Cyberspace Operations: Is a Non-traditional C2 Approach Required?

David S Alberts
IDA
dalberts@ida.org
16 March 2018

Background

Cyberspace Operations are a reality. The DOD defines cyberspace[1] as a global domain, within the information environment, consisting of the interdependent network of information technology infrastructures (infostructure) and resident data. U.S. Cyber Command (USCYBERCOM) was created in 2009 and its mission and organization have evolved since that time. Both the pre-existing Joint Task Force for Global Network Operations and the Joint Functional Component Command for Network Warfare were absorbed into USCYBERCOM. In recent testimony before Congress, Admiral Rogers, the USCYBERCOM commander stated that his mission was "to direct, synchronize, and coordinate cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners."[2] USCYBERCOM now conducts full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries. Cyberspace Operations create effects that support missions undertaken in both the physical and cyberspace domains.[3] In recognition of the importance of Cyberspace to the fight, USCYBERCOM will soon become a full and independent Unified Combatant Command.

USCYBERCOM's team member represent all of the Armed Services and are trained and equipped by Service Cyber Components (Army Cyber Command, Marine Forces Cyberspace Command, fleet Cyber Command/Tenth Fleet, and Air forces Cyber/24th Air Force as well as U.S. Coast Guard Cyber). In 2012, DOD began to build a Cyber Mission Force (CMF) to carry out DOD's cyber missions including: defend DOD networks, systems, and information; defend the homeland and national interests; and provide cyber support to military operations and contingency plans. The CMF currently consists of over 100 teams to carry out these missions, including: National Mission Teams to defend against broad cyberattacks; Cyber Protection Teams to defend priority DoD networks and systems; Combat Mission Teams to provide

[1] Congressional Research Service (CRS) Defense Primer: Cyberspace Operations December 8, 2016 cited rather than DoD sources since this is what spaces perceptions of the Public.
[2] Admiral Rogers, Commander, USCYBERCOM, testimony before SASC, February 18, 2018
[3] Cyberspace operations differ from what are referred to as Information Operations (IO) that are focused on the use of information-related capabilities e.g. deception. IO may employ cyberspace but it may involve operations in the physical domain.

integrated cyberattacks in support of a variety of missions; Cyber Support Teams to provide analytic and planning support. C2 challenges vary by team and mission.

For example, Cyber Mission Team C2 challenges include enabling synergies between cyber and kinetic force operations and effects. In 2016, reports of a 'cyber offensive' aimed at ISIS, undertaken by Joint Task Force Ares, surfaced[4]. These reports stated that the then Secretary of Defense Ash Carter wanted OCO to play a more active role in the overall campaign against the Islamic State. However, fully and effectively integrating OCO with other components of a campaign requires an integrated approach to command and control that was not in place at that time. General Thomas, head of U.S. Special Operations Command, said that Task Force Ares efforts, when combined with the efforts of Special Operations forces, other elements of CYBERCOM, intelligence agencies and international partners produced "an operation which provided devastating effects on the adversary."[5] In testimony before Congress, Admiral Rogers, the Commander, CYBERCOM, also highlighted the important contribution that "supporting fires" provided by Cyberspace Operations played in the campaign against ISIS, and noted that Cyberspace Operations are being employed in Afghanistan to "protect Coalition forces, target terrorist leaders and disrupt the operations of hostile forces."[6] The Command and Control arrangements that enabled this synergy are still in their infancy. As suitable C2 Approaches are developed and refined, a commander's ability to work OCO into the battle plan in a manner similar to orchestrating a variety of kinetic operations will continue to be enhanced.

We can expect that our ability to conduct offensive cyber and integrate OCO into battle plans will continue to improve. The U.S. 2018 National Defense Strategy recognizes the importance of Cyberspace Operations and the need to continue efforts to integrate cyber capabilities into the full spectrum of military operations. Our progress depends upon the development of a set of command and control approaches and arrangements tailored specifically for different types of Cyberspace Operations and the operations of which they are a part. Furthermore, the word 'cyber' appears over 100 times in the Joint Operating Environment 2035: The Joint Force in a Contested and disordered World.[7]

Introduction

This paper takes the first step to develop and utilize approaches to command and control that will better enable us to leverage the power of Cyberspace Operations in the context of a full range of military and civil-military endeavors. Since there is a tendency to apply traditional

[4] "U.S. Military has launched a new digital war against the Islamic State, Article in the Washington Post, July 15, 2016

[5] Dan Lamothe "Pentagon's cyber attack on ISIS may shape future of combat", article in the HeraldNet, December 16, 2017.

[6] Admiral Michael S. Rogers, Statement before the Senate Committee on Armed forces February 27, 2018

[7] Michael Lenart, "Cyber, Cyber Everywhere: Preparing for 2035", CYBER, a publication of the Military Cyber Professionals Association, Winter 2017/2018, page 42-44.

approaches rather than systematically explore the desirability of developing new approaches that may have significant advantages, the appropriateness of traditional approaches first needs to analyzed to make sure it would be appropriate in, at least, some kinds of Cyberspace Operations under some circumstances.

C2 Agility Theory tells us that there is no "one-size-fits-all" approach to C2 that is appropriate for all missions and circumstances[8]. The evidence from case studies and experiments further indicate that inappropriate approaches to C2 can lead to serious adverse consequences and even mission failure[9] [10] [11]. More importantly, C2 Agility Theory[12] [13] also provides a way to analyze and assess the efficacy of different approaches to C2 for a given mission and circumstances as well as the agility of a given approach to C2 for an Endeavor Space. C2 Agility Theory has been tested and applied to both traditional and non-traditional military missions and thus provides both a body of evidence[14] and an analytical approach that can be employed to answer questions about the appropriateness for Cyberspace Operations of the different C2 approaches that have been previously studied and utilized. C2 Agility Theory can be applied to answer the question, "Are traditional approaches to C2 appropriate for cyberspace operations?" as well as the implied question "If not, what other approaches to C2 are more appropriate?" This concept paper discusses what we may reasonably conclude from the existing body of evidence and what additional evidence and analyses are needed to "design" an appropriate C2 approach for Cyberspace Operations.

C2 Approach Appropriateness

The assessment of the appropriateness of a particular C2 Approach for a given mission and set of circumstances begins with the determining the location of the C2 Approach in the C2 Approach Space. Previous work has mapped Traditional C2 Approaches to a region located in

---

[8] C2 Agility Theory consists of a set of empirically tested propositions (hypotheses) that explore the differences between and among various approaches to command and control and their 'appropriateness for different kinds of missions. C2 Agility Theory recognizes the dynamic nature of situations and the need to transition from one C2 Approach to another as the situation changes. A number of the references are contained in the footnotes that follow.

[9] Vassiliou, Marius and David S. Alberts "C2 Failures: A Taxonomy and analysis. Proc. 18th International Command and Control Research and Technology Symposium (ICCRTS), Alexandria, VA, June 19-21 CCRP Press, Paper 049.

[10] Vassiliou, Marius, David S. Alberts, and Jonathan R. Agre (2015). "C2 Re-Envisioned: the Future of the Enterprise" New York: CRC Press. 2015

[11] David S. Alberts, et al. "C2 by Design - Putting Command and Control Agility Theory Into Practice," Institute for Defense Analyses, IDA NS D-5614, 2015.

[12] Alberts, David S. The Agility Advantage, Washington, D.C. CCRP Press,2011

[13] NATO (2013) SAS-085 C2 Agility Final Report, NATO STO-TR-SAS-085

[14] In addition to the specific books, reports and papers referenced in this paper, there are numerous references contained in the final report of NATO (2018) SAS-104 C2 Agility: Next Steps, STO-TR-SAS-104, and many papers to be found in the proceedings of the International Command and Control Research and Technology Symposium

the lower left hand corner of the C2 Approach Space (Figure 1)[15]. Looking at each of the three dimensions of the C2 Approach Space, the region associated with Traditional C2 is characterized by a centralization of decision rights, interactions that are determined by established processes and limited access to information with information flows following the chain of command.

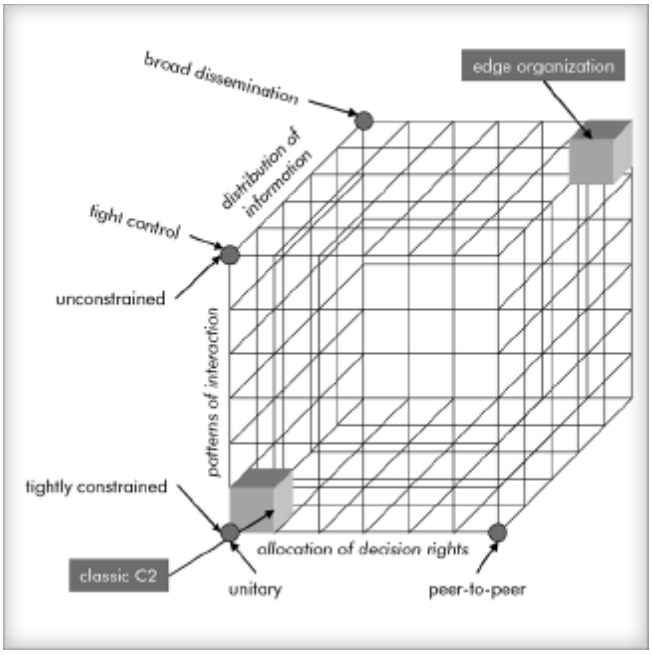

Figure 1: C2 Approach Space

Previous research has also considered a set of network-enabled approaches to C2, mapped them to the C2 Approach Space[16], (Figure 2) and tested a series of hypotheses related to the differences between and among these C2 Approaches and the nature of the missions and circumstances for which they are appropriate.

[15] Alberts, David S. and Richard E. Hayes, Understanding Command and Control, CCRP Press, 2006 p.75

[16] NATO SAS-065 Network Enabled Capability (NEC) Command and Control (C2) Maturity Model (N2C2M2), CCRP Press, 2010

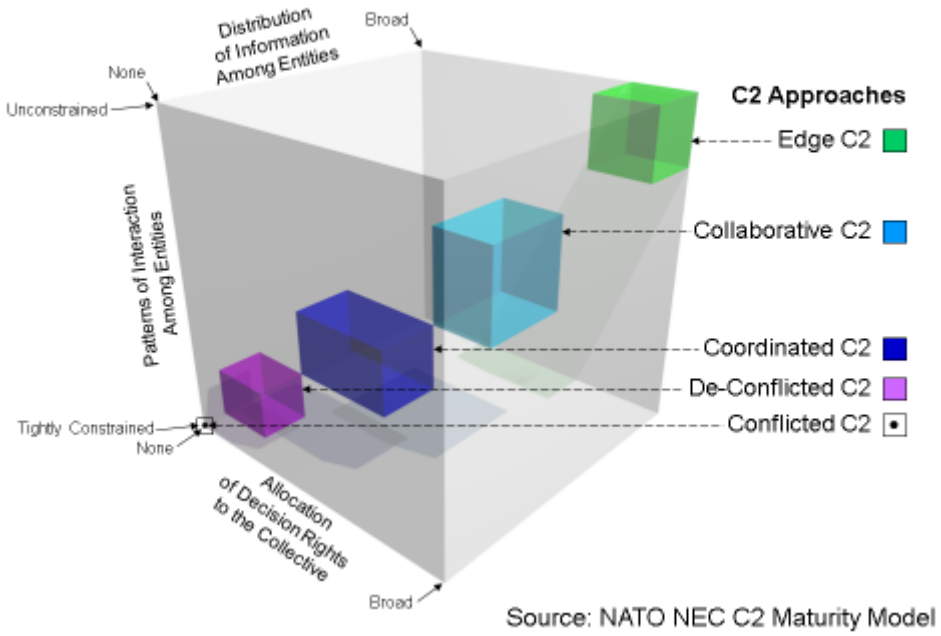

Figure 2: C2 Approaches Mapped to the C2 Approach Space

The following hypotheses[17], support by empirical evidence, provides a point of departure for a discussion of the appropriateness of Traditional C2 for Cyberspace Operations.

- No one approach to C2 is always the most appropriate (H2)
- More Network-enabled approach to C2 are more appropriate for challenging circumstances; however, less network enabled approaches are more appropriate for some circumstances (H3)
- More network enabled approaches to C2 are more agile (H4)
- More network enabled approaches are better able to maintain their intended positions in the C2 approach Space (H6)
- On-diagonal (balanced) approaches to C2 are more agile (H7)
- More mature C2 capability is more agile than the most agile C2 Approach that can be adopted (H9)
- Self-monitoring is required for C2 Maneuver Agility (H10)

Implications of C2 Agility Theory for Cyberspace Operations

H2 (no one size fits all) is predicated on the assumption there are significant C2-related differences between and among missions and the circumstances under which they are conducted. As a result of these differences, there will be a different operational design

[17] Each of these hypotheses is associated with a number, e.g. H1, used in the NATO SAS-085 C2 Agility Final Report STO-TR-SAS-085. This effort received the NATO Scientific Achievement award.

developed to fit the mission and circumstances and that to properly support the operational design an appropriate C2 Approach also needs to be designed.[18] Thus, no one approach is always the most appropriate.

If, in fact, cyberspace missions and circumstances differ in ways that have already been analyzed and found to require different C2 Approaches, then this would mean that the evidence we have indicates that there are at least some that will require non-traditional approaches to C2.

Among the circumstances that have been previously analyzed are situations that involve degradation, disruption, and loss of communications and information capabilities that impact the ability to collect and share information and collaborate[19] [20]. Other circumstances, such as a lack of trust[21] [22] in information sources and/or partners adversely affects information sharing behaviors. These circumstances could result from cyberattacks that are to be expected while operating in a highly-contested cyber environment. Previous research has found that different approaches to C2 are appropriate, depending on the extent and duration of the adverse impacts on network connectivity and/or performance[23] [24].

H6 (ability to maintain intended position in C2 Approach Space) comes into play here as well. Cyberattacks are one of the reasons that the observed C2 Approach has differed from the C2 Approach that was intended due to an inability to access information and/or the inability/unwillingness to share information. There is every reason to assume that access to and sharing of information is as critical in Cyberspace Operations as they are in other missions that have been included in previous research. Thus, more agile C2 Approaches would seem to be appropriate for operations that take place in highly contested cyber environments. Since the research also found that Traditional C2 Approaches lacked agility, this finding casts some doubt on the appropriateness of Traditional C2 for Cyberspace Operations.

H4 (more network enabled approaches are more agile) suggests that more networked enabled approaches should be considered for at least some Cyberspace Operations. Taken together, these preliminary conclusions suggest that the "C2 Toolkit" for Cyberspace Operations should

---

[18] The military practice of operational design and the need to simultaneously (and interactively) design a C2 Approach is covered in C2 by Design: A Handbook for Putting Command and Control Agility Theory Into Practice, Version 2.0 IDA Document NS D-5614 (2015)

[19] Alberts, David S., The Quest for Key Information: Does C2 Approach Matter, ICCRTS 2015

[20] Manso, Marco and Barbara Manso N2C2M2 Experimentation and Validation: Understanding its C2 approaches and Implications, 17th ICCRTS

[21] Chan, Kevin, et al. Impact of Trust on Security and Performance in Tactical Networks, 18th ICCRTS.

[22] Chan, Kevin and Mary Ruddy, Modeling trust in ELCIT-WEL to capture the impact of organizational structure on the agility of complex networks, 18th ICCRTS

[23] Alberts, David S. and Marco Manso, Operationalizing and Improving C2 Agility:
Lessons from Experimentation, 17th ICCRTS

[24] A number of the data points from the experiments undertaken by NATO SAS-085 represented situations with a loss of network links and/or nodes.

contain multiple approaches to C2. Having more than one approach to C2 available increases agility (H9).

H7 and H10 provide some criteria to use in determining the potential efficacy of a proposed C2 Approach or the design of new C2 capabilities and approaches. H7 calls for looking at the balance of the proposed C2 Approach. Balance helps to ensure that the entities have the accesses and information they need to make the decisions that are delegated to them in a timely manner. H10 requires an assessment of the ability to monitor C2-related processes and behaviors to determine if they are operating within acceptable bounds. Shortfalls in either may result in a systemic lack of C2 capability in some situations. If this is found to be the case, then that would suggest one or more high priority R&D initiatives and/or changes to doctrine, education, training, etc., in order to increase an entity's C2 Agility.

Way Ahead

These observations and conclusions, based upon C2 Agility Theory and the accumulated evidence from previous research, suggest that Traditional C2 will not be the best C2 option for all Cyberspace Operations. The implicit assumption is that C2 Agility Theory is applicable to all types of operations including Cyberspace Operations. Thus, there is no simple answer to the question, "What approach to C2 would be most appropriate for Cyberspace Operations?" Thus, there is a need for a more rigorous analysis of the appropriateness of both traditional and network-enabled approaches to C2 for Cyberspace Operations under a variety of circumstances and conditions. Exploring the set of hypotheses suggested below will serve to test both the assumption that C2 Agility Theory applies to Cyberspace Operations as well as provide an answer to the question of what approaches to C2 are appropriate. The analysis of C2 for Cyberspace Operations is complicated by both mission considerations and the nature of the enterprise required for Cyberspace Operations.

The complexity arising from the nature of the mission is a result of the variety of cyberspace missions, the need to carry out these missions in a highly contested cyber environment, and the inter-dependencies between the actions taken in cyberspace and the effects created in both cyberspace and other domains that can impact, both positively and negativity, operations in all of the domains of interest.

The complexity of the enterprise is exacerbated by the need to embed and employ non-human 'intelligence'[25] in our collectors, networks, information systems, weapons and platforms. The emergence of this socio-technical enterprise is accompanied by a first order question, "what decisions can be / should be delegated to non-human cognitive entities?" This is central to the

[25] The term "non-human" intelligence as it is used here include AI and machine learning capabilities as well as the use of decision logic and algorithms that involve choice.

development and assessment of C2 Approaches that explicitly consider mixed human-agent collaborations.[26]

The determination of which C2 Approach options are appropriate, for enterprises that employ non-human partners that can operate with some degree of autonomy, under various circumstances and conditions, will require the design and conduct of a campaign of experimentation. Such an effort would not need to start from scratch, as it can build upon a considerable body of previous C2-related research findings and utilize the Experimental Laboratory for the Investigation of Collaboration, Information sharing and Trust (ELICIT)[27] capabilities. ELICIT can support person in the loop, agent-only, and mixed human-agent experimental designs and runs. This ELICIT and the body of ELICIT research findings provide an opportunity to explore the impact on task effectiveness and efficiency of C2 Approaches that involve more or less delegation of decision rights to non-human decision makers.

Hypotheses: C2 of Cyberspace Operations

The preliminary conclusion reached above (that Traditional C2 may not be the best C2 Approach to employ in Cyberspace Operations) is based upon the implicit assumption that C2 Agility Theory applies to Cyberspace Operations. However, a determination that C2 Agility Theory is applicable does not, by itself, tell us which C2 Approach is most appropriate for which Cyberspace Operations. To obtain insights into this "appropriateness mapping" will require additional experimentation, specifically the exploration of hypotheses that seek to:

1. Explore differences between the nature of Cyberspace Operations with human v. socio-technical enterprises;
2. Determine appropriate C2 Approaches for different Cyberspace Operations; and
3. Consider Cyberspace Operations as part of multi-domain or hybrid operations.

- Nature of the Cyberspace Operations Enterprise

While some cyberspace operational tasks conceivably could employ only human decision makers, other tasks can only be successfully accomplished with non-human entities, thus these require socio-technical enterprises. The reasons for this include transactional volumes, response time requirements, and computational and/or information processing complexity. The freedom of action given to non-human entities (nature of the delegation of decision rights) can vary significantly. The first set of hypotheses that need to be formulated and tested focus on whether or not specific C2 Approaches that involve delegations of decision rights to non-human entities behave in the same way as C2 Approaches that limit their allocations of decision

[26] Fernandes, R., Hieb M. R. and Costa, P.C.G. (2016). Levels of Autonomy: Command and Control of Hybrid Forces. Paper I-060. The Proceedings of the 21th International Command and Control Research Technology Symposium, London, UK: DoD Command and Control Research Program.

[27] Ruddy, Mary, ELICIT – The Experimental Laboratory for Investigating Collaboration Information-sharing and Trust, can be found at the following link: https://www.researchgate.net/publication/253425714_ELICIT_-_The_Experimental_Laboratory_for_Investigating_Collaboration_Information-sharing_and_Trust

rights to humans. To avoid confusion with NATO SAS-085 Hypotheses, these hypotheses will be designed H101 and so on.

- H101: The locations of C2 Approaches in the C2 Approach Space are not affected by the extent to which decision rights are allocated to non-human entities.
- H102: C2 Approaches that involve the delegation of decision rights to non-human entities will be more agile.
- H103: The appropriate balance of decision rights allocation (human v non-human) will depend upon a variety of factors. These include:

    H103a: mission dynamics, work load, and time pressure
    H103b: cognitive equivalence of non-human partners
    H103c: nature of decision and existing biases
    H103d: availability of human expertise
    H103e: trust levels
    H103f: others to be identified

In order to test these hypotheses, three variants of each of the NATO C2 Approaches (e.g. conflicted, de-conflicted, coordinated, collaborative, and edge) need to be formulated. These variants include one instantiation with no decision rights allocated to non-human decision makers, one in which both humans and non-human entities have decision rights, and one where all decisions are allocated to non-human entities.

- Appropriate C2 Approaches for Cyberspace Operations

The differences between and among various Cyberspace Operations (offensive, defensive, and support) are such that they may require C2 approaches from different regions of the C2 Approach Space in order to succeed. The C2 Approach that will be appropriate for a given operation will depend upon the region in the Endeavor Space where the CSO is located and the nature of the enterprise (human v socio-technical).

- H104: Cyberspace Operations with different missions and circumstances are located in different regions of the Endeavor Space
- H105: The mapping between the Cyberspace Operations Endeavor Space and C2 Approach Space will depend upon the degree to which decision rights are delegated to non-humans.
- H106: In cases when an Endeavor involves more than one Cyberspace Operations, the C2 Approaches associated with each of these operations need to be harmonized

- C2 of Multi-Domain Operations with Cyberspace Operations

Cyberspace Operations will be undertaken as part of larger operations that involve multiple domains. At times, they will be undertaken in conjunction with kinetic operations that take place in one or more of the physical domains (Land. Air). At other times, “technical cyberspace

activities need to be well coordinated with content-based approaches like military information operations, government-wide messaging, and intelligence gathering (including all forms of security."[28] Traditional "battlefield geometry" no longer applies; "not only are physical boundaries less relevant, but the many dimensions or domains of warfare are also more closely integrated than ever before."[29]

As the set of domains that are involved in an operation become increasingly large and diverse, the more likely it is that the operation will be undertaken by a set of heterogeneous organizations, subsets of which will have their own chain of command and C2 Approach. To avoid conflicts between and among individual domain operations and the effects they create, and to develop necessary synergies, a set of command arrangements, organizational relationships, and processes between and among the participating entities is required. The set of arrangements, referred to here as C2 Harmonization, can be accomplished in different ways that correspond to regions in the C2 Approach Space. The appropriate approach to C2 harmonization will be a function of the C2 Approaches employed by the domain entities, the overall mission, and the circumstances.

- H107: In operations that involve two or more domains, a C2 harmonization approach is required to maximize effectiveness, efficiency and/or agility.

- H108: The most appropriate C2 Approach for Cyberspace Operations in the context of a Multi-Domain Operation may be different that the most appropriate approach for a stand-alone Cyberspace Operation.

The initial phase of such a research initiative would consist of two parallel efforts; one to characterize the range of Cyberspace Operations and the conditions under which they can be expected to operate (formulation of an endeavor Space) and the other to incorporate non-human decision makers into the concept of an enterprise and determine if the current approach to defining a "C2 Approach" is adequate or if it needs to be re-conceptualized.

Summary

The concept paper begins with the question "Is a non-traditional C2 Approach required for Cyberspace Operations?" It provides an answer, drawing upon what we know about the nature of Cyberspace Operations, C2 Agility theory, and the accumulated body of evidence that supports this theory. Simply put, the answer is "Yes". Having said that, the paper points out that all cyberspace operations are not the same. There are differences between Cyberspace Operations that seek to defend and thus assure the performance of cyberspace assets and capabilities and those that are offensive in nature. These operations differ in the size, scope,

[28] Linton Wells II, Cognitive-Emotional Conflict – Adversary Will and Social Resilience, PRISM 7 No. 2 page 5-17.
[29] Robert Allardice and George Topic, Battlefield Geometry in the Digital Age, PRISM 7 No. 2 page 79-97.

and strategic significance of the mission at hand as well as the circumstances in which these operations take place. Perhaps, most significantly, they range from stand-alone undertakings to being an integral part of a multi-domain operation or campaign. Because they are not the same, there is no 'one size fits all' C2 Approach that is appropriate and hence, even if there were some missions and circumstances where traditional C2 was appropriate, there are other missions and circumstances where a traditional C2 Approach is not appropriate. In fact, what we know suggests that more agile approaches to C2 are required for Cyberspace Operations. This begs the question "What specific C2 Approach is appropriate for which Cyberspace Operations?" This paper concludes that more rigorous analysis is required to answer this question and formulates a set of hypotheses that can form the basis for further exploration of C2 of Cyberspace Operations.