Carnegie Mellon University
Software Engineering Institute

TERRAIN IN CYBERSPACE OPERATIONS—TERMINOLOGY

Vincent LaPiana and Nathaniel Richmond

September 2024

DOI: 10.1184/R1/27306129

[Distribution Statement A] Approved for public release and unlimited distribution.

Executive Summary

This paper discusses the relationships between several terms used to describe characteristics of cyber operations (CO) and how they relate to other terms important to military operations and mission planning. We focus on defensive cyber operations (DCO). We discuss key terrain-cyber (KT-C) and mission-relevant terrain-cyber (MRT-C) and review current definitions for each term and their respective synonyms: cyber key terrain (CKT) and mission-relevant cyber terrain (MRCT). We describe how these terms relate to the joint doctrine multi-domain concept of key terrain. These terms identify and describe characteristics of CO that we use in our work for our government mission partners.

Department of Defense (DoD) documentation describing cyberspace-related concepts uses a variety of terminology defined in joint doctrine, but also other sometimes ambiguous terms in documents, presentations, and references, often implying a similar meaning to official terminology, yet without clear definitions. Clear definitions avoid confusion and misunderstanding based on metaphor, simile, or implied meaning that may be interpreted differently by readers with different perspectives on CO or mission planners working at different tactical, operational, and strategic levels who need to include the intended and unintended effects of CO in their mission analysis and planning.

BLUF: We use the following working definitions of these terms based on DoD doctrine and current usage in the DoD:

- MRT-C is the entire set of cyber assets, processes, services, functions, infrastructure, and personas needed to conduct or support a mission in any domain; ensure that capabilities exist to support mission-essential tasks (METs) and mission-essential functions (MEFs); and maintain mission assurance of task-critical assets (TCAs).
- KT-C is key terrain in the cyberspace domain. It includes the subset of MRT-C plus elements of adversary cyberspace that comprise specific assets, systems, services, infrastructure, and personas identified as key terrain, the use or control of which may provide friendly, or adversary forces a marked advantage for a given mission.

It is important for commanders and the technical experts on their staff to have a shared understanding of key terms in order to integrate CO into multidimensional mission analysis and mission planning.

Important Cyberspace Operations Terms

JFHQ-DODIN uses the terms cyber key terrain (CKT), key terrain – cyber (KT-C), key terrain in cyberspace, mission-relevant terrain – cyber (MRT-C), and mission-relevant cyber terrain (MRCT) during the analysis and planning of cyberspace operations (CO) and operations in other domains that involve CO support. The general meanings of these terms have broad overlap, but the differences and contexts are important to note.

Key Terrain

According to *Joint Intelligence Preparation of the Operational Environment (JIPOE)*, key terrain describes a concept which, although broad, is specific and can be meaningfully applied at tactical, operational, and strategic levels in military planning and analysis [Joint Chiefs of Staff 2009]. From the perspective of a specific military mission, key terrain may exist in any or all five domains: land, maritime, air, space, and cyber. The JIPOE defines key terrain as

> *Any locality, or area, the seizure or retention of which affords a marked advantage to either force. Therefore, it is often selected as a decisive point and a tactical-level or operational-level objective. Certain key terrain, such as an airport or seaport, could be designated as an operational-level objective if it significantly affects the Joint Forces Commander's (JFC's) ability to deploy or employ joint force components. For example, an operational commander may consider as key terrain an urban complex that is an important transportation center, a road network providing passage through restrictive terrain, or a geographic area that provides critical agricultural, industrial, or natural resources. [Joint Chiefs of Staff 2009]*

In addition, the JIPOE details several characteristics of key terrain [Joint Chiefs of Staff 2009]:

1. *Key terrain varies with the level of command. For example, a large city may represent an important objective to an operational-level commander, whereas a tactical commander may consider it to be an obstacle.*
2. *Terrain which permits or denies maneuver, such as bridges or chokepoints, may be key terrain.*
3. *Major obstacles rarely constitute key terrain. Thus, the high ground dominating a river, rather than the river itself, is considered key terrain.*
4. *Key terrain may include areas and facilities that may have an extraordinary impact on mission accomplishment (e.g., ballistic missile launch facilities, cruise missile launch sites, airfields).*

These four concepts and characteristics of key terrain may have analogs in cyberspace, especially concepts 1, 2, and 4. Of note is the difference in the importance of information, information management, and public perceptions of military actions at the tactical, operational, and strategic levels. There will also be circumstances in which military actions at the tactical level are sound but at the strategic level are not due to the impact on political or strategic freedom of action that may result from battle

[Distribution Statement A] Approved for public release and unlimited distribution.

damage, effects on civilian populations, or, in the specific case of cyber operations, the revealing of cyber capabilities, tools, and techniques to the public and adversaries and reuse of cyber weapons by an adversary.

Key Terrain in Cyberspace

JP 3-12 *Cyberspace Operations* describes key terrain in cyberspace as follows:

> ***Key terrain in cyberspace*** *is analogous to key terrain in the physical domains in that holding it affords any combatant a position of marked advantage. In cyberspace, it may only be necessary to maintain a secure presence on a particular location or in a particular [computing] process as opposed to seizing and retaining it to the exclusion of all others. Note that it is possible for friendly and adversary forces to occupy the same terrain or use the same process in cyberspace, potentially without knowing of the other's presence. An additional characteristic of terrain in cyberspace is that these localities have a virtual component, identified in the logical network layer or even the cyber-persona layer. [Joint Chiefs of Staff 2018]*

The terms *key terrain – cyber* (KT-C) and *cyber key terrain* (CKT) are synonyms of *key terrain in cyberspace*, based on our observations of how they are used in the DoD and in service-specific documents related to CO, and key terrain–cyber (KT-C) is the doctrinally preferred term at this time.

The definition of KT-C is conceptual, explaining what it is and how it is fundamentally the same as key terrain in any domain, but it does not define what things (constructs, assets, capabilities, or personas) are key terrain, since key terrain is always mission specific.[1]

Mission-Relevant Terrain – Cyber (MRT-C)

Mission-relevant terrain – cyber (MRT-C) and mission-relevant cyber terrain have both been used to define the same concept used in mission planning and mission assurance. Although both terms are still used in DoD documents, MRT-C is the doctrinally preferred term today and should be used.

MRT-C is information that identifies and documents the hardware, software, and infrastructure (e.g., cabling, power, space, and cooling) required to accomplish a mission. MRT-C should include the physical and logical components of cyberspace terrain that support a specific mission. It may be part

---

[1] KT-C includes "…understanding of the cyberspace domain to include human interaction that spans the entire spectrum from competition to conflict and recognition that DoD is in continuous engagement with adversaries …" [USCYBERCOM 2018, pp. 3–4].

[Distribution Statement A] Approved for public release and unlimited distribution.

of and connected to a task-critical asset (TCA)[2] or a defense-critical asset (DCA).[3] Examples of MRT-C are information systems, assets, devices, internal/external links, operating systems, services, applications, ports, protocols, software on servers, user and service accounts, and other functions of a system required by a TCA [DoD 2022].

MRT-C is not limited to terrain that supports the cyber mission. It includes assets and capabilities that support Combatant Command / Service / Agency / Field Activity (CC/S/A/FA) missions, whether they occur in cyberspace or in another domain supported by cyber assets.

Whereas Key Terrain – Cyber refers to physical and logical components of cyberspace in blue, gray, or red space, terrain the use of which is key to accomplishing a mission regardless of whose space it resides in, MRT-C is cyberspace assets, services, and capabilities available to and under the control of the Joint Forces Commander or under other friendly control.

MRT-C identifies assets, processes, capabilities, and functions in blue and gray cyberspace that need to be defended and whose defense should be prioritized based on TCAs, MEFs, and METs, all of which will be specific to a particular mission. MRT-C focuses on the physical and network layers of cyberspace and their relevance to mission planning. As the DODIN increases its use of hybrid, non-DoD services such commercial cloud providers, MRT-C will include more non-DoD commercial assets, services, data, data stores, and functions.[4]

The transition from the term MRCT to MRT-C in joint doctrine reflects an effort by the DoD to define and use terminology that has specific, doctrinally defined meanings and conforms to well-defined DoD terms like terrain. While the meanings of MRCT and MRT-C are essentially identical, MRT-C is the correct term according to current doctrine. Nevertheless, we have seen examples of both terms used in mission-planning documents to identify cyber assets and services needed to conduct cyber operations or to support operations in other domains.

Our perspective centers on defensive cyber operations (DCO) and DODIN operations, as do the sources we are using to understand working definitions of cyber operations terms. This perspective focuses on the physical and network layers of the Cyberspace Layer Model,[5] as do the above descriptions of MRT-C, because the physical and network layers of cyberspace are the primary focus of DCO

---

[2] A TCA is defined as an asset that, if lost, causes a mission-essential task (MET) to fail. [See also DoD 2022, p. 72, and DoD 2018, p. 19.]

[3] DCA – A subset of TCAs, identified as critical to strategic missions. Nominated by Joint Staff J34 and approved by ASD(HD&ASA). [See DoD 2018, p. 18.]

[4] The increased use of and dependence on gray or blue non-DoD cyberspace will produce several effects. It will necessitate commercial contract relationships with non-DOD service providers that give the DoD required access to and protection of mission-critical assets and services in those non-DoD environments, and it will eliminate or diminish the DoD's ability to direct action by subordinates through official regulations and orders since such control authorities will instead flow through contracts.

[5] Cyberspace Layer Model (aka Cyberspace Operational Domain): cyber-persona layer (digital representations of actors or entity identities), logical network layer (network elements related to one another and abstracted from physical location), and physical network (IT devices and infrastructure) [Joint Chiefs of Staff 2018, p. 1-2].

[Distribution Statement A] Approved for public release and unlimited distribution.

and DODIN operations. However, we recommend expanding the definition of MRT-C to include the persona layer of cyberspace which, depending on the nature of a given mission, may be designated as key terrain by the mission commander. The definition of MRT-C does include accounts that can equate to cyber personas, but we think that explicitly including virtual entities and the persona layer of cyberspace in the definition underscores how significantly CO can influence human attitudes and behavior and affect military operations. Such an approach would recognize the potential strategic impact and consequences, intended and unintended, of CO as well as the relevance of CO on Operations in the Information Environment as addressed in recent DoD doctrine in publications such as Joint Publication 3-04 "Information in Joint Operations,[6]" Marine Corps Doctrinal Publication – 8 "Information" (MCDP-8),[7] and Army Doctrine Publication 3-13 "Information."[8]

The purpose of gathering and reporting MRT-C for a specific mission is to identify cyber assets, services, functions, and related physical infrastructure. In contrast, KT-C may include logical abstractions such as cyber personas or the cyber terrain control of which is needed to obtain desired effects within the information environment, such as access to trusted media sources used by the target audience. This may explain why we have seen MRT-C and not KT-C used in mission-planning documentation, since mission analysis and planning link tasks, functions, and capabilities back to assets. It is also possible that key terrain is identified in later mission-planning stages, distinct from those related to MRT-C.

Finally, MRT-C focuses on tasks, functions, capabilities, and ultimately assets that are available to the commander and must be defended. MRT-C is therefore limited to blue and gray space and will be the space in which defensive cyber operations take place. In contrast, KT-C may include blue, gray, red, and white space, and could include DCO, DCO-RA, and OCO.

Diagrams Showing the Relationship of MRT-C to KT-C

We include two diagrams to visualize the relationship between MRT-C and KT-C in two mission threads. The first represents a mission in which CO support a kinetic mission involving the space, air, and land domains. The second mission thread represents CO that may include Defensive Cyber Operations – Response Actions (DCO-RA).

Mission Thread 1: "Respond to warning of missile attack: Intelligence reports a high probability that Red space assets may attack a Blue space base in the area of operations (AO) with missiles within the next 60 days."

Mission-critical assets and capabilities:

- physical/kinetic and electronic weapons systems to deter the adversary and defend the AO

---

6 JP 3-04 is unclassified but has not been publicly released.

7 https://www.hqmc.marines.mil/agencies/deputy-commandant-for-information/mcdp-8-information/

8 https://armypubs.army.mil/ProductMaps/PubForm/ADP.aspx (select ADP 3-13)

[Distribution Statement A] Approved for public release and unlimited distribution.

- early warning sensors (land, airborne, and space based)
- anti-missile (AM) defensive systems
- command-and-control (C2) systems integrating electronic warfare and AM systems
- cover and other means of protecting people and critical assets

Cyber services, applications, data, and processes needed for this mission: Some of these are MRT-C if they support TCAs, DCAs, or mission-critical and mission-essential assets.

- communications infrastructure (email, VTC/VOIP, Microsoft Teams, radio)
- applications, data, processes, and services that update information in accordance with the commander's decision-making (Observe–Orient–Decide–Act loop) cycles and synchronize responses between JFC and higher headquarters: sensor data; threat intelligence; visualization tools; situational awareness of self, allies, and threat
- knowledge of mission-critical assets' vulnerabilities, mitigations, and methods of remediation

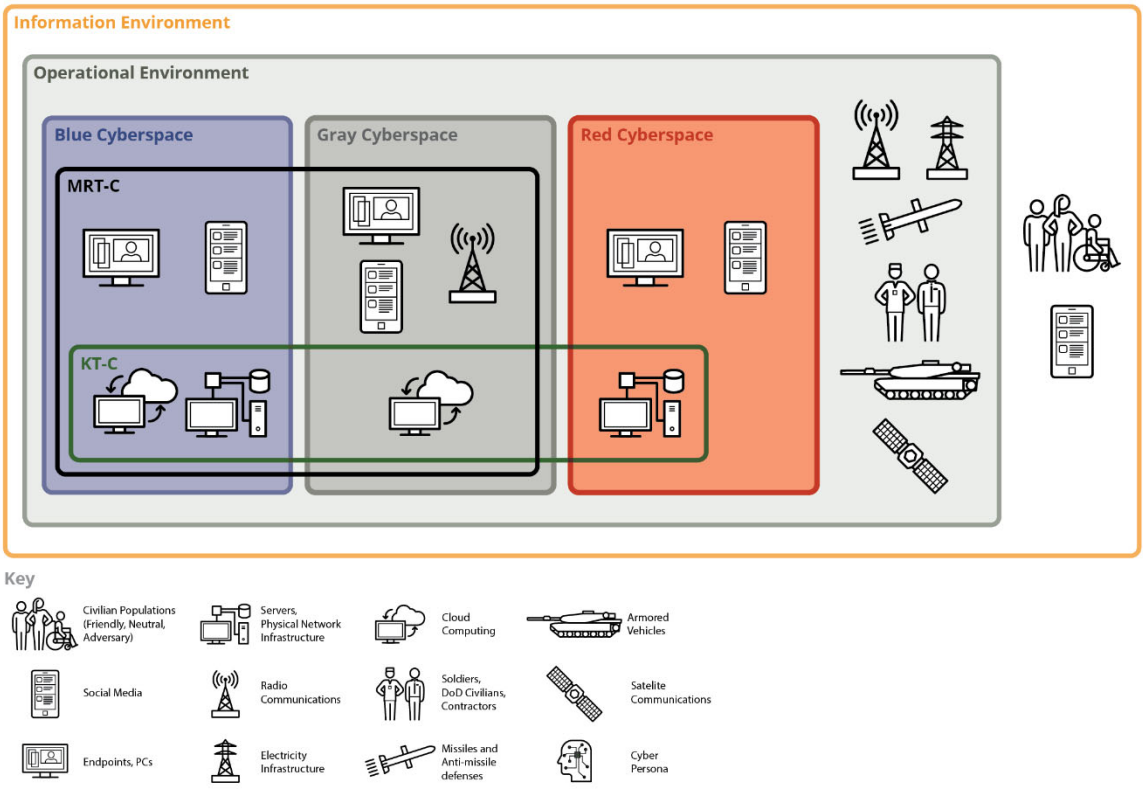

Figure 1: Mission Thread 1

Terrain (overall operational environment) includes key terrain and blue, gray, and red cyberspace.

CO may create effects, by design or not, in the Information Environment (white space), physical, network, persona, and cognitive domains.

[Distribution Statement A] Approved for public release and unlimited distribution.

MRT-C is identified during mission analysis, Courses of Action (COA) development, and MET and MEF development with their underlying capabilities mapped back to assets. In this mission, they include

- blue cyberspace physical network infrastructure and services such as electricity generation needed by mission-critical assets, social media, endpoints, and cloud computing
- gray cyberspace social media, endpoints, radio infrastructure, and cloud computing services and data

Key terrain:

1. Satellite communications (blue and gray space)
2. Airspace above and between adversary missile launch facilities and targets to monitor and effectively employ missile defenses
3. Anti-Missile (AM) defenses
   - Electric power the AM systems and AM C2 depend on are MRT-C
4. Soldiers, DoD civilians, and contractors with specialized skills required to operate AM defenses
5. Red (adversary) missiles and C2
6. Key terrain – cyber:
   - blue cyberspace: servers and physical network infrastructure and cloud computing services and data. These assets provide capabilities used in key terrain in Items 1, 2, and 3 above. Protecting these capabilities is a priority for this mission.
   - gray cyberspace: cloud computing services and data. These assets provide capabilities used in key terrain in Item 1. Protecting access to these services and data is a priority for this mission.
   - red cyberspace: servers and physical network infrastructure. These assets provide adversary capabilities for Key Terrain Item 5. Degrading these adversary capabilities and function may be a priority for this mission, depending on the commander's ability to operate in red space.

Mission Thread 2: "Cyber Integration Mission Plan: defend against a high probability cyber-attack on a base in the Pacific AO." Identify cyber infrastructure supporting current and planned missions, which identifies METs and critical assets (from which KT-C are derived). In this example, critical assets include border routers, honeypots, and end point and network monitoring devices. Critical services include access control, user activity monitoring, data loss prevention monitoring, data backups, a COOP plan, Incident Response capabilities, and user access control.

[Distribution Statement A] Approved for public release and unlimited distribution.

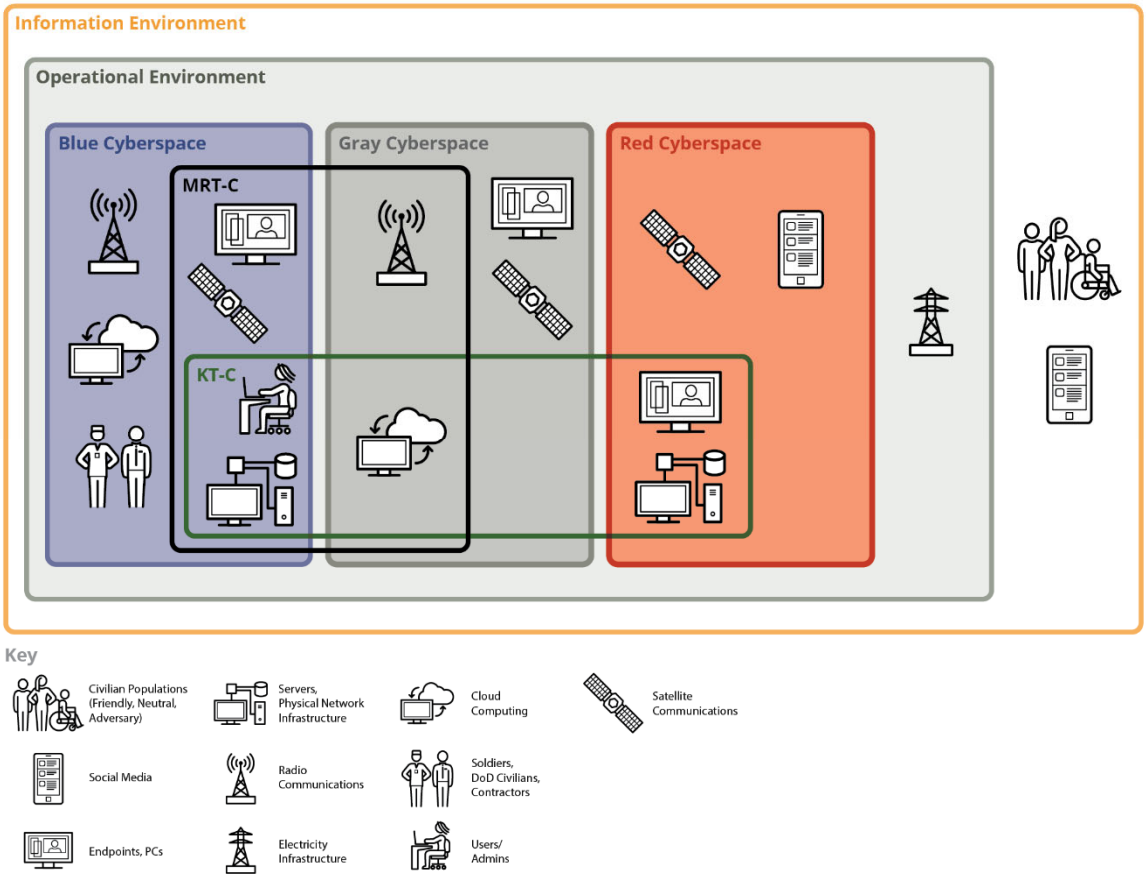

Figure 1: Mission Thread 2

Mission-critical assets and capabilities:

- tactical communications
- intel and C2 infrastructure, data, and functions
- physical defense of IT assets

Mission-essential capabilities:

- backup, IR, and COOP plans
- visualization tools
- DCO-RA

Cyber services, applications, data, and processes needed for this mission, which include protecting cyber capabilities that support other missions in this AO: Some are MRT-C if they support TCAs, DCAs, or mission-critical assets.

- communications infrastructure (email, VTC/VOIP, Microsoft Teams, radio)
- applications, data, processes, and services that update information in accordance with the commander's decision-making (Observe–Orient–Decide–Act loop) cycles: sensor data; threat intel to

[Distribution Statement A] Approved for public release and unlimited distribution.

answer the commander's critical information requirements; visualization tools; situational awareness of self, allies, and adversary
- Knowledge of AO-wide mission-essential assets' vulnerabilities, mitigations, and methods of remediation
- Physical defenses for cyber equipment; limit access to cyber equipment to essential personnel only; confirm backup and continuity of operations (COOP) plans are ready to employ (METs)
- Security operations network, host, and appliance monitoring tools and services
- Incident Response capabilities

MRT-C is identified during Mission Analysis (MA), COA development, and MET and MEF development with their underlying capabilities mapped back to assets. In this mission, they include

- gray cyberspace MRT-C: communication infrastructure and pathways used by red and blue actors and gray cyberspace cloud services and data used by the JFC
- blue cyberspace: mission-essential assets, data, services, functions, and virtual/persona functions supporting DCO and DCO-RA capabilities, and satellite communications

Gray and blue cyberspace cloud services may overlap when, for example, blue data is managed by gray services. In this example, blue cloud services and data are not identified as MRT-C.

Key terrain:

1. satellite communications in blue and gray space
2. blue space servers, data, network infrastructure, and end points
3. gray cyberspace cloud computing services and data hosting services used by the JFC
4. red space servers, data, and network infrastructure threatening offensive cyber actions targeting blue space capabilities
5. Key terrain-cyber:
   - blue cyberspace: border routers, BGP application, logs, honeypots, other mission-critical assets, and virtual/logical assets used in DCO-RA actions. These assets provide capabilities used in Key Terrain Items 1 and 2.
   - gray cyberspace: cloud computing services and data. These assets provide or support capabilities in Key Terrain Item 3.
   - red cyberspace: servers, network infrastructure, and endpoints used in the attack on blue space. These assets provide adversary capabilities for Key Terrain Item 4. The commander may determine that degrading these adversary capabilities is a priority for accomplishing this mission.

[Distribution Statement A] Approved for public release and unlimited distribution.

Discussion and Recommendations

Military operations, including those in cyberspace, take place in contested environments with degraded capabilities due to adversary actions or environmental conditions. Therefore, commanders must prioritize efforts to protect high-priority (mission-critical and mission-essential) tasks, functions, and capabilities and the assets that provide them because they cannot prioritize protecting everything. Setting these priorities correctly requires clear communications between different echelons of command and responsibility so that the highest-priority assets, services, functions, and capabilities are accurately identified, and appropriate attention and resources are devoted to protecting them according to the JFC's mission goals, in order of prioritization from mission critical down to mission enhancement.[9]

With this in mind, we recommend the following:

1. Include definitions of CO terms such as MRT-C and KT-C in documents and artifacts as the author uses them together with canonical references, if they exist. CO terms continuously evolve while documents may persist and serve as references beyond the meaning of a term or concept at publication time. The author's definition of terms will help current and future readers understand the intent and meaning of the term as the author uses it. If no canonical reference exists, an author's definition would be even more valuable.
2. Avoid using terms that are like, or mix, doctrinally defined terms (e.g., "critical cyber terrain") unless a unique meaning is assigned to the term. If similar or mixed terms are used, authors should define the exact meaning of the term so that readers are not left to infer the intended meaning for themselves.
3. Authors should explain the assumptions they make and the logic they follow to identify MRT-C, KT-C, and related concepts and terms. The reader should be able to follow decision-making logic and understand how these relate to the mission and risk assessments. Readers at appropriate echelons of responsibility or command should be able to logically relate the specific mission, MRT-C, KT-C, decisive points, key terrain, and TCAs.

   A way of thinking of the relationship between TCA, MRT-C, and KT-C is to start with a TCA for which there exists a risk factor specifying a possible means of attack that adversaries could leverage to compromise the mission. Associating a means of attack with a mission-critical or

---

[9] From Chairman of the Joint Chiefs of Staff 2019, p. 2:

(1) Mission Critical. Prevents accomplishment of mission or leads to direct impact on mission failure; no work-around or alternative exists. Capability needed immediately to mitigate risk.

(2) Mission Essential. Adversely affects the accomplishment of, or degrades mission accomplishment, and no acceptable work-around or alternative solutions exist; requirement is needed to maintain sufficient military capability or readiness and is needed no later than a specific date to prevent the loss/degradation of capability or readiness.

(3) Mission Improvement. Employment of capability increases mission accomplishment or mitigates threats to mission and mission essential capability and work-around/alternative solutions have been identified.

(4) Mission Enhancement. Addresses enhancements not critical or essential for mission accomplishment; increases efficiency, addresses user/operator annoyance with system functions beyond a help desk or problem report to resolve.

[Distribution Statement A] Approved for public release and unlimited distribution.

mission-essential cyber asset identifies it as MRT-C and may identify its capabilities as key terrain—that is, if these are critical to the success of the mission and if degraded capability were to risk mission failure.

4. Evaluate the accuracy and value of MRT-C and KT-C models to accomplishing the mission. What procedures exist to validate how accurately the MRT-C–KT-C model identifies cyberspace-related key terrain in a mission in a timely manner?
    a. The Mission Assurance Decision Support System is used in mission planning to identify and manage IT and cyber assets and infrastructure that support that mission's TCAs. It stores information that identifies, nominates, validates, and approves TCAs. It is used for mission decomposition and TCA identification and thus MRT-C identification [Office of the Joint Chiefs of Staff 2023, p. 4].
    b. A model may fail to reflect reality due to bias or the inability of the model to capture complexity in a useful manner. It may also be limited by the quality, completeness, and timeliness of its data. How do we address these?
    c. Do the collection and processing of data used to identify MRT-C depend on manual procedures? Do they scale adequately as the size and complexity of a mission increases?
    d. Are there procedures or tools available that can improve the reliability and accuracy of identifying and prioritizing MET, MRT-C, and KT-C?
    e. After-the-fact analysis of the accuracy and completeness of planning processes' results should facilitate measuring how well MRT-C and KT-C were identified prior to mission execution.
    f. Methods such as dependency modeling (e.g., Johns Hopkins Applied Physics Lab DAGGER tool10) may provide alternative ways of measuring the accuracy and value to the mission commander of identifying MRT-C and KT-C using current methods.

Conclusion

Terms used to integrate CO into multidimensional mission analysis and mission planning must communicate concepts clearly in a manner that conforms to existing operations-planning processes and that commanders and their staff can clearly understand. The same terms must also effectively and unambiguously communicate orders to the cyber soldiers, airmen, sailors, marines, and guardians—the technical experts who create, administer, and defend the cyber tools and assets that provide functions and capabilities for cyber and cyber-supporting operations.

[10] https://www.jhuapl.edu/dagger/

[Distribution Statement A] Approved for public release and unlimited distribution.

Our purpose is to describe a subset of cyberspace operations terms relevant to our work supporting cybersecurity missions, focusing on DCO, and to state our understanding of clear, usable definitions for these terms in our work.

Glossary

Includes definitions, if not previously given.

CC/S/A/FA	Combatant Command / Service / Agency / Field Activity
CKT	Cyber Key Terrain
DCA	Defense Critical Asset
DCO-RA	Defensive Cyber Operations – Response Actions
KT	Key Terrain
KT-C	Key Terrain – Cyber
MEF	Mission-Essential Function
MET	Mission-Essential Task
MRCT	Mission Relevant Cyber Terrain
MRT-C	Mission Relevant Terrain – Cyber
TCA	Task Critical Asset

Bibliography

URLs are valid as of the publication date of this report.

[DoD 2018]

Mission Assurance (MA). DoD Directive 3020.40, Change 1. Department of Defense. 2018. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040p.pdf?ver=2018-09-11-131221-983

[DoD 2022]

Mission Assurance Construct. DoD Instruction 3020.45, Change 1. Department of Defense. 2022. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/302045p.pdf?ver=2018-08-14-081232-450

[Distribution Statement A] Approved for public release and unlimited distribution.

[Joint Chiefs of Staff 2009]
Joint Intelligence Preparation of the Operational Environment. Joint Publication 2-01.3. Office of the Joint Chiefs of Staff. 2009. https://www.usna.edu/Training/_files/documents/References/1C%20MQS%20References/Joint%20Publication%202-01-3%20JIPOE.pdf

[Joint Chiefs of Staff 2018]
Cyberspace Operations. Joint Publication 3-12. Office of the Joint Chiefs of Staff. 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-15

[Joint Chiefs of Staff 2019]
Requirements Management Process for Mission Partner Environment. CJCSI 6290.01. Office of the Joint Chiefs of Staff. 2019. https://www.jcs.mil/Portals/36/Documents/Library/Instructions/CJCSI%206290.01.pdf?ver=2019-10-03-132509-320

[Joint Chiefs of Staff 2021]
DoD Dictionary of Military and Associated Terms. Joint Doctrine Library. 2021. https://www.supremecourt.gov/opinions/URLs_Cited/OT2021/21A477/21A477-1.pdf

[Joint Chiefs of Staff 2023]
Mission Assurance Construct Implementation. CJCSI 3209.01A. Office of the Joint Chiefs of Staff. August 2023. https://www.jcs.mil/Portals/36/Documents/Library/Instructions/CJCSI%203209.01A%20(JS-221219-T8WP)%20VDJS%20Signed.pdf

[Paulsen 2018]
Paulsen, C. The Trouble with Terms. *IT Professional*. Volume 20. Issue 6. November/December 2018. Pages 5–8. https://ieeexplore.ieee.org/document/8617759

[Pederson 2022]
Pederson, Maj Eric; Palermo, Don; Fancey, Stephen; & Blevins, Tim. *DoD Cyberspace: Establishing a Shared Understanding and How to Protect It*. Air Land Sea Space Application Center. 2022. https://www.alsa.mil/News/Article/2891794/dod-cyberspace-establishing-a-shared-understanding-and-how-to-protect-it/

[USCYBERCOM 2018]
U.S. Cyber Command. *2018 Cyber Space Strategy Symposium Proceedings*. July 2018. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Cyberspace%20Strategy%20Symposium%20Proceedings%202018.pdf?ver=2018-07-11-092344-427

[Voice 2022]
Voice, Jeffrey A., Col. (Ret). Leveraging the Ontology of the Operational Cyber Mission Stack (OCMS). *The Cyber Defense Review*. Fall 2022. Pages 109–119. https://cyberdefensereview.army.mil/Portals/6/Documents/2022_fall/07_Voice.pdf

[Distribution Statement A] Approved for public release and unlimited distribution.

Legal Markings

Copyright 2024 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This work is licensed under a Creative Commons Attribution-Noncommercial 4.0 International License. Requests for permission for non-licensed uses should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

DM24-0048

Contact Us

Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

Phone: 412/268.5800 | 888.201.4479
Web: www.sei.cmu.edu
Email: info@sei.cmu.edu