Factors Influencing Agility in Allocating Decision-Making Rights For Cyberspace Operations

20th ICCRTS Paper 096

Steven W. Stone
Robert Morris University
swsst320@mail.rmu.edu

ABSTRACT

In 2011, the United States (U.S.) Department of Defense (DoD) named cyberspace a new operational domain and is working to make the cyberspace environment a suitable place for achieving national objectives and enabling military command and control (C2). The DoD's emerging doctrine attempts to address the uniqueness of military operations in cyberspace and clarify the command relationships for cyberspace operations. However, military planners are attempting to apply C2 doctrine developed for military operations in the physical domain to military operations in the cyberspace domain. The spatial and temporal dimensions of cyberspace are significantly different than the physical domain and are much more complex and dynamic. Thus, military operations in cyberspace likely require different and more agile C2 and decision-making methods to be successful. The challenge facing the DoD is that it does not yet understand how to measure the decision-making agility of a cyberspace operations organization in the face of the complex dynamics presented by the cyberspace domain. Several theoretical models suggest factors that may affect the allocation of decision-making rights for cyberspace operations. This paper presents on-going research into the factors influencing agility in allocating decision-making rights for cyberspace operations amongst the organizations conducting these operations.

KEYWORDS: *Decision Making; Command and Control; Military; Cyberspace Operations;*

INTRODUCTION

The growing use of cyberspace has reached the point where a wide range of social, political, informational, economic and military activities are dependent on it and are vulnerable to both interruption of its use and usurpation of its capabilities (Kuehl, 2009). The physical platforms, systems, and infrastructures that provide global connectivity to link information systems, networks, and human users with massive amounts of information that can be digitally sent anywhere, anytime, to almost anyone, has greatly increased access to information and has affected human cognition, dramatically impacting human behavior, and decision making (Kuehl, 2009).

In order to effectively conduct cyberspace operations in support of the Nation's security and military operations, the Secretary of Defense directed the establishment of U.S. Cyber Command in 2009 (United States Department of Defense, 2009). In 2011, the U.S. Department of Defense (DoD) named cyberspace a new operational domain (Williams, 2014). The purpose of both actions was to achieve the United States' national security objectives in or through cyberspace. In support of these objectives, the Under Secretary of Defense for Policy stated "There is a compelling need for a comprehensive, robust and articulate cyber power theory that describes, explains, and predicts how our nation should best use cyber power in support of U.S. national and security interests" (Kramer, Starr, & Wentz, 2009, p. xv). Subsequent to that statement, the U.S. military began to develop an understanding of, and doctrine for, utilizing cyberpower, "the ability to use cyberspace to create advantages and influence events in all of the operational environments and across the instruments of power" (Kuehl, 2009, p. 38).

The U.S. Cyber Command and the military services are working to make the cyberspace environment a suitable place for achieving our national objectives and enabling military command and control (C2). The DoD defines cyberspace as "A global domain within the

information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (United States Department of Defense, 2014, p. 63). The DoD further defines cyberspace operations as "The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace" (United States Department of Defense, 2014, p. 63). In 2013, the DoD published Joint Publication 3-12, Cyberspace Operations (U.S. Department of Defense, 2013). This emerging doctrine attempts to address the uniqueness of military operations in cyberspace and clarify cyberspace operations command relationships. However, there is a lack of research on decision-making in the face of the complex dynamics presented by the cyberspace domain.

STATEMENT OF THE PROBLEM

The challenge facing the DoD is that it does not yet understand the factors affecting, nor how to implement, agility in allocating decision-making rights in the face of the complex dynamics presented by the cyberspace domain. The cyberspace domain is significantly different from the physical domain in both the temporal and spatial dimensions. Cyberspace is inherently global in nature and cyber effects often occur at the speed of light. This new domain presents a much more dynamic and complex operational environment for the U.S. Military. However, the DoD is currently applying C2 doctrine developed for operations in physical space to operations conducted in cyberspace. This attempt by military planners to apply C2 doctrine developed for physical military operations to cyberspace operations may be inappropriate. The temporal and spatial differences presented by cyberspace require the military to examine its long-held doctrine for C2. Military operations in cyberspace likely require different and more agile C2 and decision-making methods to be successful. Alberts & Hayes explain "Agile C2 is a function of both the agility of decision-making and the agility of the decisions made" (2006, p. 148).

This situation suggests a need to consider the relationship of the organization to its environment in order to determine the appropriate organizational design (Galbraith, 1973, p. v). Several authors have called for additional research in this area. The Commander of United States Cyber Command has stated, "Our traditional command and control and organizational constructs do not enable the speed and agility required to keep pace with change in the cyber domain" (United States Department of Defense, 2015, p. 2). Alberts (2014) has called for research into the "…identification of key variables and relationships that should be included in a model of Command and Control Agility Potential whose output would be an entity's C2 AQ (agility quotient)" (Alberts, 2014, p. 1). Gore, Banks, Millward, & Kyriakidou (2006) conclude that a major goal of decision-making research is the development of ecologically valid practical methods for minimizing error and improving decision quality. This research examines the factors that may affect the U.S. Military's agility in allocating decision-making rights for cyberspace operations.

Differences in the Cyberspace Domain

For much of recorded history, military forces had only two physical domains in which to operate, the land and the sea. Both domains had different physical characteristics and humans used different technologies to operation in these domains. In addition to walking, military operations in the land domain were enhanced by the wheel, and various vehicles. Because humans can swim for only so long, war fighting on the sea was possible only with the aid of technology: the galley, sailing ship, steamship, and nuclear submarine (Kuehl, 2009). Two additional war-fighting domains were added in the 20th Century: air and outer space. Military operations in both of these domains were made possible by advances in technology, the development of aircraft and spacecraft. Each of these four physical domains is marked by

radically different physical characteristics, and they are usable only through the use of technology to exploit those characteristics (Kuehl, 2009).

Cyberspace has uniquely defining characteristics when compared to the land, sea, air, and outer space domains. First, cyberspace is a man-made domain. While the physical characteristics of cyberspace come from electromagnetic forces and phenomena that exist and occur in the natural world, cyberspace is a human-designed environment, created to use and exploit information, human interaction, and intercommunication. Cyberspace was created not to sail the seas or orbit the earth, but rather to "create, store, modify, exchange, and exploit" information via electronic means (Kuehl, 2009). Humankind can capture any type of information, store that information as a string of bits and bytes, modify it to suit our purposes, and then transmit it instantly to every corner of the globe.

Second, cyberspace is global in nature (Kuehl, 2009). The effects of war fighting in the physical domains are typically limited to an easily identifiable geographic area. A bomb affects a small radius around its detonation point. A bullet affects a small area around its aim point. Cyberspace effects are not limited to a small local area. Cyber effects are often global in nature. For example, malware frequently infects computer systems worldwide.

Third, activities in cyberspace can happen extremely rapidly. As cyberspace is created using electromagnetic forces found in nature, effects in cyberspace can travel at the speed of light. Kuehl states, "What makes cyberspace neither aerospace nor outer space is the use of the electromagnetic spectrum as the means of "movement" within the domain, and this clear distinction from other physical environments may be crucial to its further development within the national security structure" (Kuehl, 2009, p. 31).

Fourth, cyberspace is incredibly complicated, comprising millions of separate hardware devices, running software with millions of potential settings, and processing millions of bits of

data. Modern operating systems have thousands of settings. Many network security devices have hundreds of thousands of rules running on them at any point in time. Richard Hale, the DoD's Chief Information Security Officer states, "No human being can understand this. There is no way any human analyst has a prayer of taking all of thousands of settings multiplied by thousands of settings and making sense of that" (Hale, 2014).

Fifth, unlike the physical domains, where nature often sets the conditions of the environment, many decisions regarding the behavior of cyberspace are made by the software running on those devices. Conducting operations in cyberspace is done by changing the configuration of these complicated pieces of equipment. Peter Fonash, Chief Technology Officer for the Department of homeland Security Office of Cybersecurity and Communications, states, "The first technology that I would want to have is a capability to do automated decision-making and automated courses of action. Instead of waiting for a human to perceive a threat, make sense of it, and decide on a response — let alone wait for higher-ups to authorize it — we need software that can perform all those functions by itself, moving at the same speed as the attacking malware" (Fonash, 2014).

PURPOSE OF THE STUDY

The purpose of this quantitative exploratory study is to identify the factors influencing the U.S. Military's agility in allocating decision-making rights for cyberspace operations. This study will analyze factors identified from the literature and factors identified by experts in the field. The goal of this study is to provide military decision makers with a list of factors to consider when determining the allocation of decision-making rights for cyberspace operations.

RESEARCH QUESTION

The research question for this study is: What factors influence the U.S. Military's agility in allocating decision-making rights for cyberspace operations?

METHODOLOGICAL DESIGN

Given the complex nature of this problem and the somewhat open-ended nature of the research question, the researcher proposes to use the Delphi research method to identify the factors influencing the U.S. Military's agility in allocating decision-making rights for cyberspace operations.

The Delphi panel will be recruited from experts in C2 and Cyberspace Operations. For purposes of this research, an expert is defined as a person that has at least five years of practical experience working in cyber operations; or a person that has an advanced degree in an information management field with over 10 years of research in cyberspace operations, C2, or decision-making theory. The panel will be recruited through the researcher's participation in, and contacts with, the cyberspace operations, C2, and decision-making research communities.

DECISION MAKING THEORY

Hoffman describes organizational design as "the relatively enduring allocation of work roles and administrative mechanisms that creates a pattern of interrelated work activities and allows the organizations to conduct, coordinate, and control its work activities" (Hoffman, 1998, p.6). One of the primary dimensions of organizational design is the decision making structure. Hoffman states that the "Decision making structure involves the centralization and decentralization of decision making. Organizational decision-making has been formally defined as being the process of identifying and solving problems within organizations (Hoffman, 1988, p. 7). The performance of an organization is determined, at least partially, by how well problems

are identified and solved. Thus, an organization's decision-making structure is one of the most critical areas of the organization's design. Several theoretical models of decision-making, such as Albert's and Hayes' model of C2, the Military Decision Making Process, Galbraith's Information Processing Model, Drucker's examination of the 'New Organization', Klein's Recognition-Primed Decision Model and Shattuck & Miller's Dynamic Model of Situated Cognition suggest factors that may affect the allocation of decision-making rights for cyberspace operations.

Theoretical Model of Command and Control and Decision Making Agility

The U.S. Military's C2 doctrine has been developed and refined over many years of military operations in the industrial age. However, there is significant debate as to whether these decision-making relationships will be effective in the information age. Alberts (2007) argues that the traditional DoD C2 approach is no longer sufficient for military operations in cyberspace.

Alberts and Hayes (2006) describe three dimensions of a theoretical model of C2 or, in non-military parlance, organizational culture, that are useful in this research: The organization's allocation of decision-making rights, the organization's patterns of interaction, and the organization's distribution of information. Peterson describes the components of a decision as: a decision maker, a desired outcome, goal or objective, a set of alternatives, information on the state of the world, and the choice of an act from the set of alternatives (2009). The U.S. Department of Defense defines a decision as, "decision —In an estimate of the situation, a clear and concise statement of the line of action intended to be followed by the commander as the one most favorable to the successful accomplishment of the assigned mission" (United States Department of Defense, 2014, p. 66).

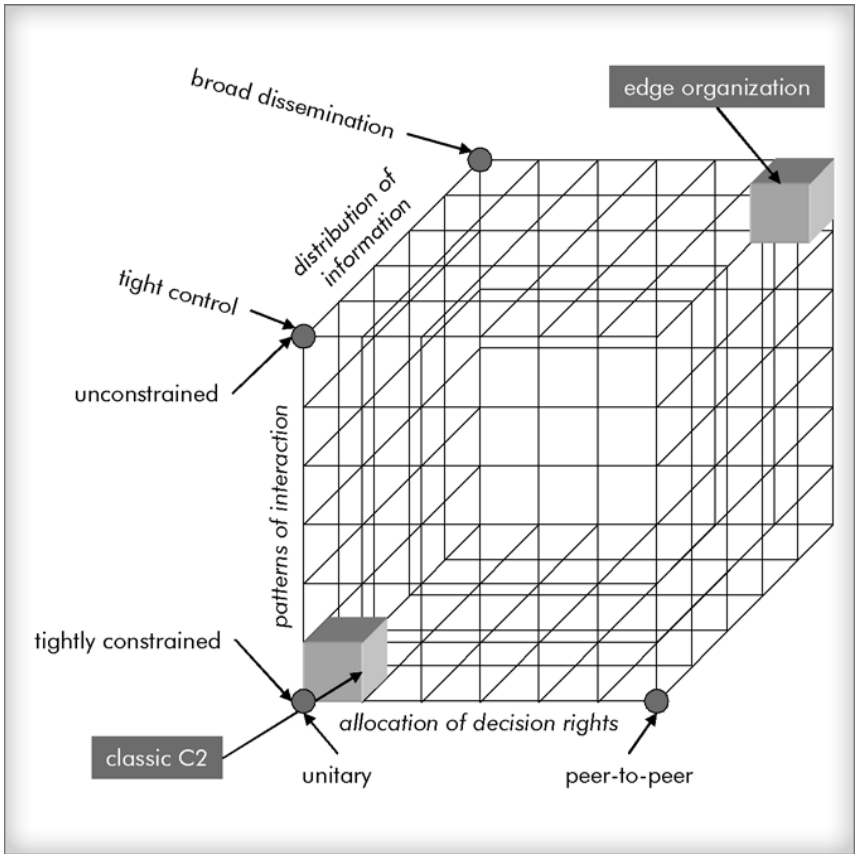

Figure 1. Model of command and control (Albert and Hayes, 2006)

Alberts and Hayes describe decisions as:

Decisions are choices among alternatives. Decision rights belong to the individuals or organizations accepted (whether by law, regulation, practice, role, merit, or force of personality) as authoritative sources on the choices related to a particular topic under some specific set of circumstances or conditions. The allocation of decision rights is their distribution within the international community, a society, an enterprise, or an organization. In this context, the organization of interest is a military, a coalition, an interagency effort, or an international effort including military elements. There can be different distributions of those rights across functions, echelons, time, or circumstances. (Alberts & Hayes, 2006, p. 83)

The allocation of decision-making rights is a linear dimension with two logical endpoints. At the origin of the allocation of decision-making rights on the horizontal axis, decision-making rights are unitary; all rights held by a single actor. At the other end point, decision-making rights are allocated uniformly with every entity having equal rights in every decision (Alberts & Hayes, 2006). Alberts and Hayes hypothesize that complex dynamic environments, like cyberspace operations, require more agile approaches to C2. Albert's hypothesis is that agile C2 requires the organizational ability to rapidly change their approach towards each of the three dimensions in the theoretical model of C2 (Alberts & Hayes, 2006). Alberts defines C2 agility as:

> Agility is the synergistic combination of robustness, resilience, responsiveness, flexibility, innovation, and adaptation. Each of these attributes of agility contributes to the ability of an entity (a person, an organization, a coalition, an approach to command and control, a system, or a process) to be effective in the face of a dynamic situation, unexpected circumstances, or sustaining damage. Effectiveness without agility is fragility. (Alberts, 2007, p. 23)

Alberts and Hayes also describe the value of agile decision-making as "All things being equal, agile decisions (those that work in the face of changes in circumstances) are preferred to decisions that are brittle and will only work well if the situation is as understood and anticipated" (Alberts & Hayes, 2006, p. 148). They continue to describe agility in decision-making as "Agility can also be created by making decisions that increase the number and variety of available options, but option creation is never a goal in itself and must be coupled with decisions to act effectively (Alberts & Hayes, 2006, p. 148). And they summarize this thinking by stating, "Agile C2 is a function of both the agility of decision-making and the agility of the decisions made" (Alberts & Hayes, 2006, p. 148).

Military Command & Control and The Military Decision Making Process

The U.S. Department of Defense has a large body of organizational design documentation that describes how the U.S. military is organized and functions. In military parlance this body of documentation is called Doctrine. The U.S. military's term to describe its organizational design and decision-making process is C2. The DoD defines C2 as "The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission" (United States Department of Defense, 2014, p. 44). The DoD goes on to further define the components of C2. DoD defines Command as "The authority that a commander in the armed forces lawfully exercises over subordinates by virtue of rank or assignment. An order given by a commander; that is, the will of the commander expressed for the purpose of bringing about a particular action." (United States Department of Defense, 2014, p. 44). This definition is further explained as:

> Command includes both the authority and responsibility to effectively use available resources to accomplish assigned missions. Command at all levels is the art of motivating and directing people and organizations into action to accomplish missions. The C2 function supports an efficient decision-making process. Enabled by timely intelligence, surveillance, and reconnaissance (ISR), the goal is to provide the ability to make decisions and execute those decisions more rapidly and effectively than the adversary. This decreases risk and allows the commander more control over the timing and tempo of operations. (United States Department of Defense, 2011, pp. III-2 – III-3)

The DoD defines the term control as "Authority that may be less than full command exercised by a commander over part of the activities of subordinate or other organizations" (United States Department of Defense, 2014, p. 54). Joint Publication 3-0 describes control as:

> To control is to manage and direct forces and functions consistent with a commander's command authority. Control of forces and functions helps commanders and staffs

> compute requirements, allocate means, and integrate efforts. Control is necessary to determine the status of organizational effectiveness, identify variance from set standards, and correct deviations from these standards. (United States Department of Defense, 2011, p. III-5)

Because military operations involve large organizations consisting of subordinate organizations distributed in a hierarchical manner, the DoD has also defined Command Relationships to describe the authorities assigned to commanders at different levels and to describe the decision–making relationships between those commanders. In DoD doctrine Command relationships are "The interrelated responsibilities between commanders, as well as the operational authority exercised by commanders in the chain of command; defined further as combatant command (command authority), operational control, tactical control, or support" (United States Department of Defense, 2014, p. 46).

The DoD's doctrine on command and control is heavily dependent on the person designated as the Commander. The history of DoD C2 doctrine places great responsibility on the commander. Joint Publication 3-0 states:

> Historical analysis shows that commander-centric organizations out-perform staff-centric, process-oriented organizations. A commander's perspective of the challenge at hand is broader and more comprehensive than the staff's due to interaction with civilian leaders; senior, peer, subordinate, and supporting commanders; and interorganizational partners. Clear commander's guidance and intent, enriched by the commander's experience and intuition, are common to high-performing units. (United States Department of Defense, 2011, p. II-1)

The authority to conduct operations and make decisions is granted solely to the commander. While the commander has a staff that performs their tasks and often makes decisions on behalf of the commander, the authority and responsibilities belong to the designated

commander. The effectiveness of the C2 process rests largely on the skill and experience of the commander. The DoD doctrine for operations states:

> While command authority stems from appropriate orders and other directives, the art of command resides in the commander's ability to use situational leadership to maximize operational performance. The combination of courage, ethical leadership, judgment, intuition, situational awareness, and the ability to consider contrary views gained over time through training, education, and experience helps commanders make difficult decisions in complex situations. (United States Department of Defense, 2011, p. II-1)

The DoD has also developed a deliberate decision-making process to aid the commander in gathering the information necessary to make a decision, examine the alternatives for the decision, and to decide upon the best alternative. This process is named the Military Decision Making Process (MDMP). The MDMP is described as:

> The military decision making process is an iterative planning methodology to understand the situation and mission, develop a course of action, and produce an operation plan or order. The military decision making process (MDMP) helps leaders apply thoroughness, clarity, sound judgment, logic, and professional knowledge to understand situations, develop options to solve problems, and reach decisions. This process helps commanders, staffs, and others think critically and creatively while planning. (U.S. Department of the Army, 2014, p. 9-1)

In 2013, the DoD published Joint Publication 3-12, Cyberspace Operations. This document describes how the DoD defines cyberspace operations and how it intends to conduct military operations in cyberspace. The DoD describes two cyberspace objectives relevant to the conduct of military operations as: providing freedom of maneuver in cyberspace and projecting power in and through cyberspace to achieve campaign objectives (United States Department of Defense, 2013).

There are three categories of cyberspace missions for attaining these two objectives: DOD information network (DODIN) operations; defensive cyberspace operations (DCO); and offensive cyberspace operations (OCO) (Williams, 2014, p.14). DoD further describes cyberspace operations (CO) as:

> CO missions are categorized as OCO, DCO, and DODIN operations based on their intent. OCO are CO intended to project power by the application of force in and through cyberspace. DCO are CO intended to defend DOD or other friendly cyberspace. DODIN operations are actions taken to design, build, configure, secure, operate, maintain, and sustain DOD communications systems and networks in a way that creates and preserves data availability, integrity, confidentiality, as well as user/entity authentication and non-repudiation. (U.S. Department of Defense, 2013, p. vii)

DoD also defines four actions in conducting cyberspace operations: "Cyberspace forces execute four actions to create the necessary effects in the domain: cyberspace defense; cyberspace operational preparation of the environment (OPE); cyberspace intelligence, surveillance, and reconnaissance (ISR); and cyberspace attack" (Williams, 2014, pp. 14-15). "Cyberspace defense actions are conducted by the commander with authority over the information environment to protect, detect, characterize, counter, and mitigate threats and vulnerabilities" (Williams, 2014, p.19). "Cyberspace ISR is normally authorized under military authorities and conducted to provide critical operational information to support follow-on actions" (Williams, 2014, p.19). "Cyberspace OPE consists of non-intelligence actions that set the stage for follow-on operations" (Williams, 2014, p.19). Finally, "cyberspace attack counters the adversary's ability to achieve objectives through degradation, disruption, or destruction of infrastructure and/or capabilities. Cyberspace attack can also manipulate data in a way that impacts the adversary's information systems" (Williams, 2014, p.19).

Major General Williams, former Director of Operations at U.S. Cyber Command, describes the C2 of cyberspace operations as: "The Joint Force Cyber Component Commander (JFCCC) will direct DODIN Ops and DCO to provide freedom of maneuver in cyberspace and will direct offensive cyberspace operations (OCO) to project power in and through cyberspace" (Williams, 2014, p. 18). DoD describes the effective C2 of cyberspace operations as: "The successful execution of CO requires the integrated and synchronized employment of offensive, defensive, and DODIN operations, underpinned by effective and timely operational preparation of the environment" (U.S. Department of Defense, 2013, p. vii). Major General Williams also describes the role of the commander as balancing the constraints, restraints, costs, benefits, and risks associated with each mission area, and assessing the impacts across all three mission areas when any changes are made. Major General Williams states: "Commanders must achieve a balance that satisfies their mission objectives at an acceptable level of risk" (Williams, 2014, p. 16).

Information Processing Theory

Galbraith's Information Processing Theory presents a framework to describe the relationship of an organization to the information environment it faces (Galbraith, 1973; Galbriath, 1974). Galbraith states that the basis of his Information Processing Theory is "… the greater the task uncertainty, the greater the amount of information that must be processed among decision makers during task execution in order to achieve a given level of performance" (Galbriath, 1973, p. 4). Galbraith also states that the type of information processed, either quantitative or qualitative, affects where the information should be processed. This theory is very applicable to the military's cyberspace operations C2 issue.

New Organization Theory

Management theorist Peter Drucker's paper, "The Coming if the New Organization" discusses Drucker's thoughts on the knowledge based organization. Drucker advocates for

decentralization and simplification of the management and decision-making structure in information age organizations. Drucker discounted the command and control model and asserted that companies work best when they are decentralized (Buchanan, 2009). Buchanan's assessment of Drucker's thoughts states:

> Drucker favored decentralized organizations because they create small pools in which employees gain satisfaction by witnessing the fruits of their efforts, and nascent leaders can make mistakes without bringing down the business. When Drucker laid out these ideas in the mid-1940s, the command-and-controllers who dominated corporations were not amused. Today, of course, "stovepipe" organizations--those that remain--are widely maligned for their failure to make the most of human and information resources. (Buchanan, 2009)

Drucker advocated for the elimination of many layers of middle management and decision-making. Drucker stated that the knowledge based company would naturally modify their internal decision making structure. Drucker stated, "… as soon as a company takes the first step from data to information, its decision processes, management structure, and even the way its work gets done begin to be transformed" (Drucker, 1988, p. 3).

Drucker's thoughts on the knowledge-based organization are very applicable to cyberspace operations. The characteristics he describes fit the cyberspace operations environment very well. Many of the organizational characteristics he identified, suggest factors that may affect agility in allocating decision-making rights for cyberspace operations.

Naturalistic Decision Making

Naturalistic Decision Making (NDM) provides a theory and methodology to describe how decision makers actually make decisions in complex domains. Orasanu and Connolly (1993) identify that decision makers are often challenged by factors identified by the NDM framework including: ill-structured problems; uncertain, dynamic environments; shifting, ill-defined or

competing goals; action/feedback loops; time stress and high stakes; organizational goals and norms (Orasanu and Connolly 1993). NDM research focuses on what decision makers actually do in fast-paced, complex, and dangerous situations where there is not time to perform elaborate evaluation of alternatives or to optimize the decision (Lipshitz, Klein, & Carroll, 2006). NDM rejects the belief that that decision-making is choosing among alternative courses of action. The basic hypothesis of NDM is that decision makers generate sequential options based on experience, pattern matching, situation awareness, and story construction (Lipshitz, Klein, & Carroll, 2006). Gore et al. (2006) conclude that a major goal of NDM is the development of ecologically valid practical methods for minimizing error and improving decision quality. This theory of decision-making in complex domains is relevant to the cyberspace domain and may suggest factors that affect the allocation of decision-making rights for cyberspace operations.

Two, NDM based, decision-making theories provide additional insight into potential factors affecting cyberspace operations decision-making: The Recognition Primed Decision (RPD) model and the Dynamic Model of Situated Cognition (DMSC).

Klein and his colleagues developed the recognition-primed decision (RPD) model based on their observations of decision makers in operational settings (Klein et al. 1986). The model describes how experts use their experiences to arrive at decisions quickly and without the computational (i.e. cost–benefit or utility) analysis of traditional normative decision-making approaches (Raiffa 1968). RPD employs situation assessment to generate a likely course of action and then uses mental simulation to envision and evaluate the course of action.

The Dynamic Model of Situated Cognition extends other NDM models to include the technological aspects of decision-making. Shattuck and Miller (2006) argue that "While NDM represents a major step forward in our understanding of the activities in various fields of practice, the focus of NDM has been on the human agents in complex systems and has not emphasized the influence, contributions, and modeling of the technological aspects of these systems" (p. 1).

Shattuck and Miller continue by stating, “The DMSC captures both the human and technological components of complex systems into a single model and illustrates how both technological agents and other human agents influence the decision making of a human” (pp. 1-2). While many researchers view these multiple players as humans, these researchers agree with others who believe that these players must include both machine and human agents. Interactions between humans and machines are rife in complex systems. These interactions can lead to situation assessments that result in decisions by either the human or the machine. Unfortunately, either the machine or the human may reach an incorrect decision based on the information they receive from another (human or machine) agent.

PRELIMINARY LIST OF FACTORS AFFECTING DECISION MAKING AGILITY

To date, a review of the literature has resulted in a preliminary list of 32 factors that may affect the DoD’s agaility in allocating decision-making rights for cyberspace operations. Table 1 shows the 32 factors, including the factor title, a short description, the source for the factor and the area of literature where the factor was found. This list of factors will become the input into the first round of the Delphi study which is expected to occur in June 2015.

SUMMARY

As discussed in this paper, the U.S. military is facing challenges in cyberspace that present a much different environment than operations in the physical space. The temporal and spatial differences presented by cyberspace require the military to examine it long-held doctrine for C2. Albert’s and Hayes’ model of C2, the Military Decision Making Process, Galbraith’s Information Processing Model, Drucker’s New Organization, Klein’s Recognition-Primed Decision Model and Shattuck & Miller’s Dynamic Model of Situated Cognition provide the theoretical framework to examine the factors influencing the allocation of decision-making rights

for cyberspace operations. The outcome of this study will provide military decision makers with a list of factors to consider when determining the allocation of decision-making rights. This research will add to the body of knowledge in that it will assist the U.S. military to define the C2 structures and procedures that will enable them to be successful in conducting cyberspace operations.

TABLE 1: PRELIMINARY LIST OF FACTORS

Factor Number	Factor Title	Factor Description	Source	Literature Area
1	Command Authorities and Relationships	The interrelated responsibilities between commanders, as well as the operational authority exercised by commanders in the chain of command.	Joint Publication 1-02 (2014)	Military Doctrine
2	Mission	The task, together with the purpose, that clearly indicates the action to be taken and the reason therefore.	Joint Publication 1-02 (2014)	Military Doctrine
3	Command Intent	A clear and concise expression of the purpose of the operation and the desired military end state that supports mission command, provides focus to the staff, and helps subordinate and supporting commanders act to achieve the commander's desired results without further orders, even when the operation does not unfold as planned.	Joint Publication 1-02 (2014)	Military Doctrine
4	Time Available	The time available for decision-making.	Joint Publication 1-02 (2014)	Military Doctrine
5	Phase of Operations	Joint doctrine describes six phases of military operations: Phase 0 – Shape: Activities are performed to dissuade or deter potential adversaries and to assure or solidify relationships with friends and allies. Phase 1 – Deter: Deter undesirable adversary action by demonstrating the capabilities and resolve of the joint force. Phase 2 – Seize Initiative: seize the initiative through the application of appropriate joint force capabilities. Phase 3 – Dominate: focuses on breaking the enemy's will for organized resistance or, in noncombat situations, control of the operational environment. Phase 4 – Stabilize: Required when there is no	Joint Publication 1-02 (2014)	Military Doctrine

		fully functional, legitimate civil governing authority present. Phase 5 – Enable Civil Authority: Characterized by joint force support to legitimate civil governance in theater.		
6	Type of Cyberspace Operation	Cyberspace Operations (CO) missions are categorized as Offensive Cyberspace Operations (OCO), Defensive Cyberspace Operations (DCO), and DoD Information Network (DODIN) operations based on their intent. OCO are CO intended to project power by the application of force in and through cyberspace. DCO are CO intended to defend DOD or other friendly cyberspace. DODIN operations are actions taken to design, build, configure, secure, operate, maintain, and sustain DOD communications systems and networks in a way that creates and preserves data availability, integrity, confidentiality, as well as user/entity authentication and non-repudiation.	Joint Publication 3-12(R) (2013)	Military Doctrine
7	The Global Nature of Cyberspace	The effects of war fighting in the physical domains are typically limited to an easily identifiable geographic area. A bomb affects a small radius around its detonation point. A bullet affects a small area around its aim point. Cyberspace effects are often not limited to a small local area. Cyber effects are often global in nature	Kuehl (2009)	Cyberspace Research
8	The speed of cyberspace effects	As cyberspace is created using electromagnetic forces found in nature, effects in cyberspace can travel at the speed of light. What makes cyberspace unique is the use of the electromagnetic spectrum as the means of “movement” within the domain.	Kuehl (2009)	Cyberspace Research

9	The complicated nature of cyberspace	Cyberspace is incredibly complicated, comprising millions of separate hardware devices, running software with millions of potential settings, and processing millions of bits of data. Conducting operations in cyberspace is accomplished by changing the configuration of the settings of complicated pieces of equipment.	Hale (2014)	Cyberspace Research
10	Degree of Automated Decision Making	Unlike the physical domains, where nature often sets the conditions of the environment, the software running on the devices comprising cyberspace makes many decisions regarding the behavior of the domain.	Fonash (2014)	Cyberspace Research
11	Agility between Human and automated decision-making	Human beings are not capable of comprehending the complexity of the cyberspace domain and understanding the thousands of settings multiplied by thousands of settings in the devices comprising the domain. However, human decision-making is necessary to conduct effective cyberspace operations.	Fonash (2014)	Cyberspace Research
12	Task Uncertainty	The greater the task uncertainty, the greater the amount of information that must be processed among decision makers during task execution in order to achieve a given level of performance	Galbraith (1973)	Information Processing Theory
13	Ability to Pre-Plan	The ability of the organization to preplan or to make decisions in advance of task execution	Galbraith (1973)	Information Processing Theory
14	Type of Data Needed to Make a Decision	If the information relevant to a particular decision is qualitative, it is more effective to bring the point of decision down to the points where the information originated. If the information relevant to a particular decision is quantitative, it can be more effective to move the data to a centralized point for centralized analysis.	Galbraith (1973)	Information Processing Theory

15	Information Volume	The volume of data available to decision makers is increasing at a rapid rate. There is more data than ever before and its size continues increasing.	Fan & Bifet (2013)	Big Data Theory
16	Information Velocity	The velocity of information, the increasing rate at which data flows into an organization and becomes available to decision makers is rapidly increasing. Data is arriving continuously as streams of data and decision makers must obtain useful information from it in real time.	Fan & Bifet (2013)	Big Data Theory
17	Information Variety & Variability	There are many different types of data, such as text, sensor data, audio, video, and graph, available to decision makers. The available data is diverse, and doesn't fall into neat relational structures. The structure of the data changes as operations progress.	Fan & Bifet (2013)	Big Data Theory
18	Employees self discipline	In the information-based organization, coordination and control of decision-making will depend largely on employees' willingness to discipline themselves.	Drucker (1998)	Knowledge Management Theory
19	Information Responsibility	Drucker discusses a requirement for an information-based organization to have an organizational culture where everyone takes information responsibility by asking: Who depends on me for what information? On whom do I depend for information? Drucker states that the most important contacts in this organizational culture are the colleagues with which a person coordinates to accomplish tasks.	Drucker (1998)	Knowledge Management Theory
20	Location of Expertise	Drucker argues that the information-based organization requires far more specialists overall than the command and control organization. The specialists are found in operations organizations, not at headquarters.	Drucker (1998)	Knowledge Management Theory

21	Location of Knowledge	Drucker states that in the information-based organization, knowledge will be primarily at the lower levels of the organization, in the minds of the specialists who do different work and direct themselves.	Drucker (1998)	Knowledge Management Theory
22	Individual Relationships	Drucker states that the success of an information-based organization requires greater emphasis on individual relationships where specialists coordinate and exchange information.	Drucker (1998)	Knowledge Management Theory
23	Role of the First Line Leader	Drucker states that in the information-based organization the role of the first-line leader will change from that of a person who is working as a full time manager / commander to that of a specialist who is in charge of leading a team of other specialists.	Drucker (1998)	Knowledge Management Theory
24	Clearly Stated Organizational Goals	Goals that clearly state management's performance expectations for the enterprise and each sub-organization.	Drucker (1998)	Knowledge Management Theory
25	Feedback from Leadership	Leadership provides organized feedback that compares results with performance expectations so that every member can exercise self-discipline / self-control.	Drucker (1998)	Knowledge Management Theory
26	Problem Structure	NDM theory states that problems tend to be ill structured. That is, for some real-world problems, it is not easy or even possible to identify causes and potential courses of actions.	Orasanu and Connolly (1993)	Naturalistic Decision Making
27	Dynamic & uncertain conditions	NDM theory states that the conditions facing decision makers are frequently uncertain and dynamic. The situation is continually changing, making it difficult to assess what is happening. Static representations of the system are of little use since the situation is changing so quickly.	Orasanu and Connolly (1993)	Naturalistic Decision Making

28	Number of Goals	NDM theory states that there are often multiple goals influencing the decision and the multiple goals may be ill defined, may be in conflict, or may shift over time. Not only may these goals change from time to time, they may, in fact, conflict with one another.	Orasanu and Connolly (1993)	Naturalistic Decision Making
29	Existence of action and feedback loops	NDM theory states that decisions are not discrete events but happen amidst the flow of activity in an operation and are impacted by feedback from the decisions and activity that precede them.	Orasanu and Connolly (1993)	Naturalistic Decision Making
30	Real-time operational changes	NDM theory states that decision makers must respond in real time to changes in the operation. Diagnosis of problems and command and control often happen simultaneously.	Orasanu and Connolly (1993)	Naturalistic Decision Making
31	Multiple decision makers	NDM theory identified that multiple entities interact in the decision-making process. These entities may have either shared or different views of the situation. They must cooperate with one another and update each other in order to perform optimally.	Orasanu and Connolly (1993)	Naturalistic Decision Making
32	Organizational culture	NDM theory states that decision-making activities are embedded in organizations. Organizations have their own unique cultures, which manifest themselves in accepted norms, policies, guidelines, directives, standard operating procedures, and doctrine.	Orasanu and Connolly (1993)	Naturalistic Decision Making

REFERENCES

Alberts, D. S., & Hayes, R. E. (2006). *Understanding command and control*. Washington DC: Office Of The Assistant Secretary Of Defense For Networks And Information Integration, Command Control Research Program. Retrieved from http://www.dodccrp.org/files/Alberts_UC2.pdf.

Alberts, D. S. (2007). *Agility, focus, and convergence: The future of command and control*. Washington DC: Office Of The Assistant Secretary Of Defense For Networks And Information Integration, Command Control Research Program. Retrieved from http://www.dodccrp.org/html4/journal_main.html.

Buchanan, Leigh (19 November 2009). Peter Drucker from A to Z. *Inc. magazine*. Retrieved from: http://www.inc.com/articles/2009/11/drucker.html.

Drucker, P. F. (1998). The coming of the new organization. In *Harvard business review on knowledge management*. Harvard Business Press.

Fonash, P. (2014, December). Public comments in R. Rodriguez (Chair). *SINET Showcase and Workshops 2014*. Symposium conducted in Washington D.C.

Freedberg, S.J., (2014). Moving mountains in cyber war: Automated virtual 'maneuver'. *Breaking Defense.* Retrieved from: http://breakingdefense.com/2014/12/moving-mountains-in-cyber-war-automated-virtual-maneuver.

Galbraith, J. R. (1973). Designing complex organizations. Reading, Massachusetts: Addison-Wesley Publishing Co., Inc.

Galbraith, J. (1974). Organization design: an information processing view. *Interfaces, 4(3)*, 28-36.

Gore, J., Banks, A., Millward, L., & Kyriakidou, O. (2006). Naturalistic decision making and organizations: Reviewing pragmatic science. *Organization Studies*, 27(7), 925-942.

Grisham, T. (2009). The delphi technique: A method for testing complex and multifaceted topics. *International Journal of Managing Projects in Business, 2*(1), 112-130. doi:http://dx.doi.org/10.1108/17538370910930545

Hale, R. (2014, December). Public comments in R. Rodriguez (Chair). *SINET Showcase and Workshops 2014*. Symposium conducted in Washington D.C.

Hoffman, J. (1988). *The effects of strategic and operational decision making structure on organizational performance: Technology as a moderator* (Doctoral Dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 8818630).

Keeney, S., Hasson, F., & McKenna, H. (2011). The delphi technique in nursing and health research. Oxford, United Kingdom: Wiley-Blackwell.

Kramer, F. D., Wentz, L.K. & Starr, S. H. (Eds.). (2009). *Cyberpower and national security*. Dulles, VA: Potomac Books, Inc.

Kuehl, D.T., (2009), From cyberspace to cyberpower: Defining the problem. In Kramer, F. D., Wentz, L.K. & Starr, S. H. (Eds.), *Cyberpower and national security* (pp. 24-42). Dulles, VA: Potomac Books, Inc.

Linstone, H. A., & Turoff, M. (Eds.). (1975). *The delphi method: Techniques and applications* (Vol. 29). Reading, MA: Addison-Wesley.

Lipshitz, R., Klein, G., & Carroll, J. S. (2006). Introduction to the special issue. Naturalistic decision making and organizational decision making: Exploring the intersections. Organization Studies, 27(7), 917-923.

Peterson, M. (2009). *An introduction to decision theory*. Cambridge University Press.

U.S. Department of the Army. (2014). *Field manual 6-0, commander and staff organization and operations*. Retrieved from: http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/fm6_0.pdf.

U.S. Department of Defense. (June 23, 2009). *Establishment of a subordinate unified U.S. cyber command under U.S. strategic command for military cyberspace operations*. Retrieved from: http://online.wsj.com/public/resources/documents/OSD05914.pdf.

U.S. Department of Defense. (2011). *Department of Defense (DoD) information technology (IT) enterprise strategy and roadmap.* Retrieved from: http://dodcio.defense.gov/Portals/0/Documents/Announcement/Signed_ITESR_6SEP11.pdf

U.S. Department of Defense. (2011). *Joint publication 3-0: Joint operations.* Retrieved from: http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf.

U.S. Department of Defense. (2013). *Joint publication 3-12(R): Cyberspace operations*. Retrieved from: www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

U.S. Department of Defense. (2014). *Joint publication 1-02: Department of defense dictionary of military and associated terms*. Retrieved from: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

U.S. Department of Defense. (2015). *Beyond the build - Delivering outcomes through cyberspace: The commanders' vision and guidance for US cyber command.* Fort Meade, MD: United States Cyber Command.

Williams, B.T. (2014). The joint force commander's guide to cyberspace operations. *Joint Force Quarterly, 73,* 12-19. Washington, D.C.: National Defense University.