Military Cyber Affairs

Volume 4
Issue 1 *Command and Control of Cyberspace Operations*

Article 4

October 2019

Command and Control for Cyberspace Operations - A Call for Research

Adam S. Morgan
The MITRE Corporation, asmorgan@mitre.org

Steve W. Stone
The MITRE Corporation, sstone@mitre.org

Recommended Citation

Morgan, Adam S. and Stone, Steve W. (2019) "Command and Control for Cyberspace Operations - A Call for Research," *Military Cyber Affairs*: Vol. 4 : Iss. 1 , Article 4.
https://doi.org/10.5038/2378-0789.4.1.1051
Available at: https://digitalcommons.usf.edu/mca/vol4/iss1/4

Abstract

The United States Department of Defense (DoD) declared cyberspace as an operational domain in 2011. The DoD subsequently formed US Cyber Command and the Cyber Mission Force to conduct operations to achieve national and military objectives in and through cyberspace. Since that time, the DoD has implemented and evolved through multiple command and control (C2) structures for cyberspace operations, derived from traditional military C2, to achieve unity of effort across the global cyberspace domain and with military operations in the physical domains (land, sea, air, and space). The DoD continues to struggle to adapt its command and control (C2) methods from the physical domains to the cyber domain. Applying traditional military C2 constructs to the cyberspace domain leads to several problems due to the uniqueness of cyberspace from the other domains. Cyberspace presents a very different operational environment than the physical domains, where time and space are compressed.

In this paper, we describe the factors that make cyberspace different from the other operational domains and the challenges those differences impose on existing C2 constructs. We propose a campaign of experimentation, consisting of a series Cyberspace C2 experiments, to address these challenges by conducting research into the taxonomy of C2 nodes, decisions, information, and relationships, which can be used to simulate and refine DoD Cyberspace Operations C2 constructs.

1. Introduction

The environment in which the Department of Defense (DoD) operates has been changed by the rapid development and adoption of information technologies such as electronics, telecommunications infrastructures, and information systems[1]. The adoption of these technologies has resulted in the environment known as cyberspace. 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."[2] Cyberspace has increased the amount of information that can be digitally sent anywhere, anytime to almost anyone. The increased access to information has affected human cognition, dramatically impacting human behavior, and decision-making.[3]

The DoD declared cyberspace as an operational domain in 2011. The DoD subsequently formed US Cyber Command and the Cyber Mission Force to conduct operations to achieve national and military objectives in and through cyberspace. The DoD defines cyberspace operations as "The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace."[4]

Since declaring cyberspace as an operational domain, the DoD has implemented and evolved through multiple command and control (C2) structures for cyberspace operations, derived from traditional military C2 doctrine, to achieve unity of effort across the global cyberspace domain and with military operations in the physical domains (land, sea, air, and space).[5]

The DoD defines command and control as, "The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Also called C2."[6] Throughout history, the U.S.

---

[1] Kuehl, D.T. 2009. "From cyberspace to cyberpower: Defining the problem," in *Cyberpower and national security*, ed. Kramer, F. D., Wentz, L.K. & Starr, S. H. Dulles, VA: Potomac Books, Inc.
[2] 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, 63.
[3] Kuehl, "From cyberspace to cyberpower: Defining the problem".
[4] U.S. Department of Defense. *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms*, 63.
[5] Pomerleau, M. February 28th, 2018. "Cyber Command granted new, expanded authorities" in *The Fifth Domain*. Retrieved from: https://www.fifthdomain.com/dod/cybercom/2018/02/28/cyber-command-granted-new-and-expanded-authorities/. And Pomerleau, M. June 22nd, 2018. "DoD makes significant updates to cyber operations doctrine", in *The Fifth Domain*. Retrieved from: https://www.fifthdomain.com/dod/2018/06/22/dod-makes-significant-updates-to-cyber-operations-doctrine/.
[6] U.S. Department of Defense. *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms*, 44.

military has been very effective conducting operations in the physical world and has developed a large body of command and control doctrine for operations in the physical domain. Recently, in response to the changing environment for military operations, the DoD has begun development of new doctrine for multi-domain operations. Multi-domain operations presents a new operational framework, "a cognitive tool to assist commanders to visualize and describe the application of combat power in time, space, and purpose."[7] across all domains (land, sea, air, space and cyberspace).

However, the DoD continues to struggle to adapt its C2 methods from the physical domains (land, sea, air, and space) to the cyber domain. Cyberspace presents a very different operational environment than the physical domains where time and space are compressed.[8] In another definition of cyberspace, Daniel Kuehl states "cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies."[9] Applying traditional military C2 constructs to the cyberspace domain leads to several problems due to the uniqueness of cyberspace from the other domains. In this paper, we describe the factors that make cyberspace different from the other operational domains and the challenges those differences impose on existing C2 constructs. The greatest challenge facing the DoD is that it does not yet understand how to conduct agile C2 of cyberspace operations, nor does it possess strategies to implement agile C2 in the face of the complex dynamics presented by this domain. In 2015, Admiral Mike Rogers, then Commander of US Cyber Command, 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. We must adapt, and soon!"[10] We believe that the DoD must think about cyberspace in a new way and not be imprisoned by its excellence in the physical space which may prevent it from thinking in new ways to meet new challenges.[11]

Statement of the Problem

The DoD is currently applying command and control (C2) concepts developed for operations in physical space to operations conducted in cyberspace. "Because cyberspace is significantly different in both time and space, cyberspace presents a much more dynamic and complex operational environment for the U.S. military.

[7] Perkins, D. G. & Holmes, J. M. 2018. "Multi-Domain Battle, Converging Concepts Toward a Joint Solution", in *Joint Forces Quarterly*, 88, (1st Quarter 2018): 54-57, 55.
[8] Stone, S. 2016. "Factors related to agility in allocating decision-making rights for cyberspace operations." Doctoral dissertation, Robert Morris University.
[9] Kuehl, "From cyberspace to cyberpower: Defining the problem", 28.
[10] 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: 2.
[11] Morgan, G. 2006. *Images of organization*. Thousand Oaks, CA: Sage Publications.

The temporal and spatial differences presented by cyberspace require the military to examine its long-held doctrine for C2 and decision-making."[12]

Purpose of the Paper

In this paper, we describe the factors that make cyberspace different from the other operational domains and the challenges those differences impose on existing C2 constructs. We then propose a series of cyberspace C2 experiments to address these challenges. These C2 experiments will conduct research into a taxonomy of C2 nodes, decisions, information, and relationships, which can be used to simulate and refine DoD cyberspace operations C2 constructs.

Hypothesis and Research Questions

Key to any research proposal is the statement of the hypothesis and clear research questions to be answered. Our hypothesis for this research is:

> Command and Control of cyberspace operations, supporting multi-domain operations, will be most effectively implemented as a hybrid construct of coordinated, collaborative, and edge C2 models, within different decision spaces, and at different levels of war (national/strategic, operational, and technical/tactical).

Our overarching Research Question is:

> How might the U.S. Department of Defense conduct command and control (C2) of cyberspace operations?

The subordinate research questions are:

1. How effective are different C2 approaches at different levels of cyberspace operations (national/strategic, operational, and tactical/technical)?
2. How might differing cyberspace operations C2 approaches support multi-domain operations?
3. What comparative advantages do different cyberspace operations C2 approaches provide?
4. Which cyberspace C2 approaches allow the United States to maintain an advantage over our adversaries?

Methodological Design

We propose a campaign of experimentation exploring agile C2 of cyberspace operations. This campaign of experimentation is a set of related experimental activities that explore and mature knowledge about command and control for

[12] Stone, S., *Factors related to agility in allocating decision-making rights for cyberspace operations*, 11.

cyberspace operations.[13] We propose that this campaign of experimentation conduct a series of experiments, using table-top exercises, constructive simulations, and live simulations, to assess the potential effectiveness of various C2 approaches for cyberspace operations. We believe that this research will add to the body of knowledge in that it will assist the U.S. military in defining the C2 structures and procedures that will enable them to be successful in conducting cyberspace operations as part of the multi-domain operations of the DoD.

Summary

The DoD is struggling to adopt its C2 doctrine, developed for the physical domain, to the cyber domain. "The military officers and civilians leading cyberspace operations have been influenced by their military education and experience in leading military operations in physical space. As such, they are attempting to describe how they will conduct cyberspace operations using the concepts and doctrine from physical operations."[14] This approach may be flawed because the time and space characteristics of cyberspace are significantly different than the physical domain. "To be successful, military operations in cyberspace likely require new and more agile C2 methods."[15] However, it is not possible to completely abandon the existing C2 doctrine as cyberspace operations must be conducted in coordination with military operations in the land, sea, air, and space. Unfortunately, we believe that the current state of the development of C2 for cyberspace operations is based on iterations of trial and error resulting in incremental improvements but lacking an objective way to measure effectiveness. Therefore, research into new approaches to C2 is necessary to achieve success in cyberspace operations.

[13] Alberts, D. S., and Hayes, R. E. 2005. *Code of Best Practice: Campaigns of Experimentation*. Washington DC: Office of The Assistant Secretary of Defense for Networks and Information Integration, Command Control Research Program.
[14] Stone, S., *Factors related to agility in allocating decision-making rights for cyberspace operations*, 14.
[15] Ibid. 12.

2. Military Command and Control Doctrine: The Need for Change

"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."[16] The U.S. military's term to describe its organizational design and decision-making process is command and control (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."[17] Command is the authority that a commander in the armed forces lawfully exercises over subordinates by virtue of rank or assignment. Command also is defined as "An order given by a commander; that is, the will of the commander expressed for the purpose of bringing about a particular action."[18] Control is defined as "Authority that may be less than full command exercised by a commander over part of the activities of subordinate or other organizations."[19]

The DoD has 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.[20]

The U.S. military's C2 doctrine, including decision-making processes, has been developed and refined over years of military operations in the industrial age. However, there is significant debate as to whether these decision-making processes will be effective in the information age. Alberts argues that the traditional DoD C2 approach is no longer sufficient for military operations in the information age. The current DoD doctrine for operations in the physical domains (land, sea, air, and space) has served the U.S. military very well in the past. However, rapid advances

[16] Ibid. 24.
[17] U.S. Department of Defense. *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms*, 40.
[18] Ibid. 40.
[19] Ibid. 50.
[20] U.S. Department of the Army. 2012. *Army doctrine reference publication (ADRP) 5-0. The operations process*, (2012). Retrieved from http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/adrp5_0.pdf, 2-11.

in technology and the 'leveling' of access to advanced technology is eroding the effectiveness of current C2 doctrine.[21]

Recently, the DoD has begun development of new doctrine for Multi-Domain Operations. Multi-Domain Operations doctrine is a response to the realization that the environments where the DoD must operate have been changed by advances in technologies such as cyberspace, electromagnetic spectrum, robotics, artificial intelligence, nanotechnology, biotechnology, three-dimensional printing and others.[22] These advances have led to the realization that the DoD can no longer operate independently in each domain (land, sea, air, space and cyberspace). There is also a realization that the previous doctrine was overly focused on geographic boundaries. Multi-domain operations is a doctrinal concept designed to address the changed operational environment.[23] Perkins and Holmes state, "We must shift from a model of interdependence to one of integration, which includes flexible C2 designs, better integrated communications systems, and development of tailorable and scalable units, and, in key areas, policies that enable adaptability, and innovation."[24]

The adversaries of the United States have developed their own doctrine for using technology, including cyberspace, and information for military operations. For example, recent Russian operations in Ukraine and Crimea present an example of an adversary effectively using cyberspace and information, in tight integration with the physical domains, to achieve their operational and strategic objectives. Analysis of Russian cyberspace operations in Ukraine point out potential weaknesses in the U.S. DoD's doctrine for cyberspace operations, specifically the treatment of cyberspace as another physical domain. In their 2015 paper, *Brandishing the Cybered Bear: Information War and the Russia-Ukraine Conflict*, Unwala and Ghori state, "For the United States, the 'information war' concept is divided up into different doctrines and policies as if it were another physical domain of war."[25] While Russia's integrated use of cyberspace operations and information warfare in tight synchronization with operations in the physical domains demonstrated significant success. "It is possible that this synergistic potential of warfare is only realized through Russia's holistic conceptualization of "information war," rather than the U.S. categorization of cyberspace operations versus information operations, military information versus non-military information, and offensive capabilities versus defensive capabilities."[26] When applied to the cyber domain, the current DoD C2 doctrine is lacking the speed and agility necessary to effectively conduct cyberspace operations in support of multi-domain operations.

---

[21] Alberts, D. S. 2007. "Agility, focus, and convergence: The future of command and control." The International C2 Journal 1. No. 1 (2007). Retrieved from http://www.dodccrp.org/html4/journal_main.html.

[22] Perkins, D. G. & Holmes, J. M., "Multi-Domain Battle, Converging Concepts Toward a Joint Solution"

[23] Ibid.

[24] Ibid. 57.

[25] Unwala, A. & Ghori, S. 2015. "Brandishing the Cybered Bear: Information War and the Russia-Ukraine Conflict," *Military Cyber Affairs*, (Volume 1, Issue 1, Article 7, 2015), 9. Available at: http://scholarcommons.usf.edu/mca/vol1/iss1/7

[26] Ibid. 9.

Differences in the Cyberspace Domain

Cyberspace is inherently different than the physical domains. Alexander Klimburng states, "… the tradition of viewing cyber as just another domain obfuscates significant differences between cyber and air, land, sea or space."[27] Cyberspace has a number of significant differences from the physical 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."[28] Because cyberspace is man-made and the hardware, software and data comprising cyberspace can change rapidly, cyberspace lacks the "object permanence" of the physical domains.[29] Kallberg and Cook from the Army Cyber Institute state, "Our C2 doctrine does not envision an environment where objects can appear, disappear, reappear, and change at computational speed."[30]

Second, the "terrain" of cyberspace is incredibly complicated, comprising millions of separate hardware devices, running software with millions of potential settings, and processing millions of bits of data.[31] The conditions in the cyberspace domain are largely determined by software and there are a large number of actors, including the private sector, affecting conditions and changing the 'terrain'.

Third, Cyberspace is also global in nature. Unlike the effect of most weapons in the physical domains, effects in cyberspace are not limited to a geographical region. This creates an asymmetry between the cyberspace battlefield and the physical battlefield that must be taken into account.

Another difference in cyberspace is that actions can happen extremely rapidly. Conflicts can be executed at computational speed and are not bound by time and space in the same way that physical effects. "Cyberspace is significantly different in both time and space, cyberspace presents a much more dynamic and complex operational environment for the U.S. military."[32]

When compared to the physical domains, the DoD has limited observation of the cyberspace domain. The vast quantities of data available and the computational speed of operations result in a limited ability to see and assess actions in cyberspace, resulting in limited ability to measure the of effectiveness of operations and a limited ability to attribute activity to real world actors resulting in significant anonymity in cyberspace.[33]

---

[27] Klimburg, A. 2018., *The Darkening Web: The War for Cyberspace*. New York, NY: Penguin Books: 138.

[28] Stone, S., *Factors related to agility in allocating decision-making rights for cyberspace operations*: 19.

[29] Kallberg, J. & Cook, T. S. 2017. "Unfitness of Traditional Military Thinking in Cyber", *IEEEAccess,*Volume 5: 8126-8130.

[30] Ibid, 8127.

[31] Stone, S., *Factors related to agility in allocating decision-making rights for cyberspace operations*.

[32] Ibid. 11.

[33] Kallberg, J. & Cook, T. S., "Unfitness of Traditional Military Thinking in Cyber".

Cyberspace also lacks the commonly accepted behavior norms present in the physical domains. Klimburg states, "… the other domains work under implicit rules – both international laws and commonly accepted norms of behavior – that constrain not only the most dominant actor but also others."[34]

Also different is the concept of maneuver in cyberspace. While maneuver in the physical domains is routinely understood as either "the movement to place ships, aircraft, or land forces in a position of advantage over the enemy."[35] or the "employment of forces in the operational area through movement in combination with fires to achieve a position of advantage in respect to the enemy."[36] this understanding likely does not hold in cyberspace. One might consider the concept of 'maneuvering' in cyberspace as changing the configuration of a series of hardware, software, and data to achieve the desired effect.

And finally, in the DoD the cyberspace offensive and defensive forces and capabilities are more distinct than other domains. Only in cyberspace has the DoD intentionally created separate offensive and defensive forces.

These difference present significant challenges to the DoD's C2 doctrine. Thus, the DoD needs to conduct research into future command and control for cyberspace operations.

Theoretical Model of Command and Control

In order to accurately frame the C2 challenges for cyberspace operations it is necessary to identify an appropriate model of the C2 space to assess the problem. The review of the literature identified a model of the C2 space developed by the Department of Defense Command and Control Research Program. This model, developed by Dr. David Alberts and Dr. Richard Hayes, describes three dimensions of a theoretical model of C2. Alberts and Hayes describe three dimensions of a theoretical model (see Figure 1) of C2 that are useful to examine the cyber C2 space: The organization's allocation of decision-making rights, the organization's patterns of interaction, and the organization's distribution of information.[37]

[34] Klimburg, A. *The Darkening Web: The War for Cyberspace*: 138.
[35] U.S. Department of Defense. *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms*, 153.
[36] Ibid.
[37] 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.

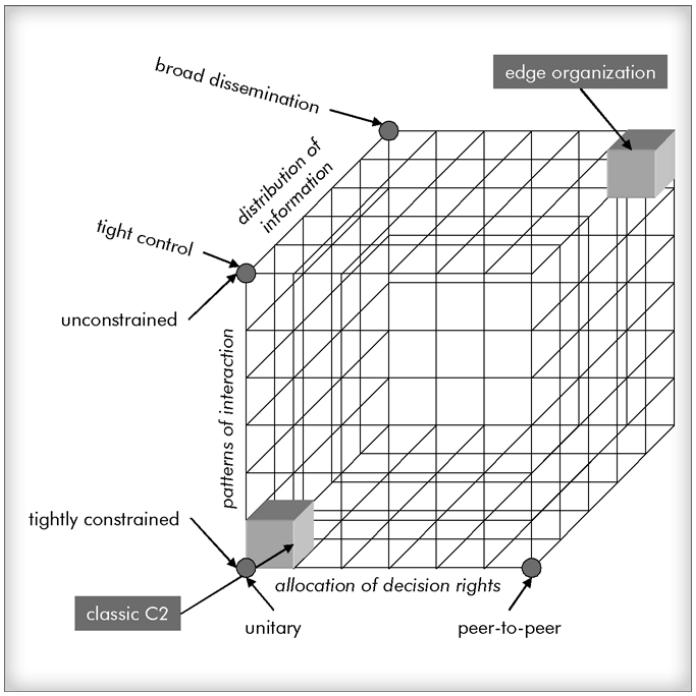

Figure 1. Alberts and Hayes' Model of Command and Control.[38]

This theoretical model of command and control can be visualized as a three-dimensional matrix, with each factor represented as one axis of a cube. Alberts describes the model as having the allocation of decision rights on the horizontal axis, the patterns of organizational interaction on the vertical axis, and the distribution of information along the depth axis. The inside of the cube represents the sample of all possible command and control arrangements. Any approach to accomplishing command and control of a military operation requires making a choice in each of the three related dimensions.

This model presents a framework for understanding the C2 challenges facing cyberspace operations. Each plane of this model provides an aspect of command, control and situational awareness (SA). SA is a critical enabler of C2 and effective C2 cannot be conducted in the absence of a sufficient level of SA. In any operation, there are one or more nodes in the C2 structure. Situational awareness is based on the patterns of interaction, who, when, etc. the entity interacts with other nodes, and distribution of information, what information is available and understandable by the node. A node's ability to command an operation is based on the patterns of interaction and the allocation of decision rights, how much authority, influence, and autonomy does the node have? A node's ability to control an effect is based on the node's situational awareness and allocation of decision rights.

[38] Reprinted from *Understanding Command and Control* by D.S. Alberts & R. E. Hayes, 2006, p. 75. Copyright 2006 by the Office of the Assistant Secretary of Defense for Networks and Information Integration, Command Control Research Program. Reprinted with permission.

Patterns of Interaction

Patterns of interaction describe how organizations interact in conducting command and control. At the origin of this axis, patterns of interaction are tightly controlled. At the opposite end of this axis, organizational interactions are unconstrained. In current DoD operations, the patterns of interaction are largely determined by the command and control relationships established in the orders directing the operation. As current military operations usually involve large organizations consisting of subordinate organizations distributed in a hierarchical manner, the patterns of interaction in a classic C2 structure are designed to ensure control from the center. Hence, the pattern of interaction follows the chain of command established for the operation. In C2 of today's cyberspace operations, these orders, with the corresponding C2 relationships, reporting structures, and flow of information are not fully optimized. Using these traditional patterns of interaction as defined by current DoD C2 doctrine may not be optimal for C2 of cyberspace operations.

However, in cyberspace operations, patterns of interaction can be considered networks.[39] The technology underpinning cyberspace makes it possible for all entities participating in a military operation to communicate. Effective communication enables collaboration, working together toward a common purpose, which is the most desirable pattern of interaction.[40] Collaboration involves actors actively sharing data, information, knowledge, perceptions, or concepts when they are working together toward a common outcome and how they might achieve that outcome efficiently or effectively.[41] Collaboration provides the opportunity for the parties to exchange views about the clarity of the data and information, as well as what it means or implies, not just to receive information.[42]

Distribution of Information

Information is a strategic asset and it is critical to the conduct of military operations. How information is distributed affects the ability of an organization to deal effectively with the challenges it faces. The distribution of information can be thought of as ranging from fully centralized repositories to a fully distributed approach where everyone has access to everything. At the origin of this axis, information is typically stored in a central location and the access of each user was predetermined and controlled by a central authority. At the opposite end of the axis, advances in communications and information technologies and the accompanying changes in the economics of information made it feasible to distribute information much more widely and make it accessible to all.

---

[39] Ibid.
[40] Ibid.
[41] Alberts, D. S., Garstka, J. J., Hayes, R. E., & Signori, D. A. 2001. *Understanding information age warfare*. Washington DC: Assistant Secretary Of Defense, C3I/Command Control Research Program.
[42] Alberts & Hayes, *Understanding command and control*.

The Distribution of information axis is significantly affected by the prevalence of large amounts of rapidly changing data, commonly called 'Big Data'. Big Data presents new opportunities to enhance a commander's understanding of the situation, but it is complex to process and interpret this data in order to have true Situational Awareness (SA) at all levels of operations – national/strategic, operational, and technical/tactical. Situational Awareness can be described as "…users must understand how their individual actions contribute to a greater whole. In other words, they must be aware of the same data and share the same legal, social, and cultural context to interpret that data."[43] Interpreting that data can be described as sensemaking, "Sensemaking consists of a set of activities or processes in the cognitive and social domains that begins on the edge of the information domain with the perception of available information and ends prior to taking action(s) that are meant to create effects in any or all of the domains."[44]
It is also a challenge to effectively distribute this data. The prevalence of large amounts of data has led to the tendency that everyone wants to see all of the data. Distributing data effectively to the right people and organizations who need the data in order to make effective decisions is a challenge.

Allocation of Decision Rights

The allocation of decision rights is a linear dimension with two logical endpoints. At the origin of the allocation of decision rights on the horizontal axis, decision-making rights are unitary, all the rights held by a single actor. At the other end of the axis, decision-making rights are allocated uniformly with every entity having equal rights in every decision. Using current DoD C2 doctrine, decision rights are usually established by the C2 relationships directed in the orders authorizing the operation. Command and control relationships such as operational control (OPCON), and tactical control (TACON) establish the decision rights that a commander may exercise.[45]

Decisions are choices among alternatives. The U.S. Department of Defense defines a decision as "…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."[46] Cyber C2 decisions can be broken into categories along two dimensions, the level of operations and the decision latency. Figure 2 depicts these two dimensions of decision making for cyberspace operations.

On the first dimension, there decisions made at the national/strategic, operational, and tactical/technical levels of cyberspace operations, modeling the traditional levels of military operations. At the national/strategic level of cyberspace

[43] Pitt, J., Bourazeri, A., Nowak, A., Roszczynska-Kurasinska, M., Rychwalska, A., Rodríguez Santiago, I., Lopez Sanchez, M., Florea, M., & Sanduleac. M. 2013. "Transforming big data into collective awareness". *Computer* 46, no. 6: 40-45.
[44] Alberts, D. S., & Hayes, R. E., *Understanding command and control*: 64.
[45] U.S. Department of Defense. *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms*: 183 and 242.
[46] Ibid: 62.

operations, the decision made are likely answering the question: How do we use cyberspace to achieve our National objectives? At the operational level, the relevant question is: How do we use 'cyberspace to achieve the JFC objective(s)? And at the technical/tactical level decisions are usually made to answer the question: How do we change the configuration of the hardware, software or data to achieve the operational objective?

The second dimension of decision making is the time available to make the decision. Decisions made at the technical/tactical level are frequently made in seconds, minutes or hours. At the operational level, there are often hours or days available to make decisions. And at the national/strategic level, decision makers usually have days or months available to make a decision. These decisions happen across the operations process: planning, preparing, executing, and continuously assessing the operation.[47]

In determining the allocation of decision rights across the many nodes in a C2 structure operating across the levels of operations, it is often difficult to balance between enabling operational and tactical entities with proper authority while maintaining the unity of effort and unity of command necessary to achieve the operational and national/strategic objectives. In most cyberspace operations there is significant interdependence between peers at the tactical level requiring higher-level orchestration, but higher-levels often don't have the visibility and expertise to make timely and effective decisions

Boyd's OODA Loop Applied to Cyberspace Operations

Another C2 model relevant to cyberspace operations is Boyd's OODA loop. Much of the current DoD C2 doctrine is based on the observe, orient, decide, act (OODA) loop developed by John Boyd in the 1960s and follows the steps of observe, orient, decide, act.[48] Executing cyberspace operations can be represented as nested and interrelated OODA loops. Specifically, based on the C2 model implemented, there are interrelated OODA loops at every C2 node. For example, OODA loops at the operational level direct and inform OODA loops at the tactical/technical level. There are nested OODA loops within each C2 node as the node conducts current operations, crisis action planning, near-term planning, and long-term planning.

[47] U.S. Department of the Army, *Army doctrine reference publication (ADRP) 5-0. The operations process*.
[48] Boyd, J. 1987. *Organic Design for Command and Control*. Retrieved from: https://www.colonelboyd.com/s/Organic-Design-for-C2_May-1987.pdf.

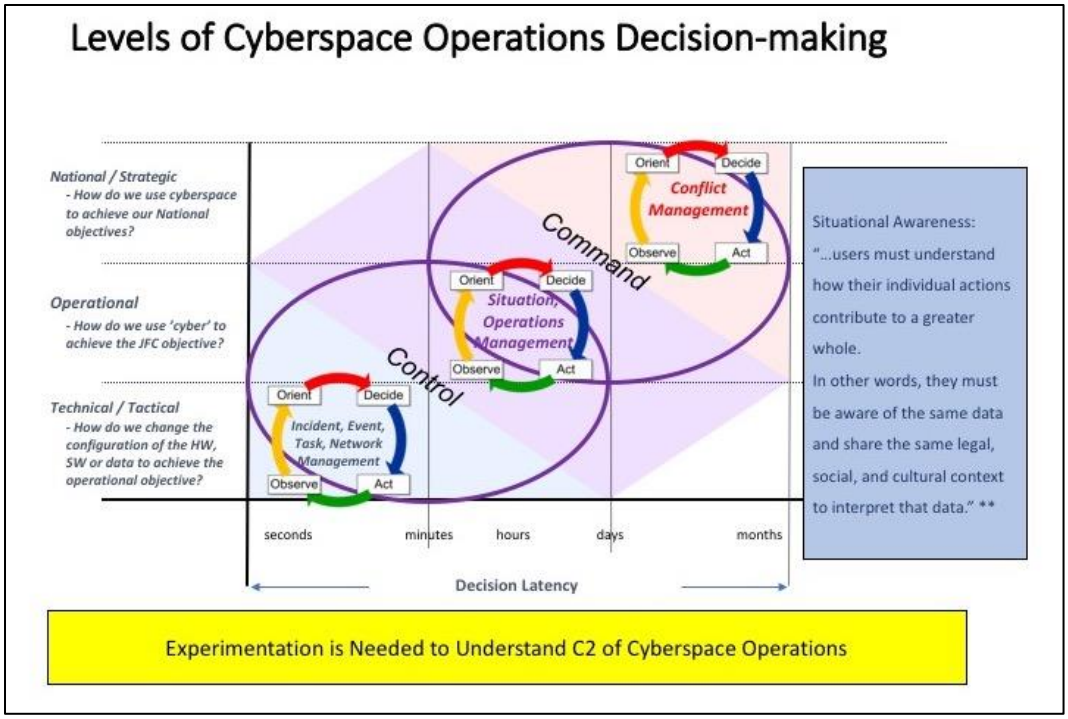

Figure 2. Levels of Cyberspace Operations Decision-making.

The OODA loop requires the ability to observe and assess ongoing events , but under conditions of anonymity, limited observation, computational speed in cyber execution, lack of object permanence, and differences in time and space, the observations feeding the loop are likely to be inaccurate.[49]

Summary

Cyberspace presents a complicated operational domain that behaves much differently than the physical operational domains, land, sea, air, and space. Alberts and Hayes hypothesize that complex dynamic environments, like cyberspace operations, require more agile approaches to C2. Albert and Hayes' hypothesis is that agile C2 requires the organizational ability to rapidly change their approach towards each of the three variables in the theoretical model of C2.[50] To address these challenges in C2 of cyberspace operations, it is necessary for the DoD to conduct research into the taxonomy of C2 nodes, decisions, information, and relationships, which can be used to simulate and refine DoD cyberspace operations C2 constructs.

[49] Kallberg, J. & Cook, T. S., "Unfitness of Traditional Military Thinking in Cyber".
[50] Alberts & Hayes, *Understanding command and control*.

3. Proposed Experimentation into Future Cyberspace Operations Command and Control

As section 1 describes, to gain insight into C2 within the cyber domain, integrating it with C2 within multi-domain operations, and to answer the research questions posed, a campaign of experimentation is needed. This campaign of experimentation is a set of related experiments that explore and mature knowledge about command and control for cyberspace operations. It will iteratively gather data on the execution of different C2 approaches to evolve our understanding of the comparative effectiveness and efficiency of different C2 approaches, within the context and limitations of the set of discrete experiments conducted. This campaign does not have a defined end point, but instead is focused on continual learning to ultimately improve our understanding of where and when to employ different C2 models and how to execute within a given C2 construct.

Each discrete experiment within the campaign has the following components, described in additional detail in the following sections:

- Independent Variable: A set of C2 models, that consist of nodes, roles, and relationships, that will be independently tested within the experiment
- Dependent Variables: A set of metrics that measure the effectiveness and efficiency of C2 execution and the components of the C2 approach
- Constant: A realistic operational scenario, with defined mission objectives, injects, and operating environment (including communication delays, error rates, and other inherent conditions of cyberspace) that tests each C2 model through the execution of cyberspace operations
- Experimental Group: A set of subject matter experts and/or automated agents that conduct Cyber C2 within the experiment

Observations throughout the experiment, leveraging a well-instrumented experimental platform, will enable calculating the dependent variable and enable intermediary inferences about the relative advantages and disadvantages of the tested C2 models. For an individual experiment, these inferences are limited to the specific scenario built into the experiment; the explicit and implicit assumptions built into that scenario; the knowledge, skill, and biases built into the experimental group; and potentially other unknown biases and measurement error built into the experiment. However, building on individual results over a diverse campaign of experimentation, will balance out many of these caveats and allow maturing our understanding and increasing our confidence in the conclusions on the application of different C2 models in the cyber domain.

Representative C2 Models

The theoretical model for command and control, discussed in section 2, represents the entire trade space for C2 approaches that can be applied to cyberspace operations. Within that 3-dimensional model a variety of C2 approaches can be extracted and modeled for experimentation from a tightly constrained, conflicted approach to a highly-collaborative peer-to-per network, and numerous variations in

between. As a starting point for research into Cyber C2, five models that were presented in the NATO C2 Agility SAS-085 report are useful.[51] These models, depicted below in Figure , consist of conflicted, de-conflicted, coordinated, collaborative, and edge models. Over the course of the campaign of experimentation, these five models may be blended or adapted into different models based on the observations and conclusions made through experimentation.

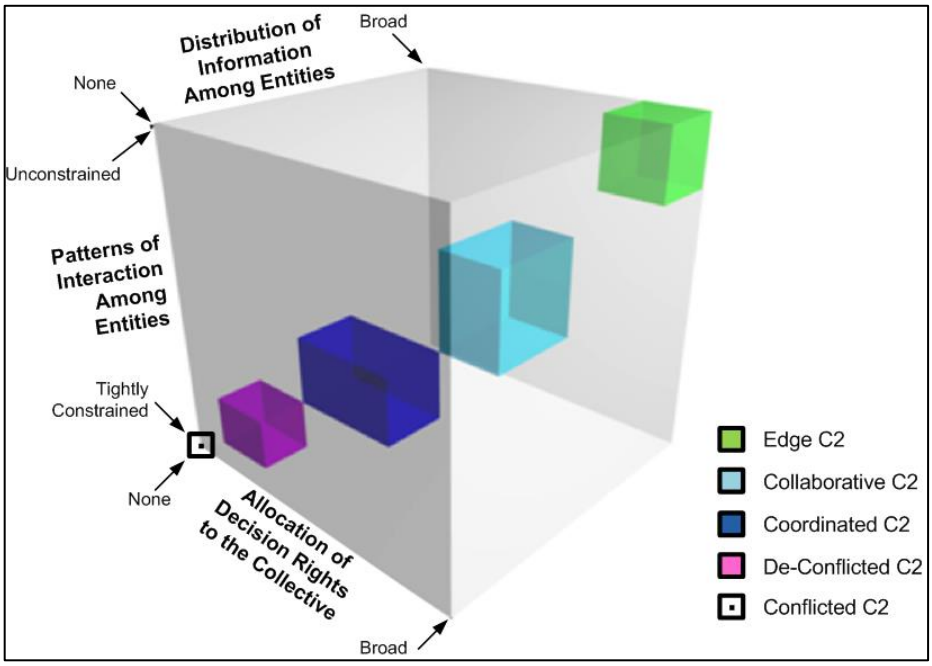

Figure 3: Preliminary C2 Models[52]

The inherent characteristics of these models are and their potential implications for cyberspace operations are described in the sections below.

[51] North Atlantic Treaty Organization, Research and Technology Organization. 2013. *Task Group SAS-085 Final Report on C2 Agility*. Retrieved from: http://www.dodccrp.org/sas-085/sas-085_report_final.pdf.
[52] Ibid.

Conflicted C2

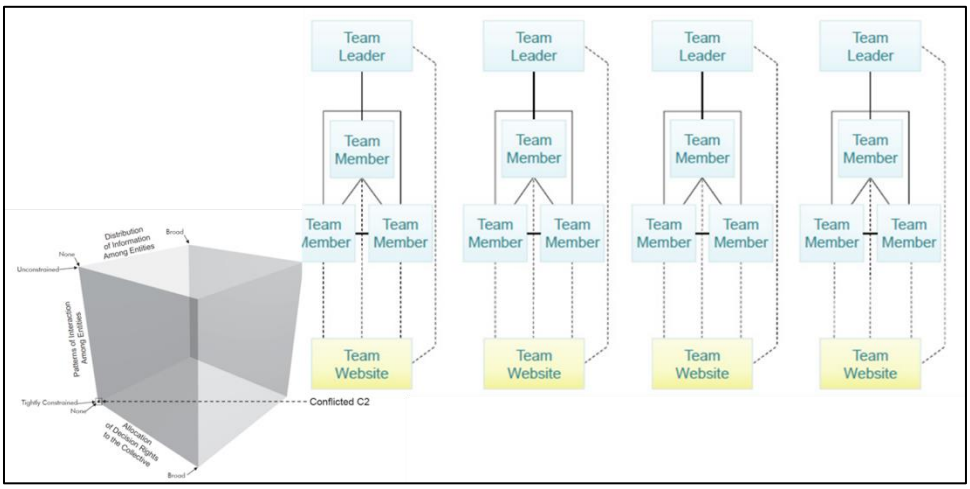

Figure 4: Conflicted C2[53]

The Conflicted C2 model is characterized by multiple independent organizations with no collective objective, no distribution of information or interaction between organizations, and no coordination of decisions. In cyberspace operations, this may make each organization more autonomous, and thus more agile, but the lack of visibility and coordination may also lead to conflicts and inefficient actions across peers due to their interdependence within the global domain.[54]

[53] Adapted from: North Atlantic Treaty Organization, Research and Technology Organization. *Task Group SAS-085 Final Report on C2 Agility*.

[54] North Atlantic Treaty Organization. 2010. *Network Enabled Capability C2 Maturity Model*. Washington DC: Assistant Secretary Of Defense, C3I/Command Control Research Program. Retrieved from: http://www.dodccrp.org/files/N2C2M2_web_optimized.pdf.

Deconflicted C2

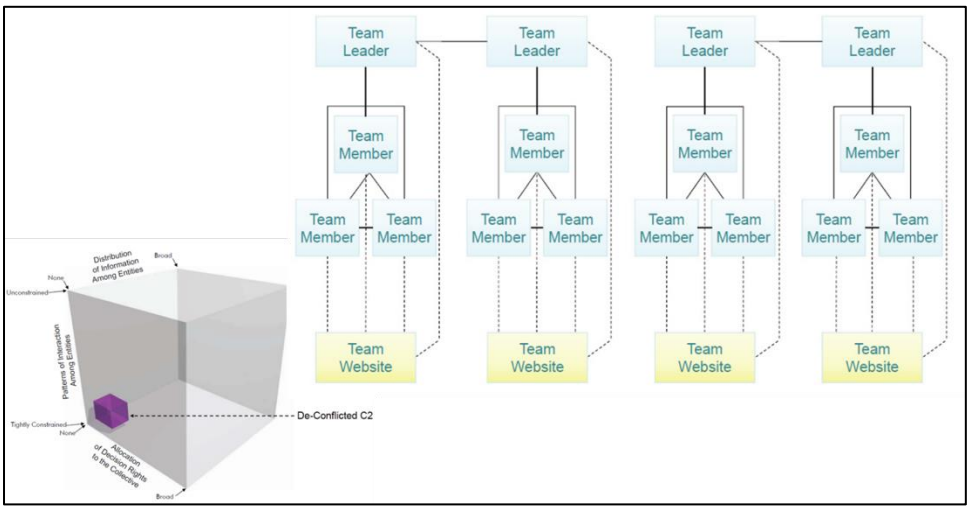

Figure 5: Deconflicted C2[55]

The Deconflicted C2 model adds a minimal amount of information flow between organizations in order to deconflict intents, plans, and actions. This model can enable partitioning of responsibility across the cyberspace domain, functions, capabilities, and/or time. However, the model only consists of limited information sharing and interaction, and no overarching authority to align individual teams' objectives. Thus, there may not be common sensemaking across organizations, decision-making is not aligned to joint objectives, and actions may not reflect a unity of effort across organizations.[56]

[55] Adapted from: North Atlantic Treaty Organization, Research and Technology Organization, *Task Group SAS-085 Final Report on C2 Agility*.
[56] Ibid.

Coordinated C2

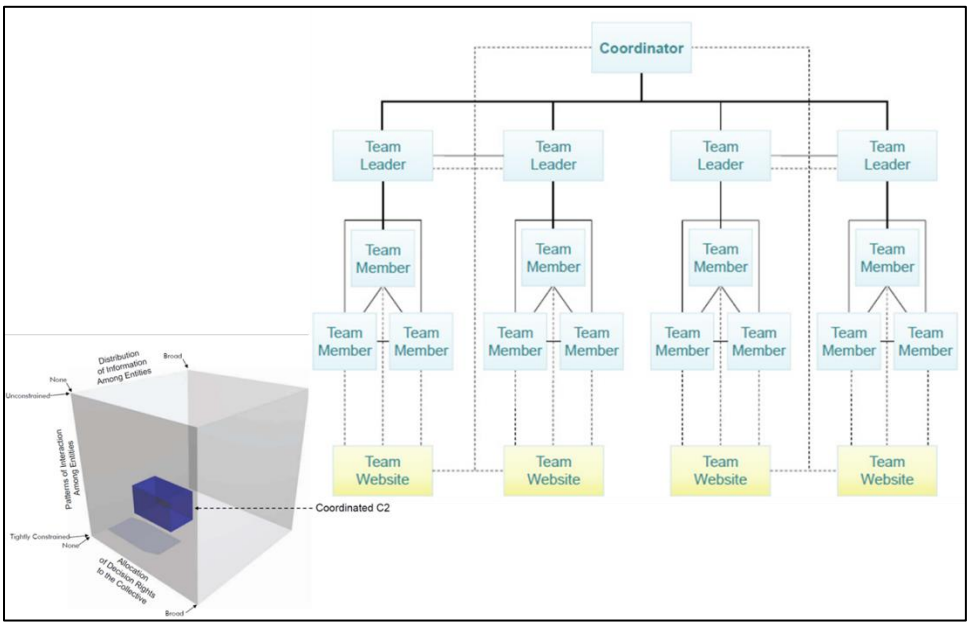

Figure 6: Coordinated C2[57]

The Coordinated C2 model is characterized by the development of a common intent and an agreement to adjust and constrain plans and decisions based on that intent. It involves more information sharing, interaction, and additional delegation of decision-making rights to the collective. It falls short of continuous interaction between organizations but does incorporate an additional organization to deliberately coordinate plans, decisions, and actions. In cyberspace operations, this coordination may improve the synchronization of strategic-level plans and objectives down to overlapping tactical/technical actions within the domain.[58]

[57] Adapted from: North Atlantic Treaty Organization, Research and Technology Organization, *Task Group SAS-085 Final Report on C2 Agility*.
[58] Ibid.

Collaborative C2

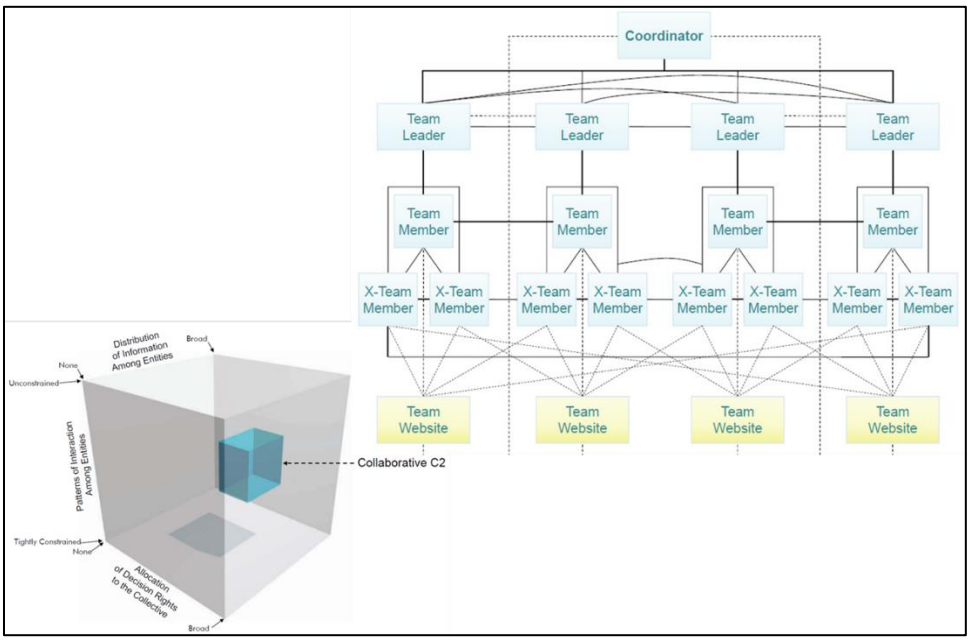

Figure 7: Collaborative C2[59]

The Collaborative C2 model is characterized by the development of a single shared plan, defined roles within a larger C2 construct, sharing and pooling of resources, and shared sensemaking. The Collaborative C2 incorporates significant delegation of decision-making authorities to the collective, while maintaining distributed execution. This model promotes a tight unity of effort, which may be essential to maintain alignment of cyberspace operations to broader military objectives, but given the complexities of the cyberspace domain, it may also present challenges for effective and efficient execution. These challenges may include developing high-quality SA across a broad cyberspace operations mission, accurate and actionable decision making, and coordinating the tactical/technical implications of those decisions. [60]

[59] Adapted from: North Atlantic Treaty Organization, Research and Technology Organization, *Task Group SAS-085 Final Report on C2 Agility*.
[60] Ibid.

Edge C2

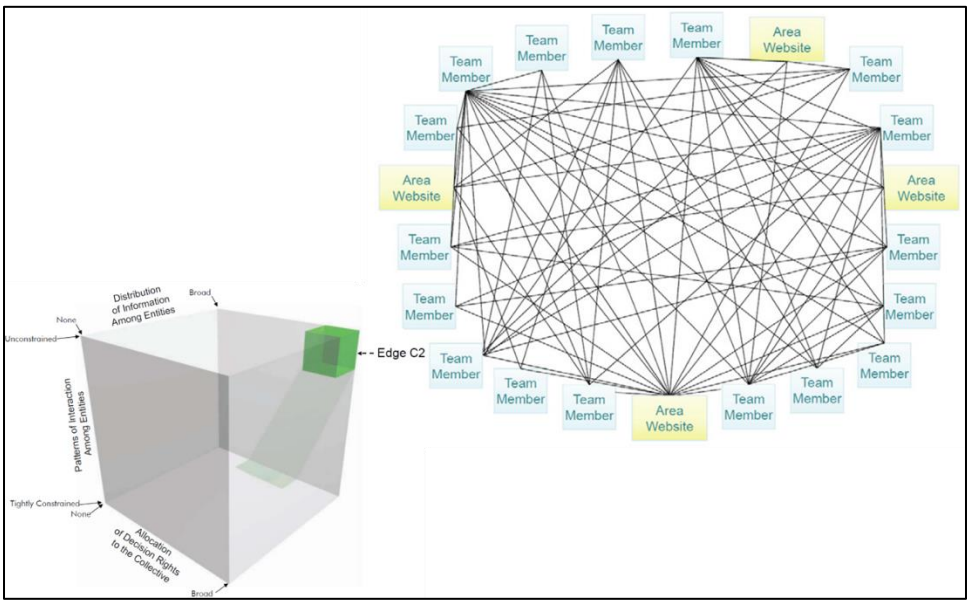

Figure 8: Edge C2[61]

"An Edge approach to C2 distinguishes itself from the other C2 approaches by replacing deliberate and formal coordination and collaboration mechanisms with the dynamics of emergence and self-synchronization."[62] . The self-synchronization enables a subset of organizations to employ other C2 models for limited time or purpose, while retaining broader authorities and decision-making rights. In cyberspace operations, a completely distributed C2 model, such as this edge approach, should promote improved situational understanding and sensemaking, but the distributed construct may also inhibit the development of a shared plan or unity of effort through execution. The effectiveness in this model is highly dependent on the details of its implementation and the capabilities that enable it – how is consensus on plans and decisions developed and orchestrated across organizations? An edge model has potential for more direct and effective information sharing, interactions, and delegation of decision-making rights, but it remains that evidence of that potential still needs to be collected and analyzed.[63]

Dependent Variables

To gain insight into Cyber C2 and measure the effectiveness and efficiency of the C2 approaches described above, experiments must be constructed to measure the ability for the C2 model to produce overall mission effectiveness. In addition, the

[61] Adapted from: North Atlantic Treaty Organization, Research and Technology Organization, *Task Group SAS-085 Final Report on C2 Agility*.
[62] Alberts, D. S., & Hayes, R. E. 2003. *Power to the edge: Command... control... in the information age*. Washington DC: Office of The Assistant Secretary of Defense for Networks and Information Integration, Command Control Research Program.
[63] Ibid.

experiment must also measure the quality of the components of the C2 approach, to include quality of command, quality of control, quality of sensemaking, quality of execution, and information quality. The below model, from *Understanding Command and Control*, depicts these 6 measures of the proposed experiments.

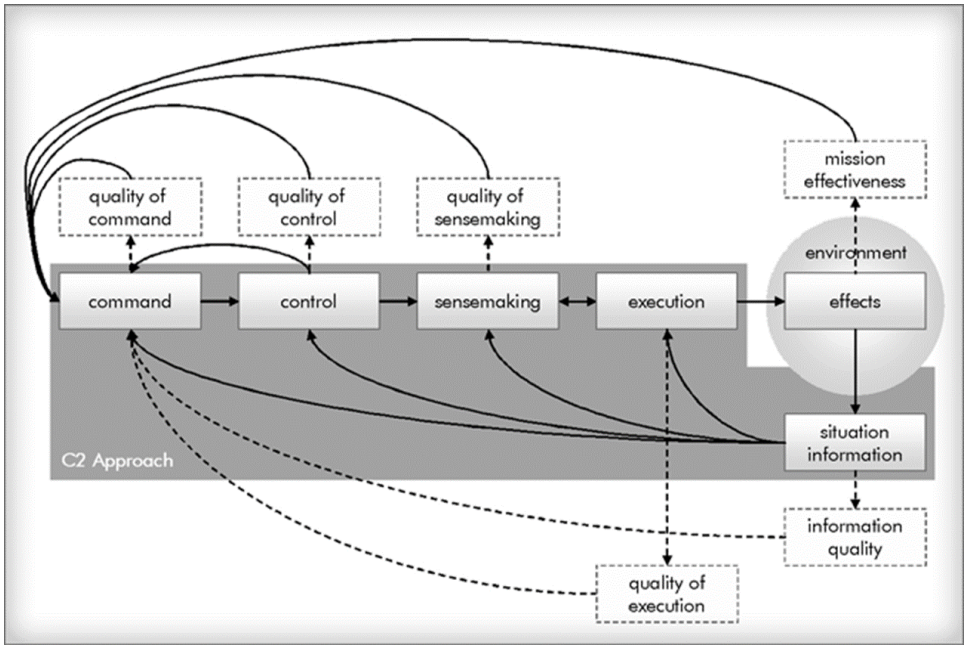

Figure 9: C2 Approach[64]

These six measures must be further decomposed into discrete metrics that can be built into an experiment. The following table delineates a preliminary set of metrics that can be used in comparative analysis of the C2 models.

[64] Alberts & Hayes, *Understanding command and control*.

DOI: https://doi.org/10.5038/2378-0789.4.1.1051

C2 Measure	Description	Metric
Mission Effectiveness	The overall measure of C2 model effectiveness in a scenario	• # Mission tasks completed • # Mission Objectives achieved
Quality of Command	Can Decisions be made?	• Time to converge on a decision • # conflicted decisions
Quality of Control	Can decisions be executed?	• % Decisions Executed • Time to execute decisions
Quality of sense-making	Do nodes arrive at good/similar SU?	• % of nodes with understanding matching reality • % of nodes with same understanding
Quality of execution	Are actions taken effective given reality and performed with unity of effort?	• # conflicted actions • # coordinated actions
Information quality	Can information be collected and distributed efficiently?	• Distribution of information - % of nodes receiving information element • % of information accuracy

Table 1: Metrics Collected during Experiment

Experimental Scenarios

The challenge with C2 experimentation within cyberspace is to construct individual experiments that are highly relevant to real-world situations and challenges. There are many considerations and compromises to make. The following characteristics will inform scenario development:

- Relevant to current challenges in cyberspace operations
- Abstract, modifiable, and extensible such that it be fully modeled and reused over multiple rounds of experimentation
- Simple enough so that it can be developed and conducted in reasonable time
- Difficult enough that it is not trivial to accomplish regardless of C2 model used

- Comprehensive in its range of difficulties, so that the characteristics of the cyberspace domain are relevant and the effects of changes in C2 model are observed[65]

Revisiting the differences in the cyberspace domain from section 2, in each scenario crafted for experimentation, certain assumptions need be made about the domain conditions, its actors, and their capabilities. To ensure an experiment is targeting the challenges that emerge in conducting C2 of cyberspace operations that hinder traditional C2 approaches, those differences must be influential within the scenario under experiment. For example, the following questions can inform scenario development around a few of the differences identified:

- Will objects in the domain disappear, be created, or be reconfigured and with what speed and frequency? (Man-made domain)
- What level of visibility, and what level of accuracy, will participants have within the domain and how will that change over time? ("Terrain" is incredibly complicated, Activities can happen extremely rapidly)
- How much overlap in responsibilities exists across different C2 nodes' Area of Operation? (Cyberspace is an interdependent, global domain)

Additionally, the scenarios must account for decision making at the strategic, operational and tactical/technical levels along with execution at the local, regional, and global levels (e.g., the decision to make a global configuration change is tactical/technical in nature despite being a global action). Since geography largely aligns with command and control in the physical domain (Global/Strategic, Regional/Operational, and Local/Tactical), and cyberspace operations must integrate C2 into multi-domain operations, the scenarios must also explore the variations in the levels of decision making in cyberspace operations, and how it integrates with multi-domain C2.

Finally, the scenarios must account the variation of national/military objectives and effects achieved both in and through cyberspace and how effective a C2 model is in achieving different types of objectives (and countering an adversary's objectives). Effects achieved in cyberspace include IT service disruptions and degradations or loss of data confidentiality, availability and integrity. Effects through cyberspace can include kinetic effects that disrupt or destroy physical systems and/or cause human injury or loss of life. It also includes cognitive effects, including exploiting individual or groups' cognitive vulnerabilities - a premise that the audience is already predisposed to accept because it appeals to existing fears or anxieties.[66] A C2 model may be effective at maintaining IT service levels, but

[65] Ruddy, M. 2007. "ELICIT --The Experimental Laboratory for Investigating Collaboration, Information-sharing and Trust." In *Proceedings 12th International Command and Control Research and Technology Symposium*, Newport, RI. Retrieved from: https://calhoun.nps.edu/bitstream/handle/10945/31228/ICCRTS07_Ruddy.pdf?sequence=1.

[66] Waltzman, R. 2017. *The Weaponization of Information, The Need for Cognitive Security.* Washington, DC. The RAND Corporation. Retrieved from: https://www.rand.org/pubs/testimonies/CT473.html.

could lack the ability to counter an Information Operation targeting a Force's cognitive vulnerability.

Following are three experimental scenarios that seek to address the challenges with realistically modeling the environment and account for uniqueness in the cyberspace domain. These scenarios act as a starting point for experimentation, but must be enhanced and broadened as experimentation matures, lessons are learned, and new research questions and hypothesis are presented.

1. Supporting a local commander with mission critical services from an external service provider – The Cyber domain is inherently global – and shared – forcing commanders to rely on external service providers, possibly with different priorities and situational understanding, to provide services critical to mission success. Managing competing priorities by commanders across an organization as large as the DoD is challenging. The scenario will inject a directed cyber-attack by an adversary the commander is engaged with in a multi-domain battle. Relaying the urgency, pertinent information, and sharing threat intelligence with the external service provider will be critical to defining the mission critical service for the commander.
2. Coordinating offensive and defensive forces in the cyber domain against an adversary – Cyber is the unique in that offensive and defensive forces are distinct, creating another layer of needed coordination when engaging with an adversary. An offensive attack to support military objectives may be met with a response from the adversary, requiring defensive forces to be aware of offensive actions that can cause blowback. The defensive forces will need access to intelligence to improve their readiness. Similarly, internal defensive actions can be supplemented with offensive actions intended to disrupt or deny the adversary actions, or to provide a deterrence against future actions. The scenario will test the collaboration and unity of effort between offensive and defensive forces given different C2 constructs.
3. Defending against persistent adversaries with methods that impose a cost to the adversary that is more than they gain from an attack – Traditional defensive actions attempt to detect adversaries, attempt to remove them from compromised networks, and harden defensives to prevent them from returning. These actions are easy for persistent adversaries to evade in future attacks through small modifications in their techniques and tools. This makes defense much more expensive than offense in the cyber domain, putting less aggressive organizations at a disadvantage. Further, it disincentivizes the adoption of cyber norms during peacetime. Tipping the equation so that defensive forces can inflict more cost on persistent adversaries requires more intelligence, more coordination of response actions, and more consideration of multi-domain or whole-of-government responses. This scenario will test whether C2 constructs can effectively collaborate on adversary actions and effectively coordinate more complex responses than the detect, mitigate, and recover actions that are typically employed.

Research Design

The research will be conducted through a series of online experiments to compare the relative efficiency and effectiveness of *command and control (C2)* organizational structure within the cyber domain in performing tasks that require decision making and collaboration. The experiments will be based on scenarios that inject the unique challenges within the cyber domain discussed in section 2. It will include subject matter experts and/or simulated roles interacting through a messaging interface to share situational awareness, collaborate and coordinate decisions and actions, provide directions to subordinate organizations, and to confirm task completion. Based on the C2 models discussed, the experiment will measure mission effectiveness and the components of C2 contributing to it – quality of command, quality of control, quality of sense-making, quality of execution, and information quality.

Data Collection and Analysis

Through the experiment, messages between nodes in the C2 model will be collected to measure timing, accuracy, and state of activity (e.g., task completion, decision made). This data will be aggregated and processed to provide a quantitative result of the metrics implemented in the experiment for each of the six measures of a C2 model, described at the beginning of section 3. Across multiple runs of the experiment, including runs of each C2 model under test, it will be possible to rank order the C2 models for each measure (e.g., quality of command, quality of control) as well as the C2 models' overall ability to produce mission effectiveness.

The results of these experiments will be heavily influenced by the assumptions built into the model, variations in participant actions, and limitations of the experimental scenarios and operational environment implement. Given the complexities of the experiment and the cyber domain, the methodology should not be expected to predict results that would occur in a real scenario but should indicate potential advantages and disadvantages of employing different C2 constructs in the cyber domain and areas for continued experimentation.

Validity and Reliability

The complexity of the cyberspace operations and limitations in modeling real world scenarios, the validity and reliability of the conclusion from any single experiment must be treated with low confidence. Through iterations over a campaign of experimentation, and feedback from real world operations, additional data will refine the results; help to evolve experimental techniques, scenarios, and environment; and inform the formulation and refinement of research questions and hypothesis.

Summary

The DoD may be able to improve C2 of cyberspace operations by expanding C2 concepts developed for the physical domains and embark on a campaign of

experimentation to understand, evaluate, and ultimately employ new C2 models from the broader C2 trade space. In this paper, we described the factors that make cyberspace different from the other operational domains and the challenges those differences impose on existing C2 constructs. We then proposed a series Cyberspace C2 experiments to address these challenges, leveraging extensive work by the DoD Command and Control Research Program and the North Atlantic Treaty Organization. These experiments will be constructed to test and refine our hypothesis:

> Command and Control of Cyberspace Operations, supporting Multi-Domain Operations, will be most effectively implemented as a hybrid of coordinated, collaborative, and edge C2 models, within different decision spaces.

From this, we believe actionable results will inform how the U.S. Department of Defense conducts Command and Control (C2) of Cyberspace Operations.

AUTHOR BIOGRAPHIES

Adam Morgan is a Principal Cyberspace Operations Engineer in the Defense Technology Department at the MITRE Corporation in McLean Virginia. Mr. Morgan serves as MITRE's Project Leader for U.S. Army Cyber Command (ARCYBER). In this position, Mr. Morgan and his team assist ARCYBER in improving the Army's capability to conduct cyberspace operations. Prior to joining MITRE, Mr. Morgan worked at the Defense Information Systems Agency as a computer scientist. Mr. Morgan earned his Bachelor of Science degree in computer science from Virginia Tech and his Master of Science degree in computer science from George Mason University.

Dr. Steve Stone is a Senior Principal Cyberspace Operations Engineer and the Department Head for the Defense Technology Department at the MITRE Corporation in McLean Virginia. He leads a team of over 50 engineers supporting the Office of the Secretary of Defense (OSD) with analysis and practical application of advanced technologies to maintain and grow U.S. military mission superiority. The Defense Technology Department provides OSD with deep expertise in cyberspace operations, warfighter communications, radio frequency spectrum management, cloud computing, threat analysis, and countering threats from weapons of mass destruction. Dr. Stone retired from the United States Army in 2006 as a Functional Area 24 Information Systems Engineer. His last assignment was at the Joint Task Force for Global Network Operations where he developed the concept of NetOps and was the principal author of the U.S. Strategic Command's Joint Concept of Operations for Global Information Grid NetOps. He received his Bachelor of Science degree in aerospace engineering from the United States Military Academy, West Point, New York. He completed a Master of Science degree in computer science at the Naval Postgraduate School, Monterey, California and a Master of Education degree at Old Dominion University, Norfolk, Virginia. He earned his Doctor of Science in information systems and communications from Robert Morris University, Pittsburgh, Pennsylvania where he completed initial research into a model for agile command and control of cyberspace operations.

Approved for Public Release; Distribution Unlimited. Case Number 18-4338. The authors' affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions or viewpoints expressed by the authors.