Table 1 (14:8). The desired result is to identify the information that is required to provide adequate situational awareness to accomplish each sub goal and primary goal that was identified. Endsley focused on goals because he believed that goals form the basis for decision making in complex operational environments (14:8).

Table 1. Endsley's Information Requirements Analysis Method (14:8)

Goal-Directed Task Analysis	
Step 1.	Identify primary missions and goals.
Step 2.	Identify sub-goals that support primary mission and goals.
Step 3.	Identify information required to achieve goals.

Finally, Yadav proposed the organizational analysis and requirements specification method to identify organizational information requirements. Consistent with Endsley, Yadav starts from the top with an analysis of the organization's mission (goals). Fundamental aspects of Yadav's organizational analysis and requirements specification method are detailed in Table 2 (21:17). The organizational structure is analyzed to determine how each part of the organization contributes to mission accomplishment (21:17). This analysis allows for the identification of functions that must be performed in each part of the organization to accomplish the mission. The functional requirements serve as the baseline for determining information requirements and information characteristics of each level of the organization to support decision making and accomplish the mission (21:17).

Table 2. Yadav's Information Requirements Analysis Method (21:17)

Step 1.	Do aggregate structural analysis a. Describe organization missions and goals. b. Describe operating core. c. Describe structural configuration.
Step 2.	Do broad functional analysis a. Describe major functional organizational strategies, goals and measures of performance. b. Describe functional structure. c. Describe major organization systems used for integration.
Step 3.	Do detailed analysis of the organizational functions a. Describe function goals and measures of effectiveness for functions to be supported. b. Describe sub-functional units and structures. c. Describe functional systems.
Step 4.	Analyze managerial functions to be supported a. Determine broad categories of managerial activities. b. Determine managerial roles under major activities. c. Identify actions to be supported under each managerial activity.

The Department of Defense has also developed a method for identifying information requirements in Joint Publication 3-0 *Joint Operations*. This method depicted in Figure 9 captures information requirements in the context of the mission, commander’s intent, and concept of operations (5:III-3, 13). It incorporates the methods outlined by Endsley and Yadav where goals serve as the central guiding feature of all information requirements analysis. The key elements identified during this method are referred to as the Commander’s Critical Information Requirements (CCIRs) (5:III-11). The CCIRs include Priority Intelligence Requirements (PIRs) and Friendly Forces Information (FFI) (5:III-11). PIRs drive the intelligence collection process and include information about the adversary and the operating environment (5:III-11). FFIs include the operational capabilities of friendly forces (5:III-11). The CCIRs must define the situation, identify the actors (friendly and adversary), and identify strengths, weaknesses, and capabilities of all actors (5:II-20). The lack of tactics techniques and procedures combined with the non-physical nature of the cyberspace domain will make the identification of the CCIRs a difficult task for cyberspace commanders.

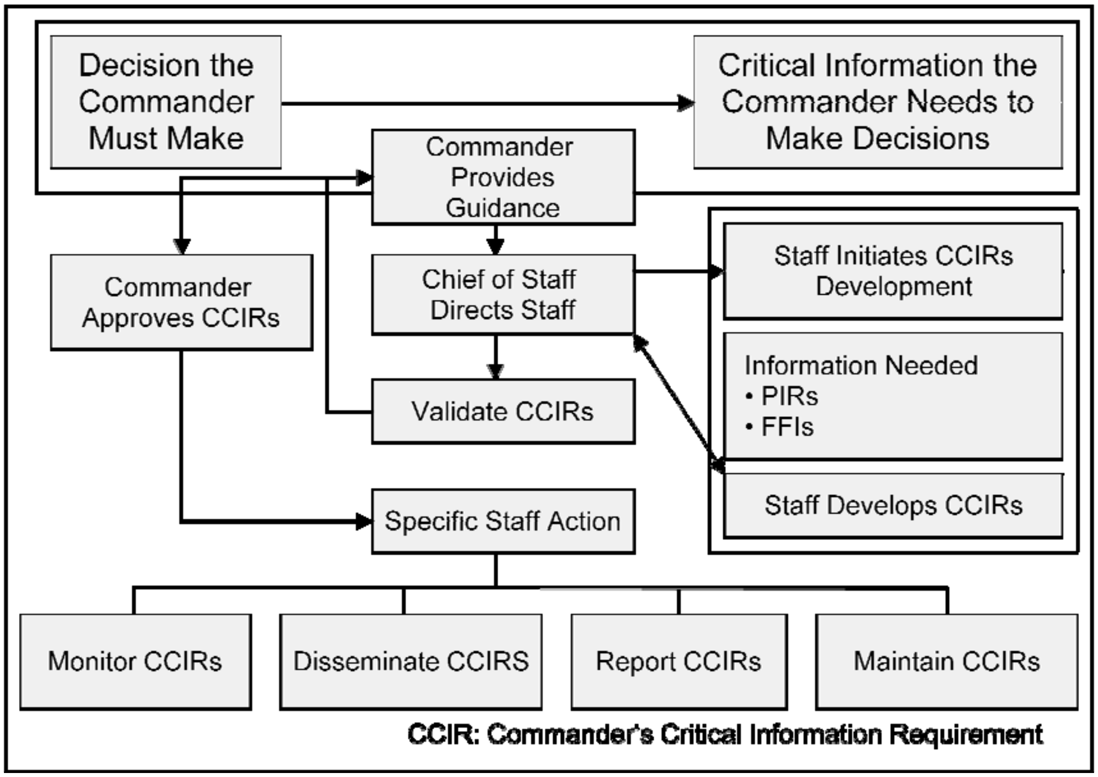

Decision the Commander Must Make
Critical Information the Commander Needs to Make Decisions
Commander Provides Guidance
Commander Approves CCIRs
Chief of Staff Directs Staff
Staff Initiates CCIRs Development
Information Needed
• PIRs
• FFIs
Validate CCIRs
Staff Develops CCIRs
Specific Staff Action
Monitor CCIRs
Disseminate CCIRS
Report CCIRs
Maintain CCIRs
CCIR: Commander's Critical Information Requirement

Figure 9. CCIR Process (5:III-3)

The Joint Intelligence Preparation of the Battlespace (JIPB) process is used to identify and collect PIRs. The questions asked during the JIPB process are also useful in indentifying FFIRs. The JIPB process depicted in Figure 10 includes four steps that ensure the systematic analysis of the environment and adversary (6:II-1). The JIPB process is both continuous and cyclical to ensure CCIRs are accurate at all stages of executing an operational mission (6:II-1). The four steps of the JIPB process are: Step 1: define the battlespace environment, Step 2: describe the battlespace's effects, Step 3: evaluate the adversary, Step 4: determine adversary course of action (6:II-1). The elements of each step of the JIPB process are listed in Table 3 (6:II-3, II-9, II-45, II-54).

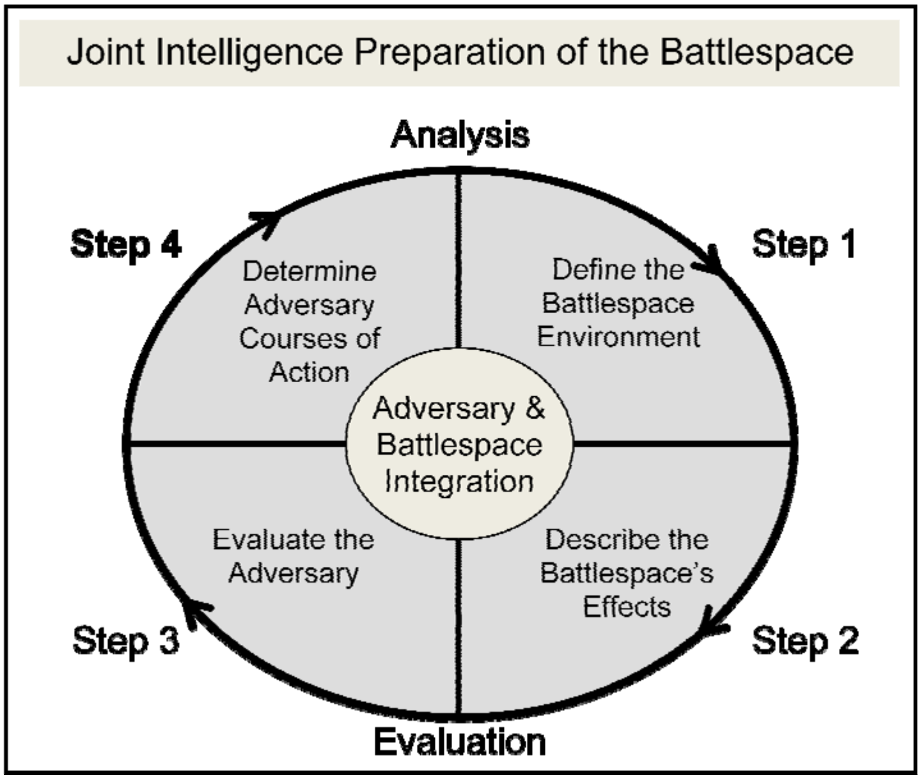

Joint Intelligence Preparation of the Battlespace
Analysis
Step 4
Step 1
Determine Adversary Courses of Action
Define the Battlespace Environment
Adversary & Battlespace Integration
Evaluate the Adversary
Describe the Battlespace's Effects
Step 3
Step 2
Evaluation

Figure 10. JIPB Process (6:II-1)

Table 3. Steps of the Joint Intelligence Preparation of the Battlespace Process (6:II-3, II-9, II-45, II-54)

Step 1. Define the Battlespace Environment

a. Identify the limits of the joint force's operational area
b. Analyze the joint force's mission and joint force commander's intent
c. Determine the significant characteristics of the joint force's operational area
d. Establish the limits of the joint force's areas of interest for each geographic battlespace dimension

e. Determine the full, multi-dimensional, geographic and non-geographic spectrum of the joint force's battlespace
f. Identify the amount of battlespace detail required and feasible within the time available
g. Evaluate existing data bases and identify intelligence gaps and priorities
h. Collect the material and intelligence required to support further JIPB Analysis.

Step 2. Describe the battlespace effects

a. Analyze the battlespace environment
b. Describe the battlespace's effects on adversary and friendly capabilities and broad courses of action

Step 3. Evaluate the adversary

a. Identify adversary centers of gravity
b. Update or create adversary models
c. Determine the current adversary situation
d. Identify adversary capabilities

Step 4. Determine adversary courses of action

a. Identify the adversary's likely objectives and desired end state
b. Identify the full set of courses of action available to the adversary
c. Evaluate and prioritize each course of action
d. Develop each course of action in the amount of detail time allows
e. Identify initial collection requirements

Summary

This chapter provided background information about C2 information requirements for the Director of Cyberspace Forces. Cyberspace was defined as a warfighting domain that encompasses all electronic equipment operating throughout the electromagnetic spectrum. The role of information in C2 was then discussed to demonstrate the importance of timely and accurate information for achieving effective C2. In addition, information in the traditional warfighting domains was analyzed to highlight information in physical warfighting domains as well as the information domain. Next, Air Force Cyber Command's mission and structure was analyzed to highlight the unique information requirements of a complex and non-physical cyber domain. Finally, information requirements analysis methods were analyzed to potentially determine the C2 information requirements of the Director of Cyberspace Forces. Effective C2 of cyberspace will require development of a valid method for determining the C2 information requirements. The remainder of this research will focus on developing a hybrid methodology for identifying the C2 information requirements of the Director of Cyberspace Forces.

III. Methodology

Overview

A content analysis of C2 research, military C2 doctrine, situational awareness research, information requirements analysis research, and Air Force cyberspace documents was conducted to develop a method for identifying C2 information requirements for the cyberspace domain. The method for determining the C2 information requirements for the Director of Cyberspace Forces will be developed in three phases. The assigned missions and goals of the cyberspace domain will be identified in phase one. A hybrid information requirements analysis method will be constructed during phase two. Finally, during phase three, the hybrid information requirements analysis method will be modified to demonstrate how it can be configured to enable identification of C2 information requirements for achieving goals at either the strategic, operational, or tactical levels of war.

Phase One

The purpose of Phase One of this research is to identify the missions, goals, and operations areas associated with cyberspace. Identifying the missions, goals, and operations areas of cyberspace is the first step in identifying the information required to achieve them. The *Air Force Cyber Warfare Operational Concept* will serve as the primary source for identifying missions and goals of the cyberspace domain. Air Force Doctrine Document 2-5 *Information Operations* will also used to identify potential missions and goals of cyberspace because the types of missions and operational functions associated with information operations are very similar to the types of missions and operational functions that will be conducted in cyberspace.

Phase One will be accomplished in two steps. The first step is to identify the Air Force's overarching missions and goals of cyberspace and information operations. This step is required to facilitate the identification of sub-goals that are required to support effective operations in cyberspace later on in the information requirements analysis process. The second step is to categorize the subordinate missions, goals, and operations areas of cyberspace and information operations into offensive, defensive, and support categories. This step is necessary to enable decision makers to identify information requirements in association with the category of goal they are attempting to accomplish.

Step One.

The purpose of step one is to identify the Air Force's primary missions and goals associated with cyberspace and information operations. The overarching mission and supporting goals associated with cyberspace will be extracted from the *Air Force Cyber Warfare Operational Concept*. The *Air Force Cyber Warfare Operational Concept* will also be analyzed to identify all subordinate missions, goals, end states and operations areas that are associated with the overarching mission and goals. The overarching mission and supporting goals associated with information operations will be extracted from Air Force Doctrine Document 2-5 *Information Operations*. Air Force Doctrine Document 2-5 *Information Operations* will also be analyzed to identify all subordinate missions, goals, end states, and operations areas associated with information operations.

This step is critical to the identification of information that is required to support mission and goal achievement in cyberspace and information operations.

Step Two.

The purpose of this step is to categorize the subordinate missions, goals, and operations areas of cyberspace and information operations into offensive, defensive, and support categories. During this step, cyber warfare operations will be incorporated along with information operations into one comprehensive list to ensure all operations are accounted for. The *Air Force Cyber Warfare Operational Concept* and Air Force Doctrine Document 2-5 *Information Operations* will be analyzed to identify the types of operations that must be conducted to accomplish the missions, goals, sub-goals, and end states identified in step one and determine requirements for the offensive, defensive, and support categories. Once the requirements of the categories are determined, each of the missions, goals, sub-goals, and end states identified in step one will be assigned to the appropriate offensive, defensive, or support category.

Phase Two

The purpose of Phase 2 is to develop a hybrid information requirements analysis method that utilizes aspects of methods developed by Endsley and the Department of Defense. The steps taken to create the hybrid information requirements analysis method will be accomplished to build validity into the cyberspace C2 information requirements analysis process. Endsley's three-step goal-directed information requirements analysis method will serve as the baseline for the hybrid method. The primary missions and goals will be identified in Step 1. Sub-goals that support higher-level goals will identified in step two. The Department of Defense's CCIR process will be accomplished in Step 3 of the hybrid information requirements analysis method. The hybrid information requirements analysis method developed in this research will be in the form of a template.

During Step 1, the primary goals associated with operations in cyberspace will be identified. Step 1 of the hybrid information requirements analysis method template will require users to insert a goal in the corresponding Step 1 goal section.

Step 2 of the hybrid information requirements analysis method will require the identification of an appropriate sub-goal with higher-level goal identified in Step 1. For example: Deterring cyberspace attacks against vital US interests is a sub-goal of the primary goal of achieving cyber superiority. Step 2 of the hybrid information requirements analysis method template will require users to insert an appropriate sub-goal in the corresponding Step 2 sub-goal section.

Step 3 of the hybrid information requirements analysis method will incorporate the Department of Defense's CCIR process. Principles of JIPB will be utilized to add validity to the CCIR process and ensure the information gathered is adequate for achieving military objectives. The JIPB process will be employed to solicit quality C2 information that will enable the Director of Cyberspace Forces to make effective decisions. A list of questions that correspond with JIPB process requirements will be developed to solicit both PIRs and FFIs. The four steps of the JIPB will be combined into one group of questions that corresponds with JIPB process requirements. The JIPB and corresponding questions will be divided on the template into PIRs and FIRs. Step 3 of the hybrid information requirements analysis method template will list PIRs and FIRs and associated JIPB process questions. Users will be required to answer the questions associated with the PIRs and FFIs to collect the required C2 information.

Phase Three

The purpose of Phase Three will be to demonstrate how the hybrid information requirements analysis method template can be modified to identify C2 information required to achieve goals at either the strategic, operational, or tactical level of war. There are no modifications required for Steps 1 and 2. The JIPB's supporting questions in Step 3 of the hybrid information requirements analysis method will be modified to solicit increasingly more detailed information to support achieving more detailed goals.

The hybrid information requirements analysis template will be modified three times. The first time, the template will be modified to solicit information requirements necessary to achieve strategic level of war goals. A strategic level of war goal will be input in step one of the method. A corresponding sub-goal will be input in step two of the method. The CCIR questions that correspond with the JIPB process requirements will be modified to support achievement of a strategic level of war goal in step three of the method.

The second time, the template will be modified to solicit information requirements necessary to achieve operational level of war goals. An operational level of war goal will be input in step one of the method. A corresponding sub-goal will be input in step two of the method. The CCIR questions that correspond with the JIPB process requirements will be modified to support achievement of an operational level of war goal in step three of the method.

The final time, the template will be modified to solicit information requirements necessary to achieve tactical level of war goals. A tactical level of war goal will be input in step one of the method. A corresponding sub-goal will be input in step two of the method. The CCIR questions that correspond with the JIPB process requirements will be modified to support achievement of a tactical level of war goal in step three of the method.

The information requirements analysis method developed in this chapter will provides a template for meeting the C2 information needs of the Director of Cyberspace Forces. The level of detail required to achieve specific goals will change as the goals do. The hybrid information requirements analysis template will serve as a starting point for determining the information requirements of the Director of Cyberspace Forces to facilitate effective C2 of cyberspace.

IV. Analysis and Results

The purpose of this chapter is to develop an information requirements analysis method that will meet the C2 information needs of the Director of Cyberspace Forces. The literature review and content analysis of C2 research, military C2 doctrine, situational awareness research, information requirements analysis research, and Air Force cyberspace doctrine provides a framework for identifying the C2 information requirements of the Director of Cyberspace Forces. The information requirement analysis method is developed in three phases. Cyberspace missions and goals are identified in phase one. A hybrid information requirements analysis method is developed in phase two. In phase three, the hybrid information requirements analysis method is modified to demonstrate how it can be used to identify C2 information requirements for achieving goals at either the strategic, operational, or tactical level of war.

Phase One

The purpose of Phase One of this research is to identify the missions, goals, and operations areas associated with cyberspace. Identifying the missions, goals, and operations areas of cyberspace is the first step in identifying the information required to achieve them. The *Air Force Cyber Warfare Operational Concept* serves as the primary source used to identify the missions, goals, and requirements for cyberspace. Air Force Doctrine Document 2-5 *Information Operations* was also used to identify potential missions and goals of cyberspace because information operations already has well developed operational doctrine and both information operations and cyber operations are executed across and throughout the traditional domains to achieve desired effects (10:1).

Phase One is accomplished in two steps. The first step is to identify the Air Force's overarching missions and goals for cyberspace and information operations. The second step is to categorize the subordinate missions, goals, and operations areas of cyberspace and information operations into offensive, defensive, and support categories.

Step One.

The purpose of Step One is to identify the Air Forces' overarching missions and goals of cyberspace and information operations. The Air Force mission in cyberspace is to redefine airpower by extending the Air Force's global vigilance, reach, and power into the cyberspace domain (8:ii). This mission statement serves as the starting point for determining subordinate missions, goals, and operations areas that are required to support accomplishment of the Air Force's mission in cyberspace.

The primary goal associated with the Air Force's mission in cyberspace is to achieve cyber superiority. Achieving cyber superiority requires ensuring our ability to operate freely in cyberspace while denying the ability to operate freely in cyberspace to our adversary (8:5). The end state goals of cyber superiority are (8:4).

- Deter and prevent cyberspace attacks against vital US interests
- Rapidly respond to attacks and reconstitute networks
- Integrate cyber power into the full range of global and theater effects
- Defeat adversaries operating through cyberspace
- Freedom of action in cyberspace for US & Allied commanders
- Persistent cyberspace situational awareness

The Air Force Information Operations Mission is to integrate the employment of capabilities of influence operations, electronic warfare operations, and network warfare operations, in concert with specified integrated control enablers, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own. The primary goal associated with the Air Force's mission in information operations is to achieve information superiority. Information superiority is a degree of dominance in the information domain, which allows friendly forces the ability to collect, control, exploit and defend information without effective opposition.

Step Two.

The purpose of Step Two is to categorize the missions, goals, and operations areas of cyberspace and information operations into offensive, defensive, and support categories. Cyber warfare operations are incorporated with information operations to ensure a robust spectrum of operations is accounted for. The incorporated operations are then assigned to an offensive, defensive, or support category. *The Air Force Cyber Warfare Operational Concept* states that cyber superiority is achieved through the successful execution of counter cyber operations (8:8). Counter cyber operations consist of offensive and defensive counter cyber operations (8:8). Cyber warfare support is conducted to ensure the survivability and sustainability of the cyber infrastructure, oversee cyber weapons system development, and cyber force development.

Air Force Doctrine Document 2-5 *Information Operations* divides both electronic and network warfare into offensive, defensive, and support operations. The support category of information operations is defined more clearly than cyber warfare support and is used in this analysis to provide more structure to the cyber warfare support operations. The integrated control enabler component of information operations is also incorporated into the cyber warfare support function because it encompasses the types of support requirements that facilitate extending cyber capabilities across the traditional war fighting domains.

Offensive Counter Cyber Operations.

Offensive counter cyber operations includes electronic attack and network attack and are conducted against personnel, facilities, equipment, radio networks, satellite networks, radar networks, data links, telemetry, digital track files, telecommunications networks, and wireless communications networks. The goal of offensive counter cyber operations is to deny, degrade, disrupt, destroy, deceive, corrupt, or usurp the adversary’s cyber capabilities. Table 4 represents a comprehensive list of missions and goals of offensive counter cyber operations.

Table 3. Offensive Counter Cyber Operations

Offensive Counter Cyber Operations
Mission • Attack the adversary’s   • Personnel   • Facilities   • Equipment   • Data Networks   • Radio Networks   • Satellite Networks   • Radar Networks   • Data Links   • Telemetry   • Digital Track Files   • Telecommunications Networks   • Wireless Communications Networks

Goals • Deny • Degrade • Disrupt • Destroy • Deceive • Corrupt • Usurp The adversary’s cyber capabilities

Defensive Counter Cyber Operations.

Defensive counter cyber operations include electronic protection and network defense and are conducted to protect friendly forces, facilities, equipment, and vital interests from an adversary’s cyber attack. The goals associated with of defensive counter cyber operations are to preserve, protect, detect, react to internal and external attacks, determine the nature of cyber threats, recover, reconstitute friendly cyber capabilities before, during, and after an adversary attack, and develop defensive courses of actions. Table 5 represents a comprehensive list of missions and goals of defensive counter cyber operations.

Table 4. Defensive Counter Cyber Operations

Defensive Counter Cyber Operations
Mission • Protect friendly: o Personnel o Facilities o Equipment o Data Networks o Radio Networks o Satellite Networks o Radar Networks o Data Links o Telemetry o Digital Track Files o Telecommunications Networks o Wireless Communications Networks

From an adversary's cyber attack
Goals • Preserve • Protect • Detect • React to internal and external attacks • Determine the nature of cyber threats • Recover • Reconstitute friendly cyber capabilities before, during, and after an adversary attack Against the adversary's cyber warfare attack capabilities
Output • Defensive courses of action To respond to potential a potential cyber attack

Cyber Warfare Support Operations.

Cyber warfare support operations include electronic warfare support, network warfare support, and integrated control enablers. Cyber warfare support operations cover a broad range of activities including: collection of electromagnetic data for immediate tactical applications, collection and production of network related data, electromagnetic spectrum de-confliction, vulnerability assessment, crypto logical planning and de-confliction, intelligence collection, processing, exploitation and dissemination, network operations, parametric data reflecting electronic characteristics of various electronic warfare threat systems, characteristics of threat and target systems, network profiling, event analysis, open source review, and the identification of potential vulnerabilities in the adversaries cyber systems predictive battlespace awareness and precision navigation and timing. The goals associated with cyber warfare support operations are to find, fix, track, target, engage, assess the adversary's cyber capabilities and assess vulnerabilities in friendly cyber capabilities. Products produced within cyber warfare support operations include: cyber order of battle, electronic order of battle, and network order of battle.

Table 6 represents a comprehensive list of missions and goals of cyber warfare support operations.

Table 5. Cyber Warfare Support Operations

Cyber Warfare Support Operations
Missions • Collect electromagnetic data for immediate tactical applications • Collect and produce network related data • Network profiling • Event analysis • Network operations • Electromagnetic spectrum de-confliction • Vulnerability assessment of friendly and adversary cyber systems • Crypto logical planning and de-confliction • Intelligence collection, processing, exploitation, and dissemination • Characteristics of threat and target systems • Determine electronic characteristics of various electronic warfare threat systems • Develop predictive battlespace awareness • Precision navigation and timing
Goals • Find • Fix • Track • Target • Engage • Assess The adversary’s cyber warfare capabilities • Assess • Maintain Friendly cyber capabilities
Output • Cyber order of battle o Electronic order of battle o Network order of battle

Phase Two

The purpose of Phase 2 is to develop a hybrid information requirements analysis method that utilizes aspects of methods developed by Endsley and the Department of Defense. Endsley's three-step goal-directed information requirements analysis method serves as the baseline for the hybrid method. Primary missions and goals are identified in Step 1. Sub-goals that support higher-level goals are identified in Step 2. The Department of Defense's CCIR process replaces Step 3 of Endsley's method (see Table 7).

Table 6. Hybrid Information Requirements Analysis Method

	Hybrid Information Requirements Analysis Method
Step 1.	Identify primary missions and goals.
Step 2.	Identify sub-goals that support primary missions and goals.
Step 3.	Identify the Commander Critical Information Requirements.

Actions required in Step 1 of the hybrid information requirements analysis method were accomplished in Phase One of this chapter. Step 2 of the hybrid information requirements analysis method requires information gatherers to associate an appropriate sub-goal with the primary and goal that was identified in Step 1. For example: Deterring cyberspace attacks against vital US interests is an appropriate sub-goal of the primary goal of achieving cyber superiority. Determining the sub-goals will be a recurring process until the correct level of granularity is achieved to identify information requirements that support the various levels of C2 decision that must be made.

Step 3 of the hybrid information requirements analysis method employs the Department of Defense's CCIR process. Principles of the JIPB process are utilized to add rigor to the CCIR process and ensure the information gathered is adequate for achieving military objectives. The JIPB process requirements and corresponding questions listed in Table 8 represent the level of detail required to provide the Director of Cyberspace Forces with C2 information and support effective decision-making.

Table 7. JIPB Process Requirements and Supporting Questions

JIPB Process Requirements	**Supporting Questions**
1. Define the battlespace environment • Identify the limits of the joint force's operational area • Analyze the joint force's mission and joint force commander's intent • Determine the significant characteristics of the joint force's operational area	PIRs • Who is the adversary? • What are the adversary's strategic and operational objectives? FFIs • What are the limits of the joint force's operational area? • What is the joint forces' mission? • What is the joint forces commander's intent? • What are our strategic and operational objectives?
2. Describe the battlespace's effects. • Describe the battlespace's effects on adversary and friendly capabilities and broad courses of action	PIRs • How does the adversary operate in cyberspace? • How does the adversary utilize cyber assets to achieve effects throughout other warfighting domains? • What elements of the physical environment limit cyberspace capabilities? • How does the adversary defend its cyber capabilities? FFIs • What are our limitations to cyberspace operations in this physical environment? • What cyber effects are available to attack the adversary's cyber defenses?
3. Evaluate the adversary.	PIRs

• Identify adversary centers of gravity • Identify adversary capabilities	• What are the adversary’s strategic and operational cyber centers of gravity? • What are the adversary’s offensive cyber capabilities? • What are the adversary’s defensive cyber capabilities? <u>FFIs</u> • What are our strategic and operational cyber centers of gravity? • What are our offensive cyber capabilities? • What are our defensive cyber capabilities?
4. Determine adversary COAs. • Identify the adversary's likely objectives and desired end state • Identify the full set of courses of action available to the adversary • Identify the adversary’s objectives • Identify the COAs available to the Adversary • Identify the adversary’s capabilities • Identify the adversary’s vulnerabilities	<u>PIRs</u> • What is the adversary’s desired end state? • What COAs are available to the adversary? • What are the adversary’s cyber capabilities? • What are the adversary’s cyber vulnerabilities? <u>FFIs</u> • What is our desired end state? • What COAs are available to us? • What are our cyber capabilities? • What are our cyber vulnerabilities?

A template for determining the C2 information requirements of the Director of Cyberspace Forces was developed to ensure the information gathered supports achieving the identified sub-goal and that the sub-goal is associated with the appropriate overarching goal (see Figure 11).

Cyberspace Information Requirements Analysis Method	
Step 1. Goal Identification	
Goal:	Goal?
Step 2. Sub-Goal Identification	
Sub-Goal:	Sub-Goal?
Step 3. Determine CCIRs	
PIRs	a. Who is the adversary? b. What are the adversary’s strategic and operational objectives? c. How does the adversary operate in cyberspace? d. How does the adversary utilize cyber assets to achieve effects throughout other warfighting domains? e. What elements of the physical environment limit cyberspace capabilities? f. How does the adversary defend its cyber capabilities? g. What are the adversary’s strategic and operational cyber centers of gravity? h. What are the adversary’s offensive cyber capabilities? i. What are the adversary’s defensive cyber capabilities? j. What is the adversary’s desired end state? k. What COAs are available to the adversary? l. What are the adversary’s cyber vulnerabilities?
FFIs	a. What are the limits of the joint force’s operational area? b. What is the joint forces’ mission? c. What is the joint forces commander’s intent? d. What are our strategic and operational objectives? e. What are our limitations to cyberspace operations in this physical environment? f. What cyber effects are available to attack the adversary’s cyber defenses? g. What are our strategic and operational cyber centers of gravity? h. What are our offensive cyber capabilities? i. What are our defensive cyber capabilities? j. What is our desired end state? k. What COAs are available to us? l. What are our cyber vulnerabilities?

Figure 11. Cyberspace Information Requirements Analysis Method

Phase Three

The purpose of Phase Three is to demonstrate how the hybrid information requirements analysis method can be modified to identify C2 information required to achieve goals at either the strategic, operational, or tactical level of war. There are no modifications required for Steps 1 and 2. Step 3 of the hybrid information requirements analysis method must be modified to require increasingly more detailed information to support achieving goals that are more detailed.

Figure 12 represents the hybrid information requirements analysis method that is configured to support C2 information requirements at the strategic level of war. The information requirements analysis method template developed in phase two represents information requirements for the strategic level of war. As such, no modifications are made to Step 3 of the method.

Cyberspace Information Requirements Analysis Method	
Step 1. Goal Identification	
Goal:	Achieve Cyber Superiority
Step 2. Sub-Goal Identification	
Sub-Goal:	Defeat adversaries operating through cyberspace
Step 3. Determine CCIRs	
PIRs	a. Who is the adversary? b. What are the adversary's strategic and operational objectives? c. How does the adversary operate in cyberspace? d. How does the adversary utilize cyber assets to achieve effects throughout other warfighting domains? e. What elements of the physical environment limit cyberspace capabilities? f. How does the adversary defend its cyber capabilities? g. What are the adversary's strategic and operational cyber centers of gravity? h. What are the adversary's offensive cyber capabilities? i. What are the adversary's defensive cyber capabilities? j. What is the adversary's desired end state? k. What COAs are available to the adversary?

	l. What are the adversary’s cyber vulnerabilities?
FFIs	a. What are the limits of the joint force’s operational area? b. What is the joint forces’ mission? c. What is the joint forces commander’s intent? d. What are our strategic and operational objectives? e. What are our limitations to cyberspace operations in this physical environment? f. What cyber effects are available to attack the adversary’s cyber defenses? g. What are our strategic and operational cyber centers of gravity? h. What are our offensive cyber capabilities? i. What are our defensive cyber capabilities? j. What is our desired end state? k. What COAs are available to us? l. What are our cyber vulnerabilities?

Figure 12. Cyberspace Information Requirements Analysis Method Configured for Strategic Level Information Requirements

Figure 13 represents the hybrid information requirements analysis method that is configured to support C2 information requirements at the operational level of war. The primary goal (Step 1) in this example is eliminate surveillance radar capability in Country X. The sub-goal (Step 2) in this example is to destroy the communications connectivity between the four surveillance radar sites in Country X. The PIRs and FFIs in Step 3 are more detailed to support achieving these goals. The modifications are printed in bold italic (***bold italic***) to highlight modifications. This operational level of warfare information requirements analysis method can be compared to Figure 11 to see modifications.

Cyberspace Information Requirements Analysis Method	
Step 1. Goal Identification	
Goal:	Eliminate surveillance radar capability in Country X
Step 2. Sub-Goal Identification	
Sub-Goal:	Destroy the communications connectivity between the four surveillance radar sites in Country X
Step 3. Determine CCIRs	
PIRs	a. Who is the adversary? b. What are the adversary’s strategic and operational objectives ***in reference to their surveillance radar***? c. How does the adversary operate ***their surveillance radar***? d. ***How is communications connectivity provided between the adversary’s four surveillance radar sites?*** e. How does the adversary utilize ***surveillance radar*** assets to achieve effects throughout other warfighting domains? f. What elements of the physical environment limit ***surveillance radar*** capabilities? g. How does the adversary defend ***the communications connectivity between their four surveillance radar sites***? h. What are the adversary’s ***communications connectivity*** centers of gravity ***between their four surveillance radar sites***? i. What are the adversary’s offensive capabilities ***related to communications connectivity between their four surveillance radar sites***? j. What are the adversary’s capabilities ***to defend communications connectivity between their four surveillance radar sites***? k. What is the adversary’s desired end state ***of having communications connectivity between their four surveillance radar sites***? l. What COAs are available to the adversary ***if communications connectivity between their four surveillance radar sites is lost***? m. What are the adversary’s ***communications connectivity*** vulnerabilities ***between their four surveillance radar sites***?
FFIs	a. What are the limits of the joint force’s operational area? b. What is the joint forces’ mission? c. What is the joint forces commander’s intent? d. What are our strategic and operational objectives? e. What are our limitations to cyberspace operations in this physical environment ***that will impact our ability to destroy the communications connectivity between the four surveillance radar sites in Country X***? f. What cyber effects are available to attack the adversary’s ***communications connectivity between the four surveillance***

	radar sites in Country X? g. What are our strategic and operational cyber centers of gravity ***relative to destroying the adversary's communications connectivity between their four surveillance radar sites***? h. What are our offensive cyber capabilities ***to destroy the communications connectivity between the four surveillance radar sites in Country X*** ? i. What are our defensive cyber capabilities ***to defend our cyber assets that are utilized to destroy communications connectivity between the four surveillance radar sites in Country X***? j. What is our desired end state? k. What COAs are available to us ***to destroy communications connectivity between the four surveillance radar sites in Country X***? l. What are our cyber vulnerabilities ***associated with destroying communications connectivity between the four surveillance radar sites in Country X***?

Figure 13. Cyberspace Information Requirements Analysis Method Configured for Operational Level Information Requirements

Figure 14 represents the hybrid information requirements analysis method that is configured to support C2 information requirements at the tactical level of war. The primary goal (Step 1) in this example is to eliminate off site communications capabilities at Base A in Country X. The sub-goal (Step 2) in this example is to destroy the adversary's telephone connectivity between Base A and the rest of Country X. The PIRs and FFIs in Step 3 are more detailed to support achieving these goals. The modifications are printed in bold italic (***bold italic***) to highlight modifications. This tactical level of warfare information requirements analysis method can be compared to Figure 11 to see modifications.

Cyberspace Information Requirements Analysis Method	
Step 1. Goal Identification	
Goal:	Eliminate off site communications capabilities at Base A in Country X
Step 2. Sub-Goal Identification	
Sub-Goal:	Destroy the adversary's telephone connectivity between Base A and the rest of Country X
Step 3. Determine CCIRs	
PIRs	a. Who is the adversary? b. What are the adversary's strategic and operational objectives? c. How does the adversary ***provide telephone connectivity between Base A and the rest of Country X***? d. How does the adversary utilize ***telephone connectivity between Base A and the rest of Country X*** to achieve effects throughout other warfighting domains? e. What elements of the physical environment limit ***telephone connectivity between Base A and the rest of Country X***? f. How does the adversary defend its ***telephone connectivity between Base A and the rest of Country X***? g. What are the adversary's strategic and operational cyber centers of gravity ***related to telephone connectivity between Base A and the rest of Country X***? h. What are the adversary's offensive cyber capabilities ***related to telephone connectivity between Base A and the rest of Country X***? i. What are the adversary's defensive cyber capabilities ***to defend telephone connectivity between Base A and the rest of Country X***? j. What is the adversary's desired end state? k. What COAs are available to the adversary ***if telephone connectivity between Base A and the rest of Country X is attacked***? l. What are the adversary's cyber vulnerabilities ***related to telephone connectivity between Base A and the rest of Country X***?
FFIs	a. What are the limits of the joint force's operational area? b. What is the joint forces' mission? c. What is the joint forces commander's intent? d. What are our strategic and operational objectives? e. What are our limitations to cyberspace operations in this physical environment ***related to destroying telephone connectivity between Base A and the rest of Country X***? f. What cyber effects are available to attack the adversary's cyber defenses ***related to destroying telephone connectivity between Base A and the rest of Country X***?

	g. What are our strategic and operational cyber centers of gravity ***related to destroying telephone connectivity between Base A and the rest of Country X***? h. What are our offensive cyber capabilities ***related to destroying telephone connectivity between Base A and the rest of Country X***? i. What are our defensive cyber capabilities? j. What is our desired end state? k. What COAs are available to us ***related to destroying telephone connectivity between Base A and the rest of Country X***? l. What are our cyber vulnerabilities ***related to attacking telephone connectivity between Base A and the rest of Country X***?

Figure 14. Cyberspace Information Requirements Analysis Method Configured for Tactical Level Information Requirements

The information requirements analysis method developed in this chapter provides a template for meeting the C2 information needs of the Director of Cyberspace Forces. The level of detail required to achieve specific goals will change as the goals do. The hybrid information requirements analysis template is intended to serve as a starting point for determining the information requirements of the Director of Cyberspace Forces to facilitate effective C2 of cyberspace.

V. Conclusions and Recommendations

Conclusions

The goals of this research effort were to demonstrate the need to identify C2 information requirements and develop a method of identifying C2 information requirements that would enable the Director of Cyberspace Forces to execute effective C2 of cyberspace. Emphasizing the role of information in C2 and highlighting the complex nature of cyberspace demonstrated the need to identify C2 information requirements in an effort to facilitate effective decision-making. A hybrid information requirements analysis method was developed to support the identification of C2 information for cyberspace. The hybrid information requirements analysis template was designed to enable modifications that enable the collection of C2 information for the strategic, operational, and tactical levels of war.

The hybrid information requirements analysis method successfully incorporates Endsley's goal directed task analysis method with the Department of Defense's CCIR process. Principles of the JIPB process successfully added rigor to the CCIR process and provide a valid framework for determining cyber information requirements that are required for effective C2 of a war fighting environment. The hybrid information requirements analysis method developed in this research successfully identifies C2 information requirements for the Director of Cyberspace Forces to enable effective C2 of cyberspace.

Recommendations for Future Research

The following paragraphs provide some topic areas for future research in areas related to the identification of C2 information requirements for the Director of Cyberspace Forces.

Intelligence Preparation of the Cyber Battlespace. The information requirements analysis method developed in this research could be used to construct intelligence preparation of the cyber battlespace theories. The missions and goals identified in this research are very likely to be similar to an adversary's missions and goals in cyberspace. The information requirements scheme from the hybrid information requirements analysis method could be combined with missions and goals of cyberspace and produce method for identifying and selecting cyber targets to achieve operational and/or strategic cyber objectives.

Develop Cyber Order of Battle. Due to the relative newness of recognizing cyberspace as a war fighting domain, there are no cyber order of battle theories that encompass cyber operations conducted throughout and across the entire electromagnetic spectrum. The C2 information requirements analysis method developed in this research could serve as a foundation for developing cyber order of battle theory. The missions, goals, and C2 information requirements provided in this research could provide a basis for developing cyber order of battle theory.

Develop Cyber Common Operating Picture (COP). A COP is a useful tool providing both operators and commanders with the ability to visualize the battlespace. The missions, goals, and C2 information requirements identified in this research could serve as a baseline for providing a cyber COP for the strategic, operational, and tactical view of the battlespace.

Assign Value Attribute to Cyber C2 Information. It is important to be able to assign a value to attribute to information to indicate the significance of the information to the war fighter. The value attribute assigned to C2 information would indicate which cyber assets are most critical for successful operations in cyberspace. The value attributes could be used to develop defense strategies, circuit activation, and restoral priorities. The missions, goals, and C2 information requirements could be utilized to assign value attributes to cyber C2 information.

Summary

This research presents a method for identifying the C2 information requirements of the Director of Cyberspace Forces. Cyberspace is currently an extremely dynamic environment in terms of development of doctrine, policy, and the way ahead for cyber operations. Much of this research effort is based on the *Air Force Cyber Warfare Operational Concept*, which is an evolving document that has experienced major direction shifts during the past two years. It is quite possible that the document could undergo another radical revision, which would require revisions to the missions, goals, and operations areas used in the hybrid cyberspace information requirements analysis method developed in this research.

Chapter I presents pertinent background information related to C2 and cyberspace. Chapter I also includes scope of the research along with the research methodology. Chapter II provides background information that enables the reader to understand key research concepts related to the complexity of identifying C2 information requirements for the Director of Cyberspace Forces. The background details the categorization of cyberspace as a military warfighting domain and the role of information in C2. In addition, information in the traditional warfighting domains is discussed along with methods for determining information requirements. Air Force Cyber Command is also discussed to frame the complex operating environment in which C2 information must be identified and used. The final section of the chapter focused on various information requirements analysis methods that are useful for identifying the C2 information requirements.

Chapter III presents the methodology used in this research. A content analysis of C2 research, military C2 doctrine, situational awareness research, information requirements analysis research, and Air Force cyberspace documents was performed to develop a method for identifying C2 information requirements for the cyberspace domain. The method for determining the C2 information requirements is executed in three phases. The assigned missions and goals of the cyberspace domain were identified in phase one. A hybrid information requirements analysis method was constructed during phase two. The hybrid information requirements analysis method was modified in phase three to identify C2 information required to achieve goals at either the strategic, operational, or tactical level of war.

Chapter IV applies the methodology from Chapter III to develop a hybrid information requirements analysis method to meet the C2 information requirements of the Director of Cyberspace Forces. Cyberspace missions, goals, and operations areas were identified in Phase One. A hybrid information requirements analysis method was developed in phase two. In phase three, the hybrid information requirements analysis method was modified to demonstrate how it could be used to identify C2 information requirements for the strategic, operational, and tactical level of war.

Chapter V provides conclusions from this research and suggests potential areas for future research related to the identification of C2 information requirements for the Directed of Cyberspace Forces.

Bibliography

1. Arnborg, S., J. Brynielsson, H. Artman, and K. Wallenius. "Information Awareness in Command and Control: Percision, Quality, Utility," *Proceedings of the Third International Conference on Information Fusion.* THB1/25-THB1/32. Stockholm Sweden. 2000.

2. Boyd, J.R., Discourse on Winning and Losing (unpublished manuscript), available online at http://www.d-n-i.net/second_level/boyd_military.htm

3. Breton, Richard and Robert Rousseau. "The C-OODA: A Cognitive Version of the OODA Loop to Represent C2 Activities," *Proceedings of the 10th International Command and Control Research and Technology Symposium: The Future of C2.* McLean VA. 2005

4. Department of Defense, *Information Operations.* JP 3-13. Washington: Government Printing Office, February 2006.

5. Department of Defense. *Joint Operations*. JP 3-0. Washington: Government Printing Office, September 2006.

6. Department of Defense. *Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace*. JP 2-01.3. Washington: Government Printing Office, May 2000.

7. Department of the Air Force. *Air Warfare*. AFDD 2-1. Washington: HQ USAF, January 2000.

8. Department of the Air Force. *Cyber Warfare Air Force Operational Concept*. USAF CYBERSPACE CONOPS. Washington: HQ USAF, April 2007.

9. Department of the Air Force. *Air & Space Power Journal*. AFRP 10-1. Washington: HQ USAF, Spring 2007.

10. Department of the Air Force. *Information Operations*. AFDD 2-5. Washington: HQ USAF, 11 January 2005.

11. Department of the Air Force. *Operations and Organizationse*. AFDD 2. Washington: HQ USAF, April 2007.

12. Drucker, Peter F. *Post-Capitalist Society*. New York: HarperCollins Publishers, Inc., 1993

13. Endsley, M. R. “Design and evaluation for situation awareness enhancement,” *Proceedings of the Human Factors Society 32nd Annual Meeting,* Santa Monica CA. 1988.

14. Endsley, M. R. “Designing for situation awareness in complex systems,” *Proceedings of the Second international workshop on symbiosis of humans, artifacts and environment,* Kyoto, 2001.

15. Endsley, M. R. and Garland D. J. *Situation Awareness Analysis and Measurement.* Mahwah, NJ: Lawrence Erlbaum Associates, 2000.

16. Flach, John M. “Situation Awareness: Proceed With Caution,” *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 37: 149-157 (March 1995).

17. Gibson, William *Burning Chrome*. New York: EOS Harper Collins Publishers, 1986.

18. Joint Chiefs of Staff. *Joint Net-Centric Operations Campaign Plan.* Washington: Joint Staff; Command Control, Communications, and Computer Systems Directorate, 2006.

19. Merriam-Websters Dictionary. *Online! Cyberspace Definition*. 25 July 2007 http://www.merriam-webster.com/dictionary/cyberspace

20. Tribus, Myron “Rational Descriptions, Decisions and Designs. New York: Pergamon Press Inc., 1969.

21. Yadav, Surya B. “Determining an Organization’s Information Requirements: A State of the Art Survey,” *Communications of the Association for Computing Machinery*, 14: 3-20 (1983).

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)* 27032008	**2. REPORT TYPE** Master's Thesis	**3. DATES COVERED** *(From - To)* Jan 07 - Jan 08

4. TITLE AND SUBTITLE

IDENTIFICATION OF COMMAND AND CONTROL INFORMATION REQUIREMENTS FOR THE CYBERSPACE DOMAIN

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Aschenbrenner, Brian D., Capt, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
WPAFB, OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GIR/ENG/08-01

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Robert Kaufman
AFIOC/IO (ACC)
102 Hall Blvd Ste 345
Lackland AFB TX 78243-7038
DSN 969-5377

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The purpose of this research was to develop an information requirements analysis method that would provide the Director of Cyberspace Forces with the information required to support effective command and control of cyberspace. This research investigates the role of information in command and control, information in the traditional war fighting domains, cyberspace as a war fighting domain, and various methods of determining information requirements of organizations. This research produced an information requirements analysis method that is suitable for identifying the command and control information requirements of the Director of Cyberspace Forces.

15. SUBJECT TERMS

Cyberspace, Command and Control, Information Requirements Analysis

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Robert F. Mills (ENG)
U	U	U	UU	70	**19b. TELEPHONE NUMBER** *(Include area code)* robert.mills@afit.edu (937) 255-3636