Leveraging the Ontology of the Operational Cyber Mission Stack (OCMS)

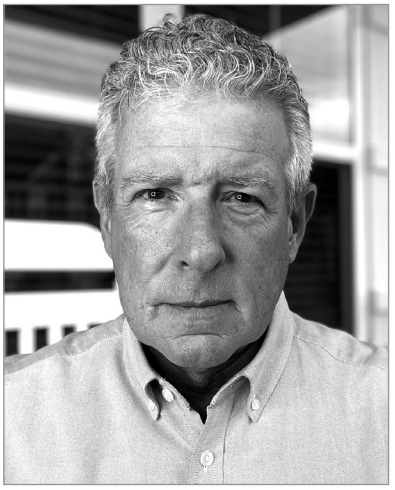
Colonel (Ret.) Jeffrey A. Voice

ABSTRACT

This article aims to identify and clarify a hierarchical construct used by defensive cyberspace planners and operators to aid in mission decomposition, assurance, and terrain mapping. The model enables the visualization of complex relationships and equities between cyberspace assets, resources, and warfighting missions.

At a time when so many Department of Defense mission-essential tasks and functions are cyber enabled, it is more critical now than ever that we strive to model the highly complex cyberspace operational environment in an understandable and useful way. Modeling is a practical means to take logical components of cyberspace, tether them to physical assets, and illuminate how they ultimately support missions. We can then prioritize mission-critical systems and capabilities, organize the defense of those cyberspace elements, and gain confidence we are defending the right things at the right time. While this model is conceptual, it represents a first step toward automating cyberspace terrain mapping that will enable defensive cyber planners and DODIN Cyberspace Forces to respond to the dynamic, man-made terrain that makes up the cyber operational environment.

> "On-tol-o-gy" (computer science) "A structure of concepts or entities within a domain, organized by relationships; a system model."
> – Houghton Mifflin 2016



COL (Ret.) Jeffrey Voice received his commission in the Army Infantry branch after completing studies at Villanova University in 1988. He has served as a Company Commander, Detachment Commander (deployed), Deputy Brigade Commander, S-3, Special Functions Officer, and Plans Team Chief in the special operations community. He also served as a Small Group Leader at the Command and General Staff College (CGSC), Ft Leavenworth, KS, and guest lecturer at the Naval Post-Graduate School (NPS) in Monterey, California where he also studied the Rule of Law and Security, Stability and Development in Complex Operations. During breaks in service, he worked in IT security and technical sales for Qwest Communications while still serving in the U.S. Army Reserve. He currently serves as a Functional Manager and Principal Defensive Cyberspace Warfare Planner for Leidos Corporation at Joint Force Headquarters – Department of Defense Information Networks (JFHQ-DODIN), J35 Future Operations division. jalanvoice@gmail.com

INTRODUCTION

In the progressively complex and dynamic cyberspace environment where, like a submarine commander, we can only perceive our operational environment through a lens of sensor data, it is difficult to connect cyber terrain and assets, to essential tasks and functions supporting warfighter missions. The Operational Cyber Mission Stack (OCMS) applies a conceptual and visual construct to Department of Defense Information Network (DODIN) cyberspace to assist defensive cyberspace planners, asset and mission owners, as well as Cyberspace Operations Forces (COF),[1(1)] identify, map, and understand the environment's operational and digital dependencies.

A significant amount of literature has been dedicated to the network mapping of physical and digital network components and logical protocols, using various models. The most common is the Open Systems Interconnection (OSI) model,[2(2,3)] which standardizes and describes the communication functions of computer systems to visualize network pathways. However, neither the OSI model nor the DoD conceived Transport Communication Protocol/Internet Protocol (TCP/IP)[(4)] model (a construct used to understand Internet protocol relationships) bridges the gap between the physical and logical elements of military cyberspace operations. The OCMS enables a commander to visualize, prioritize, and defend cyber-related elements to achieve mission accomplishment.

What is OCMS?

In Joint Publication (JP) 3-12, Cyberspace Operations, OCMS is characterized as "The ability to visualize cyber terrain, capabilities, and mission essential tasks and

1 Cyberspace Operations Forces (COF) include all maneuver forces principally tasked with Defensive Cyberspace Operations-Internal Defense Measures (DCO-IDM) and DODIN Operations (DODIN Ops), including but not limited to Cyber Protection Teams (CPTs), Cyber Security Service Providers (CSSPs), Incident/Emergency Response Teams, et al.

2 Hubert Zimmermann, "OSI Reference Model- The ISO Model of Architecture for Open System Interconnection" IEEE transaction on communications, vol.28, issue 4, April 1980. Zimmermann et al., proposed a model for architecture for Opens Systems interconnection developed by SC16. He gave some indications on initial sets of protocols that have now been developed in the OSI reference model.

3 Michael Scheidell, "Three Undocumented Layers of the OSI Model and Their Impact on Security," SECNAP Network Security Corporation.

4 Microsoft," TCP/IP protocol architecture" 2007.

objectives, facilitates cyberspace operations' primary purpose, which is to achieve objectives in or through cyberspace." The OCMS is a conceptual hierarchy and tool that enables visualization thereby revealing and clarifying relationships between the physical and logical layers of cyberspace.

Toward understanding

Joint Force Headquarters-Department of Defense Information Networks (JFHQ-DODIN) Subordinate Campaign Plan's (SCP) first Line of Effort is "Understand." This is further defined in three Supporting Lines of Effort (SLOEs), the first of which is the environment.[4] Operational planners, Area of Operations Commanders/Directors (CDRs/DIRs), and Mission-based/Functional Sector CDRs/DIRs seeking a greater understanding of their environment must employ a conceptual hierarchy to gain a better appreciation of the inherent vulnerabilities and relationships in the joint cyberspace operating environment.

Visualizing and mapping these mission elements up (or down) OCMS reveals which cyber terrain and assets are required to support a particular mission and how they relate to one another. This holistic analysis aids the identification of logical elements and physical nodes or assets necessary to support mission assurance.

A typical cyber mission stack is shown in Figure 1, supporting a notional Maritime Logistics mission. This example shows the Line of Separation (shown as a horizontal dotted line) represents the demarcation between physical cyberspace elements such as Mission Relevant Terrain-Cyber (MRT-C), nodes or assets (below the line), and logical operational elements such as capabilities, mission essential tasks/functions (METs/MEFs), and objectives listed above the line.[(5)]

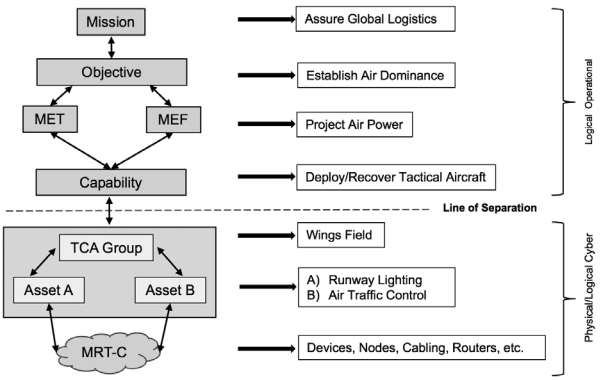


Figure 1. Typical Cyber Mission Supporting a Notional Maritime Logistics Mission.

It is important to recognize that Defensive Cyberspace Operations-Internal Defensive Measures (DCO-IDM)[5] and DODIN Ops planners focus on friendly (Blue) cyberspace to enumerate

5 It is important to note that in accordance with JP-5 Joint Planning, "Tasks direct friendly actions to create desired effect(s). These are the discrete activities directed in the campaign plan used to influence the OE. The execution of a task will result in an effect." For simplicity in illustrating the model, "effects" are omitted herein.

Assets deemed critical to a Commander's mission are referred to as Task Critical Assets or "TCAs." Where they are critical to strategic missions, they are referred to as Defense Critical Assets or "DCAs."

assets and capabilities which enable or create effects in cyberspace (and occasionally physical domains) to protect and defend them. Conversely, offensive cyberspace planners look beyond the DODIN boundary into neutral (Grey) or adversary (Red) cyberspace terrain to develop Cyberspace Effects Operations (CEO) based on a commander's objectives.

What is significant about these divergent organizational approaches is that in planning and executing defensive actions in friendly cyberspace, COF need to look inward to accurately *identify and prioritize* which cyberspace elements are most essential and most vulnerable according to mission imperatives and phases of operation[6] rather than merely executing threat agnostic contiguous defense measures.

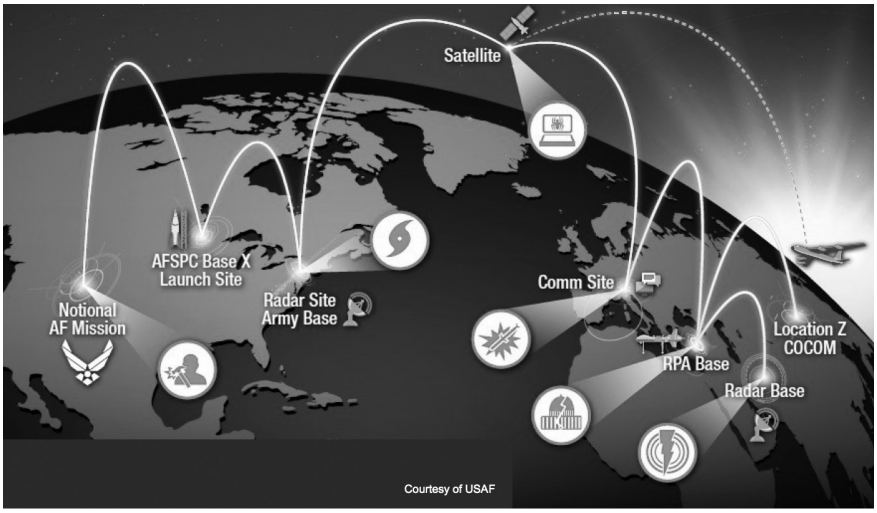


Figure 2. Example of Geographic Distribution of Assets.

What does it do?

The stack enables visualization, prioritization and integration of equities, dependencies, and assets with operational capabilities, tasks, and objectives through a logical mission thread.[7] For instance, elements necessary to carry out a notional Air Force mission like the one depicted in Figure 2[8] may be diverse and distributed geographically around the globe. Their nature and distribution may obfuscate the equities and dependencies the OCMS model endeavors to clarify.

The cyber portion of the mission thread associates two of the three layers of cyberspace (the logical network layer and the physical network layer,[6] with operational warfighting imperatives or elements. It does so by modeling the operational cyber environment to allow the viewer to identify and connect cyberspace entities (physical and logical) supporting a mission. It further

6 Phases of military operations typically begin with OPLAN approval. Operations ideally begin and end with Phase 0/Shape. Execution of the EXORD or OPORD activation begins the remaining phases. These phases consist of the following: Phase 1/Deter, Phase 2/Seize Initiative, Phase 3/Dominate, Phase 4/Stabilize, and Phase 5/Enable Civil Authority.

7 A "mission thread" is an operational and technical description of the end-to-end set of activities and systems that accomplish the execution of a joint mission.

8 Courtesy of United States Air Force, Mission Thread Analysis Overview, A.F. Energy Assurance, safie.hq.af.mil/Installation Energy.

informs the interoperability and dependency of diverse critical assets and cyber terrain supporting one or more critical capabilities.

Why do we need a model?

The ability to deconstruct and understand the interrelation of dependencies increases in complexity and importance as we widen the lens through which we visualize mission composition. The widening of that lens reveals a complex lattice of supporting and supported relationships.

Dependencies and equities become more intricate as cyberspace elements support multiple assets, capabilities, METs/MEFs, missions, etc. For example, the unshaded area in Figure 3(i) shows two task-critical assets (TCAs) supported by common MRT-C. In Figure 3(ii), we

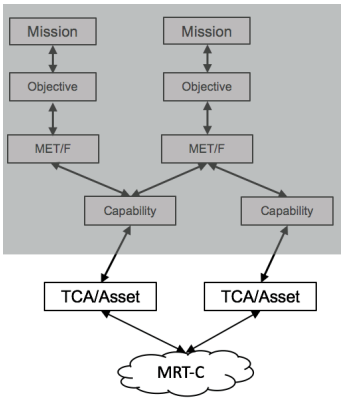


Figure 3 (i). MRTC Supporting Two Task Critical Assets/Assets.

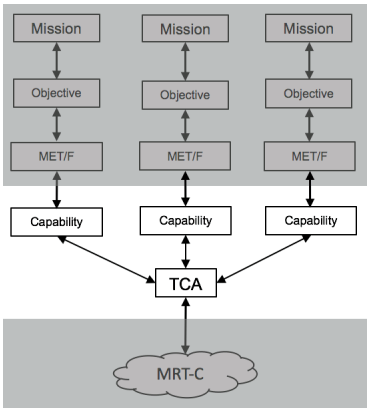


Figure 3 (ii). TCA/Asset Supporting Multiple Capabilities.

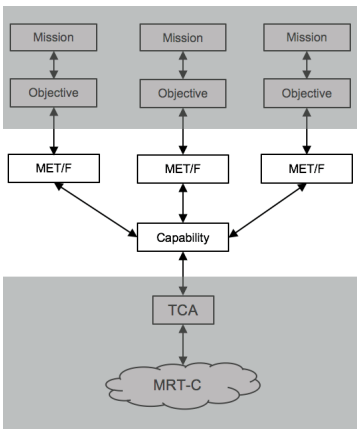


Figure 3 (iii). Capability Supporting Multiple Mets/Mefs.

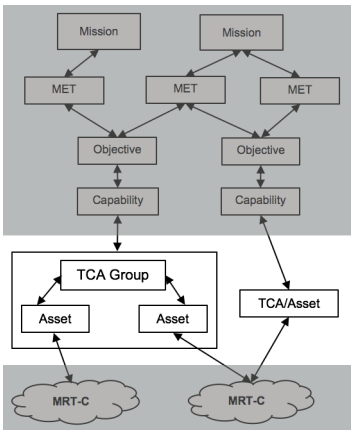
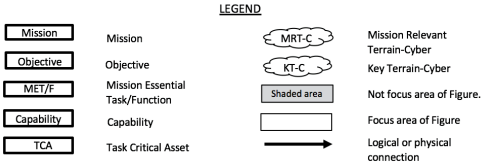


Figure 3 (iv). Multiple Assets Supporting Diverse Capabilities.



see a single TCA supporting multiple capabilities. Figure 3(iii) shows a single capability supporting multiple mission essential tasks or functions (MET/MEF). Finally, in Figure 3(iv), we can see multiple assets supporting diverse capabilities.

Where a series of critical assets are required to enable a capability, they are referred to as a TCA or Asset Group.[7] TCA Groups can be particularly problematic for mission decomposition since it is the aggregate of the assets that enable a capability. A failure of any of the supporting assets can disable the capability. An example might be a Terminal High Altitude Area Defense (THAAD) system, which requires an interceptor, launch vehicle, radar, and fire control system. Each of those elements may be identified as an asset supporting a TCA.

Figure 4 further widens the lens and shows a Mission Owner (also referred to as a Sector Commander [CDR] or Director [DIR])[9] supporting multiple Lines of Effort (LOEs) that may include multiple missions. Using OCMS, we can see that the relationship between objectives, tasks, capabilities, and assets increases exponentially. Increasing these elements means increasing the complexity of the supporting and supported relationships to be considered as well.

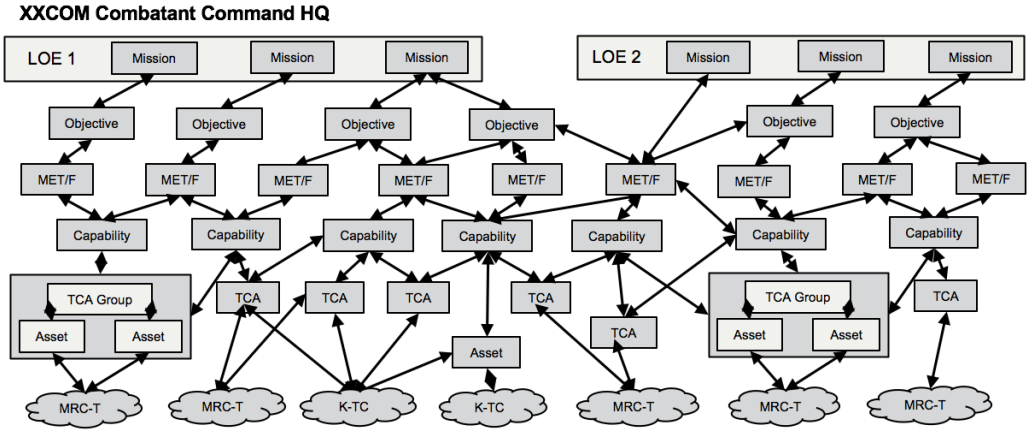


Figure 4. EOCMS Supporting Multiple Loes/Loos.

As the perception aperture continues to widen and becomes more inclusive during mission decomposition, we can see in Figure 5 that a contingency or campaign plan may involve multiple components (DODIN Sector CDRs/DIRs), each supporting multiple LOEs. Their missions are in turn supported by multiple assets provided by DODIN Area of Operation (DAO) CDRs/DIRs (asset owners or resource providers).

It is important to understand that while Mission Owners (such as Combatant Commanders [CCDRs]) are responsible for mission assurance and accomplishment, they are at the same time dependent on multiple assets provided by DAO CDRs/DIRs to accomplish those missions. They are also concurrently acting as DAO CDRs/DIRs providing capabilities to support their own missions and those of others.

9 The DODIN Area of Operation (AO) and Sector construct is discussed briefly later in this article.

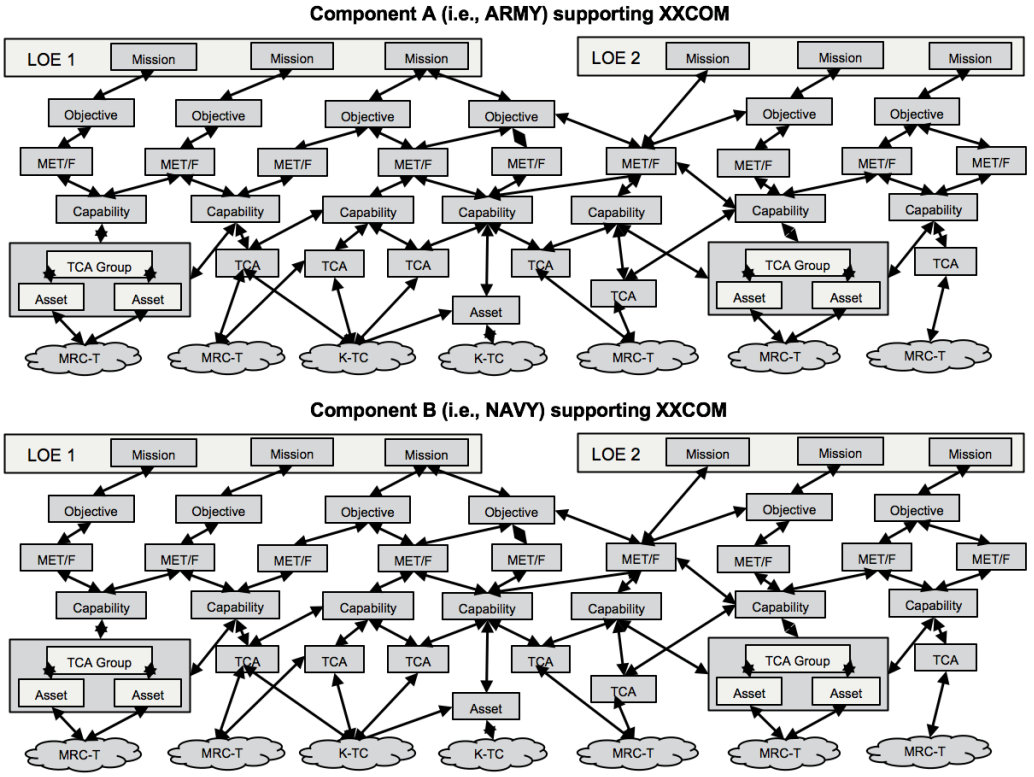


Figure 5. OCMS Supporting Multiple Components Each Supporting Multiple Loes/Loos.

If we accept that DoD Components, such as military service components or other CCMDs, may be acting as a Sector CDR/DIR (Mission Owner) while also acting as a DODIN AO CDR (a resource or asset provider facilitating a variety of capabilities by way of their own assets), then we must also accept that the task of identifying, tracking, and managing those equities and relationships becomes massive and daunting. As a result, because cyber equities and relationships are so entwined and complex, a method or construct like the OCMS is helpful if not imperative.

In support of the concept of Battlespace Awareness, U.S. Cyber Command (USCYBERCOM) Operational Guidance 3-2, "Defensive Cyberspace Operations," cites the six joint functions which underpin the execution of operations in all warfighting domains. The Command-and-Control section discusses the importance of this awareness and states that "visualization must encompass all layers of cyberspace, providing functional mapping of cyberspace objects to the objectives they support; as well as the disposition and status of friendly and adversary forces within the terrain."[8]

OCMS supports the concept of battlespace awareness as it promotes functional and operational identification and mapping of cyberspace objects, such as MRT-C and assets, to the

objectives and missions they ultimately support. The increased awareness of the defensive cyber battlespace also facilitates a commander's and COF's ability to prioritize assets and terrain in support of mission assurance by revealing relevant, key or decisive terrain.

KEY TERRAIN-CYBER (KT-C)

KT-C—cyber terrain that affords a marked advantage to the combatant who holds or controls it—can be identified using the OCMS model to unpack, analyze, and understand operational requirements, mission objectives, and vulnerabilities (i.e., single points of failure). It is important to note that KT-C, much like key terrain in other warfighting domains, can change as operations or campaigns mature.

For example, because we are essentially a commuter military, cyber terrain that enables Global Logistics may be more critical and nuanced during Phase I: Deter as forces are being built up than during Phase III: Dominate when demands may decrease as commanders might seek solely to sustain forces. As DoD COF strive to maneuver and defend KT-C, it is wise to be mindful that "unlike maneuver[ing] in the physical world, it will sometimes take place at machine and network speeds on terrain that constantly shifts."[9]

THE OPERATIONAL ENVIRONMENT (OE)

It is essential to recognize that cognizance of the fidelity of situational awareness is proportionate to the speed at which the cyberspace operational environment evolves: "Understanding the relationship of terrain to mission is critical in the development of Defensive Preparation of the Operational Environment" (DPOE).[10] This is principally because, unlike other domains that are bound by more significant corporeal restrictions, like the first law of motion that can dictate how fast a missile may fly or how far a tank may fire, cyberspace's fundamental and foundational physical restriction within the domain is the speed of light. The effects of executed capabilities can, in some cases, be delivered in nanoseconds. Further, those effects can be delivered at that speed globally.

Because cyber effects may be delivered instantly anywhere on the globe (or in Earth's atmosphere), defending the DODIN is a global responsibility. This responsibility was formally tasked to JFHQ-DODIN by USSTRATCOM as recently as 2016. Specifically, the Commander of JFHQ-DODIN was ordered to "plan, execute, direct, coordinate, and assess the execution of global DODIN operations and DCO-IDM in coordination with affected combatant commands (CCMDs) and DoD Components."[11] This codified and operationalized the global responsibility for the defense of friendly cyberspace (DODIN) and all it encompasses.

This global responsibility is reinforced and confirmed by the now Unified Functional Combatant Command, USCYBERCOM, in its 2019 Campaign Order. The order states: "USCYBERCOM and its components (JFHQ-DODIN among them) will operate in a global domain within the information environment consisting of the interdependent networks of information

technology (IT)...USCYBERCOM designates JFHQ-DODIN as the main effort for the protection of the DODIN."[12]

Therefore, because cyberspace is unlike other warfighting domains and JFHQ-DODIN maintains global reach and responsibility for defense of the DODIN, it is important to recognize "the nature of cyberspace dictates that the area of operations, influence, or interest are not constrained by geographic or political boundaries, and this may lead to rapid expansion or contraction of these areas."[13] This defines cyberspace as truly dynamic.

AO/SECTOR CONSTRUCT

The OCMS hierarchy supports Intermediate Military Objective One (IMO 1) articulated in JFHQ-DODIN's "Operation Gladiator Shield 2017"[14] which directed Combatant Commanders, Service Components, Agencies, and Field Activities to organize the cyber battlespace according to the DODIN AO and DODIN Sector construct.[15] This objective represented a major step toward structuring a manageable and defendable DODIN battlespace.

While AO is used in the construct to mean "Area of Operations," it can also almost interchangeably represent "Asset Owners" since it is the DODIN AO CDRs/DIRs that usually purchase, operate, maintain, and protect critical assets. An excerpt from USCYBERCOM FRAGORD 1 to OPORD 17-0114 states, "an Area of Operation (AO) when established within the DODIN, is defined by the commander's or director's authority to direct DCO-IDM and DODIN Ops."[16] Since we know that DODIN AO CDRs and DIRs are asset owners, this illustrates an orientation toward the assets and terrain which reside below the line of separation (Figure 1) on the OCMS. As previously alluded to, this is an inward orientation to cyberspace operations.

A subsequent passage from the same order states, "Sectors are established to reference DoD core functions and the corresponding commands, agencies, and field activities that are supported and/or impacted by a cyberspace incident or event."[17] This illustrates a focus on functions, tasks, and capabilities that enable a mission above the Line of Separation on the OCMS. The DODIN AO/Sector construct, and its orientation to assets or functions, becomes evident when using OCMS and thereby enables the decomposition of a mission and identification of which assets are supporting which capabilities.

The Need for Automation

Because the relationships among elements are so complex, the dependence of METs and MEFs on cyber is so great, and because the terrain is subject to morphing at the speed of fiber optics, there is a clear need for an automated platform or technology to aggregate and make network visualization available across all Sectors and DAOs. The Mission Assurance Decision Support System (MADSS) has been designated by the Chairman of the Joint Chiefs of Staff as the program of record for mapping DODIN cyber terrain and assets that support operational warfighting requirements. The implementation of that mission assurance platform was further ordered by CDRUSCYBERCOM in January of 2017.[18]

However, the current input of data into MADSS is a painstakingly manual process. Because cyber terrain can change so rapidly in ways that may have unexpected consequences, it is important that a fully automated strategy be implemented as soon as possible. Regardless of which platform is used, it is important to remember that because cyberspace is a man-made warfighting domain which "adds global reach, often at nearly instantaneous speeds,"[19] and because its terrain evolves and changes constantly, some form of advanced automation if not artificial intelligence will ultimately be necessary to deliver a real-time accurate visualization of the cyberspace operational environment. This automation will add immeasurably to a commander's ability to establish and maintain a cyberspace common operating picture (COP).

CONCLUSION

Because of the complexity of the cyberspace warfighting domain, it is necessary to have a mechanism or model (like OCMS) to unpack and visualize the myriad physical and logical connections and dependencies between all cyberspace elements represented in OCMS, to identify and protect operational elements supporting warfighters conducting kinetic or cyberspace operations. As stated earlier, understanding the relationship of objects in the hierarchy of the Operational Cyber Mission Stack is essential in decomposing and assuring a mission.

The model advanced in this article helps cyber planners, defenders, and mission commanders visualize and define the friendly cyberspace environment. This visualization allows the user to better track and prioritize physical and logical elements of cyberspace, going from micro to macro views of the OE as it evolves and changes on a global scale.

NOTES

1. Joint Force Headquarters – Department of Defense Information Networks (U) "OPORD 19.0005 Fight the DODIN," *Operation Order Gladiator Shield 2019*, Ft Meade: Department of Defense, February 8, 2019.
2. Hubert Zimmerman, "OSI Reference Model- The OSI Model of Architecture for Open Systems Interconnection," *IEEE Transactions on Communication*, IEEE, April, 1980.
3. Chairman of the Joint Chiefs of Staff, "(U) JP 3-12," *Cyberspace Operations*, Washington, D.C.: U.S. Department of Defense, June 8, 2018.
4. United States Cyber Command, "(U//FOUO) DODIN Operations and DCO-IDM." *Subordinate Campaign Plan*, Ft Meade, MD: United States Cyber Command, December 11, 2017.
5. United States Cyber Command, "(U) Doctrine for Cyberspace Operations." *Publication 1.* Ft Meade, MD: USCYBERCOM, June 15, 2016.
6. Chairman of the Joint Chiefs of Staff, "(U) JP 3-12." *Cyberspace Operations,* Washington, D.C.: U.S. Department of Defense, June 8, 2018.
7. Joint Force Headquarters – Department of Defense Information Networks, "(U) Asset Defense Plan/ Resource Document," Ft Meade, MD: Dept of Defense, June 2019.
8. United States Cyber Command, (U) "Operational Guidance," *Defensive Cyber Operations*, Ft Meade, Maryland: United States Strategic Command/United States Cyber Command, March 2017.
9. Gregory Conti and David Raymond, *On Cyber: Towards an Operational Art for Cyber Conflict*, Kopidion Press, 2017, 88.
10. United States Cyber Command, (U) "Operational Guidance," *Defensive Cyber Operations.*
11. United States Strategic Command, "USSTRATCOM EXORD." (U) *EXORD 16-04,* Department of Defense, February 10, 2016.
12. United States Cyber Command, (U) "*Campaign Operation Order 8500-19 Base Order,*" Ft. Meade, MD: Department of Defense, 2019.
13. United States Cyber Command, (U) "*Operational Guidance, Defensive Cyber Operations 3.2.*"
14. Joint Force Headquarters – Department of Defense Information Networks "(U//FOUO) OPORD 17-0318," *Operation Gladiator Shield Implementation*, Ft Meade, MD: Department of Defense, December 20, 2017.
15. Joint Force Headquarters – Department of Defense Information Networks "(U//FOUO) OPORD 17-0318."
16. USCYBERCOM, "(U) FRAGO 01 to *OPORD 17-0114," Designation of Named Areas of Operation*, Ft Meade, MD: Department of Defense, July 2018.
17. USCYBERCOM, "(U) FRAGO 01 to *OPORD 17-0114," Designation of Named Areas of Operation*, Ft Meade, MD: Department of Defense, July 2018.
18. (U) USCYBERCOM "(U) TASKORD 17-0008" *Mission Assurance Decision Supprot System (MADSS) Capabilities*, Ft Meade, MD: Department of Defense, January 10, 2017.
19. Conti and Raymond, *On Cyber: Towards an Operational Art for Cyber Conflict*.