Mission Thread Analysis: Establishing a Common Framework

in a Multi-discipline Domain to Enhance Defensive Cyberspace Operations

Colonel George I. Corbari
Colonel Neil Khatod
Colonel John F. Popiak
Pete Sinclair

ABSTRACT

The multi-disciplinary nature of Cybersecurity, Cyberspace Security, and Defensive Cyberspace Operations (DCO) has resulted in different interpretations of cyber-related terms among various groups. The communication gap between cybersecurity professionals and operational professionals has increased over time. Cybersecurity professionals struggle to establish priorities of work as they define and frame the risks differently from mission-focused operating professionals. Miscommunication results in a different understanding of mission requirements and different expectations between those requesting support and those providing support. Despite progress in cybersecurity tools and processes, the communication gap endures. Presently, ARCYBER is challenged to balance the demands of mission commanders requesting defense of critical missions, Congress directing actions to defend critical resources, and intelligence reports, all resulting in diversion of resources to address perceived threats. Mission Thread Analysis (MTA) is a process to help build understanding and consensus between customers (operational force) and providers (network operators and defenders), offering an analytical framework where both sides detail

This is a work of the U.S. Government and is not subject to copyright protection in the United States. Foreign copyrights may apply.

COL George I. Corbari is an Army Strategist who has served in U.S. Army Cyber Command and U.S. Cyber Command for the past 7 years. He is currently a Strategic Advisor to the Commander, ARCYBER. During the past seven years, he has served as the ARCYBER G5, Director of the Commander's Strategic Initiatives Group (ARCYBER), and Director of the Combined Action Group (USCYBERCOM). Over a 30-year career he has served throughout the United States, in the Indo-Pacific, Europe, and Afghanistan. He began his career as an Interrogator/Russian Linguist and served as an Air Defense Officer. COL Corbari holds an M.S. from the Eisenhower School for National Security and Resource Strategy, a M.Ed. in Human Performance Enhancement from Western Washington University and a B.A. in Education from Bethany College, KS.

their operational and technical requirements. MTA requires mission owners to analyze, prioritize, and depict a mission as a series of steps within a Mission Process Thread (MPT), including the data pathways or Mission Engineering Threads (MEngTs) required to complete the mission. Integrating MTA results with threat intelligence enables appropriate planning and coordination to apply the right capability to perform DCO in support of Army requirements. ARCYBER redesigned and formalized the MTA process to help inform prioritization, training, team employment, and optimization of Defensive Cyber Forces. This new MTA process, or a similar adaptation, will prove useful in planning and coordination of cybersecurity efforts across a broad range of actors, including, but not limited to: Interagency Partners; State, Local, Tribal, and Territory (SLLT) Partners; the private sector, and international partners by defining cyber defense requirements in terms in common all actors.

INTRODUCTION

Over time network operators and network defenders created terminology to describe how they mitigated vulnerabilities and contended with threats. For example, as the terms Cybersecurity,[1] Cyberspace Security,[2] Cyberspace Defense,[3] and Defensive Cyberspace Operations (DCO)[4] evolved and came into use by cybersecurity professionals, the nuances in the different definitions created gaps in understanding between cybersecurity professionals and operational professionals.[5] The different terms, often used interchangeably by operational professionals, contribute to confusion when addressing support requirements. It is particularly important when determining the degree of protection or defense required within cyberspace (see Textbox 1:

COL Neil Khatod recently retired from serving as the ARCYBER G-3, Director of Operations Officer. He has served in various leadership and staff positions during his 29-year career. Recent positions include serving the Chief of Defensive Operations (G36) for ARCYBER and as the commander of the 2nd Theater Signal Brigade in Germany. Colonel Khatod received his commission through the United States Military Academy at West Point where he graduated in 1994 with a Bachelor's degree in Spanish and French. He also has advanced degrees from the University of Oklahoma (Master's in Human Relations), the University of Maryland (Master's in Information Technology), and the National War College (Master's in National Strategy and Policy). He recently became the Chief Information Officer and Veterans Outreach lead at Hays Americas.

Differing Terminology

Cybersecurity vs Cyberspace Security vs Cyber Space Defense vs Defensive Cyber Operations vs Defensive Cyber Actions…

Consistent across multiple Department of Defense publications and strategies, oint doctrine uses the term "cyberspace security" to distinguish the tactical-level cyberspace action from the policy and programmatic term "cybersecurity" used in the Department of Defense (DoD) and United States Government (USG) policy. In order to enable more effective planning, execution, and assessment, joint doctrine distinguishes between cyberspace security and defensive cyberspace actions. DoD and USG cybersecurity policy make no such distinction, instead employing the term cybersecurity, to include the ideas of both security and defense. Doctrine uses "cyberspace security" to describe specific actions as described in this paper and "cybersecurity" only in reference to DoD or national policies for protecting cyberspace.

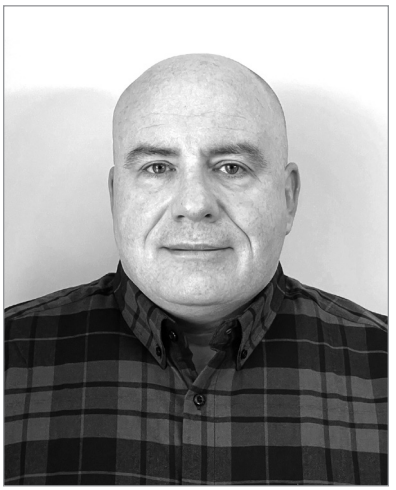
Textbox 1

Differing Terminology). To put it another way, the distinction between a proactive mitigation of vulnerabilities to prevent exploitation and execution of DCO while contending with an active threat is often lost in translation between mission owners and cyberspace professionals.[6] As a result, cybersecurity professionals struggle to establish priorities of work as they define and frame the risks differently from the operating professionals who are focused on mission accomplishment. Each group uses the same or similar words, but with different intentions or meaning. As an example, FM 3-90 defines "Disrupt" as "…a tactical mission task in which a unit upsets an enemy's formation or tempo and causes the enemy force to attack prematurely or in a piecemeal fashion."[7] However, FM 3-12 Cyberspace Operations and Electromagnetic Warfare[8] and JP 3-12 Cyberspace Operations defines "Disrupt" as "to completely but temporarily deny access to, or operation of, a target for a period of time. A desired start and stop time are normally specified. Disruption can be considered a special case of degradation where the degradation level is 100 percent."[9]

COL John F. Popiak is a cyberwarfare officer who has held command and staff positions across the Army, Cyber Command, and National Security Agency with assignments in the United States, the Republic of Korea, Europe, Africa, and Afghanistan. COL Popiak has served in a wide variety of tactical, operational and strategic cyberspace assignments. COL Popiak's previous green-tab leadership experience ranges from airborne rifle platoon leader through brigade commander of the US Army Cyber Protection Brigade.

Miscommunication results in a different understanding of mission requirements and expectations between those requesting support and those providing support within the cyberspace domain. However, where cyberspace is concerned, the breakdown results in stark differences between a mission commander's ability to operate and the technical requirements needed to securely support critical operations via cyberspace capabilities. The tension between mission command requirements and network and system security requirements adds to the challenge of those charged with DCO. Despite progress in cybersecurity tools and responses, the communication gap endures, leading to a growing disconnect between customers (mission commanders) and providers of cybersecurity. As the Cyber Mission Force (CMF)[10] has matured, so have their techniques, tactics, and procedures. What was once considered the most effective approach to defending "assets" is now considered ineffective because no asset exists separate from the systems and networks it is connected to within cyberspace. Additionally, missions commonly extend beyond the Department of Defense Information Network (DoDIN) assets to off-DoDIN systems and networks.[11]

ARCYBER presently faces numerous demands by mission commanders requesting support to defend critical missions, Congressional directives[12] to defend critical systems, and intelligence reports highlighting that the Internet is a dangerous place, resulting in diversion of resources to address perceived threats. Such demands prevent ARCYBER from effectively planning, affecting training and readiness as well as resource allocation. Finally, without a comprehensive understanding of residual risk, Army leaders are unable to understand well enough when and where they are accepting risk to systems and networks. When a crisis such as "Solar Winds"[13] occurs, Cyber Protection Teams (CPT) and analytic support capabilities are redirected from



Mr. Pete Sinclair is currently employed by Peraton as a Cyberspace Operations Planner in support of the Army Cyber G5. He retired from the Army after serving in three different branches over twenty-one years and six deployments. He is a graduate of Northern Michigan University and the School of Advanced Military Studies. He is also a graduate of the Harvard Kennedy School's Executive Education Leadership in Homeland Security program and the Homeland Protection Course at the Massachusetts Institute of Technology's Lincoln Laboratory.

their current missions to address the crisis. Prior to 2022,[14] the Army had no process for determining where it would accept risk when re-missioning capabilities to concentrate on an emerging crisis, instead relying solely upon the ARCYBER CDR to make decisions and accept risk beyond his/her scope.

In June 2020, Headquarters Department of the Army (HQDA) published HQDA Execution Order (EXORD) 211-22 requiring planners to identify Commander Critical Mission Threads and their corresponding Mission Engineering Threads, and the intelligence community to provide known and perceived threats. Finally, ARCYBER planners match those findings against the existing capabilities and capacity of ARCYBER and other Army resources to conduct DCO or provide mitigation. EXORD 211-22 outlines a process to prioritize DCO missions and related mitigation activities for approval by Army senior leaders and identifies residual risk which those leaders either accept or direct additional resources for action (see Figure 1). To address the various communication gaps and minimize confusion among all parties, we propose Mission Thread Analysis (MTA) by providing an analytical framework where all stakeholders detail their operational and technical requirements, while providing threat-informed analysis to advise and optimize DCO planning and execution.

In 2013, the Department of Defense (DoD), in collaboration with Carnegie Mellon University's Software Engineering Institute, developed the concept of a "Mission Thread Workshop." The collaboration resulted in defining "mission thread" as a sequence of end-to-end activities and events, given a series of steps, that provide one or more of the capabilities that the "system of systems" supports.[16] The introduction of a mission thread perspective has shifted focus from individual systems or equipment as stand-alone components to the realization that effective cybersecurity

must involve the identification of end-to-end data flows, usually across multiple systems.[17] Out of this understanding and the lessons learned over numerous defensive cyber operations,[18] ARCYBER planners designed the concept of Mission Thread Analysis to improve the efficiency and capacity of CPTs[19] and to support increased support from the ARCYBER staff.

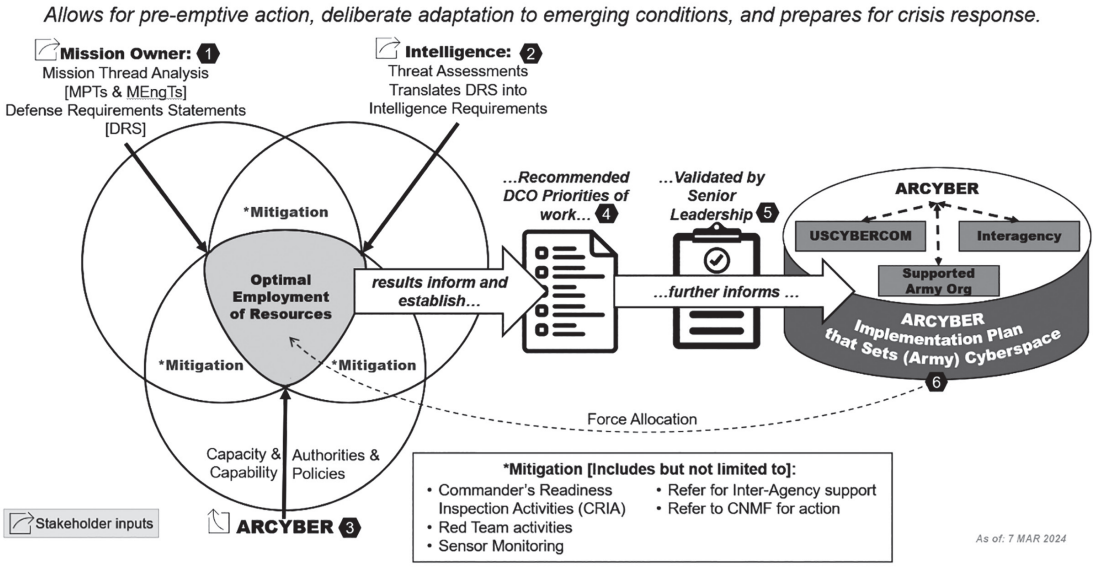


Figure 1. Optimization of Defensive Cyber Operations.[15]

Figure 1 starts with an MTA. This step requires mission owners to analyze and prioritize their critical missions and conduct and MTA to determine their DCO requirements. Mission owners depict the process of a mission as a series of steps or actions required to achieve successful accomplishment. For clarity, we call this the Mission Process Thread (MPT).[20] See Textbox 2, Mission Process Thread.[21] The MPT could be as simple as articulating a "kill chain." For example, an air defense radar detects enemy aircraft sending information to an engagement control station, and the personnel in the engagement control station communicate with the air space coordination authority to confirm the target and gain clearance of fires (see Table 1). Once cleared to fire, the battery fires a surface-to-air missile against the enemy aircraft on order of the engagement control officer. While that kill chain scenario is only part of the story, the steps tell us "what" and a little about "who" and "how," but not the details or the systems and networks involved. To get those details we need to examine the second part of MTA, the Mission Engineering Thread.

Defining "Mission Process Thread"

Based upon classified reports, notes, and AAR data following efforts to plan for and execute defensive cyberspace operations, we identified patterns of confusion across supported commands. In practice, we discovered that participants confused and interchangeably used the terms Mission Thread and Mission Engineering Thread. To alleviate the confusion of participants in MTA efforts, ARCYBER uses the term Mission Process Thread to distinguish between the two original terms. Mission Process Thread and Mission Thread share the same definition found within the "DoD Mission Engineering Guide."

Textbox 2

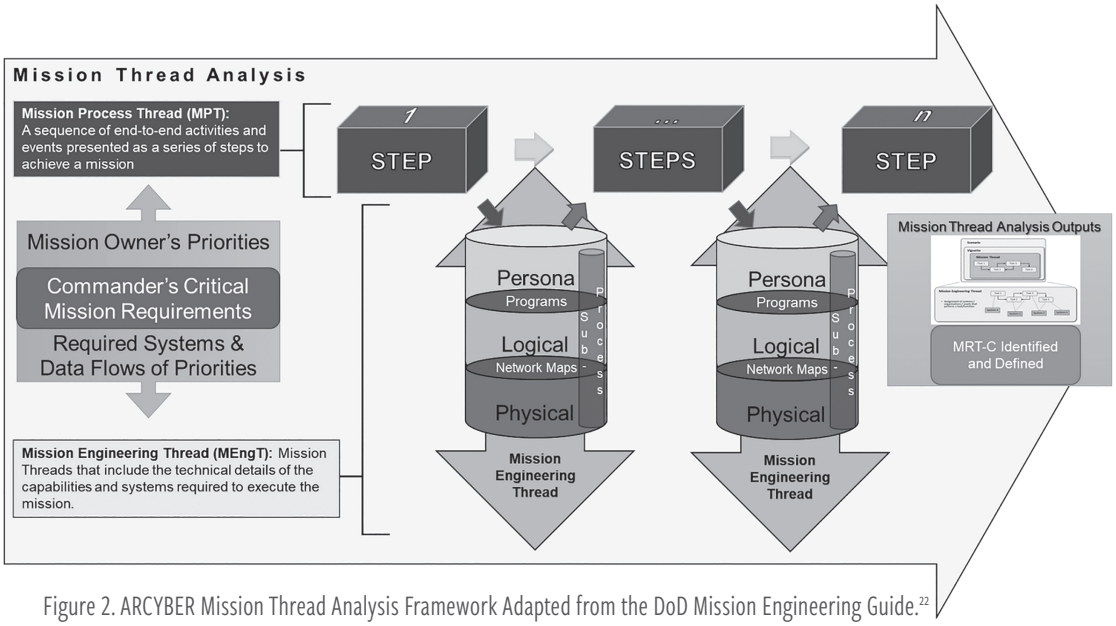


Figure 2. ARCYBER Mission Thread Analysis Framework Adapted from the DoD Mission Engineering Guide.[22]

The Mission Engineering Thread[23] (MEngT[24]) includes the hardware, systems, and networks that support the data pathways across the Persona, Logical, and Physical layers of cyberspace required to complete the mission, as described by the MPT.[25] In the example above, we would

Components of ARCYBER's Mission Thread Analysis

Mission Process Thread (simplified)	Mission Engineering Thread (simplified)
Sense to observe and identify air threats	Radar, detects aircraft through electromagnetic spectrum detection, communicates air picture through data passed to engagement control station via fiber network
Identify aircraft, detect track, provide early warning	Engagement control station receives and analyzes data portraying the target on the engagement control screen; the engagement control system identifies the track as hostile based on internal database prompting early warning alert sent as digital message over multiple command and control networks (SIPR, Mission Command Systems, Link16, fiber to big voice, and cellular messaging systems
Track aircraft, determine friend or foe	Radar and engagement control station continue to communicate track updates via fiber, track data is forwarded to the area air defense coordination cell for awareness via Link16
Confirm enemy track, gain clearance of fires	Voice and or data messaging used to confirm enemy aircraft via HF radio, TACSAT, Link16, and VOIP to communicate clearance of fires
Confirm track, fire missile, engage aircraft	Radar and engagement control station continue communicating updates via fiber, order to fire provided to system manually initiating engagement and missile launch via fiber and or line-of-sight communications
Track missile engagement, confirm battle damage assessment	Radar continues to communicate track data to the engagement control station via fiber, receives data regarding missile launch via line-of-sight communications and begins communicating with the missile in flight via HF encrypted messages to provide course correction; radar detects engagement via electromagnetic spectrum observation noting the destruction of track
Return to previous status: sense to observe and identify air threats	Operators confirm engagement with the airspace coordinator via voice or data systems and return all detection and firing systems to previous status via commands over fiber in order to observe additional threats

Table 1. Example: Fictional Kill Chain to Represent Application of MTA.

identify the MEngT from the point of detection by the radar to the system communication with the engagement control station, voice or data communication with the airspace coordination authority, continued communication between the engagement control system and the radar system, followed by the transmission of "fire" to the launching station and the follow-on data flows between various systems to complete the engagement. Identifying these MPTs and MEngT provides a complete MTA. Table 1 provides more detail on this MTA.

This fictional "kill chain" is an oversimplification to provide a broad overview of the nuances between MPT and MEngT. In the Army, we typically receive the MPT from the Operations Officer (S3 or G3). The organization's Signal Officer or Communications Officer typically provides the MEngT that includes the technical elements necessary to execute the data flows associated with all the systems and networks required to accomplish the mission. In the past, Mission Commanders would express their need to execute critical missions and request "protection" or the need to have "mission assurance." This approach required significant research and understanding by CPTs prior to their mission execution. Additionally, CPTs required very detailed technical data on specific systems or portions of networks. Although systems and databases exist to provide this information, they tend to be outdated due to lacking organizational/system owner compliance.[26] Only through gaining a full understanding of the processes and systems involved in a particular mission can CPTs have a running start to execute their mission most efficiently and effectively. The coherent identification of requirements resulting from the MTA enables ARCYBER to begin prioritizing missions and identifying risks in preparation for planning DCO missions over time.

With MPTs and MEngTs developed, the MTA provides both non-cyber and cyber representatives a common framework and shared understanding of the problem. Capturing the results of an MTA in a Defense Requirements Statement (DRS)[27] enables ARCYBER to make informed decisions about establishing priorities of work for DCF employment. The DRS is a simple fill-in-the-blank or "Mad-Libs" format that a mission owner uses to articulate its protection and defense requirements in cyberspace. The DRS allows easier understanding by mission owners of their own requirement. Further, the blanks guide the mission owner to provide the basic information required to start DCO planning and prioritization. The DRS also supports ARCYBER participation in USCYBERCOM's Cyber Forces Mission Allocation Process (CFMAP).[28] The CFMAP allows USCYBERCOM to make informed decisions on mission prioritization and apportionment of forces across the services and the various Joint Force Headquarters - Cyber (JFHQ-C). MTA also enables identification of DCF training requirements to be completed before rendering assistance. MTA enables development of the rough time estimates for a DCF to complete the mission. The MTA and the DRS serve as a confirmation brief between all parties related to the DCO mission. Finally, with the definition of MRT-C above, MTA allows for a mission analysis that will support discussions and planning with IA partners regarding the protection of MRT-C that resides outside of DoD Cyberspace.

Another value of the DRS is that it serves to start the creation of intelligence requirements within ARCYBER and the larger Intelligence Community. As captured by Figure 1 in step two, the DRS start to inform existing collection management, single source reporting, and ultimately synthesis into an all-source intelligence product regarding threats to known MRT-C. With this intelligence in hand, determinations are made regarding threats to MRT-C and if any action needs to be taken. If a response is required, step three covers determining what form that response takes. A specific response takes into account existing priorities of work and existing authorities. From there the response takes the form of a CPT under the direction of ARCYBER or if a broader response from USCYBERCOM or an interagency response is required. MTA enables ARCYBER to move from being asked to "Cyber all the things," to focus on defending specific Mission Relevant Terrain-Cyber (MRT-C)[29] for a specific Mission Owner purpose.

While the DCO-Optimization process, supports timely tactical execution of DCO, the MTA and its results also support long-term strategic decisions made by ARCYBER and beyond in steps four and five. USCYBERCOM allocates CPTs to the Army to conduct DCO through both active defense missions and providing passive measure plans to network operators based on data analytics and intelligence reports. By ARCYBER consolidating and submitting DRS to USCYBERCOM, it helps inform future force allocation decisions. Further, those same DRS help inform priority of work decisions by ARCYBER and HQDA. The MTA informs prioritization, force allocation decisions, and future intelligence requirements. MTA enables prioritization of DCO missions through a more coherent understanding of the processes and systems involved, compared to Army priorities further supported by intelligence reporting that enables better risk analysis. So while the other Army Service Component Commands (ASCCs) have "Set the Theater" tasks; as depicted in step six ARCYBER has a "Set Cyberspace" task for the Army and for portions of the Joint force.

For the Army, the MTA process helps ARCYBER to prioritize, train, employ, and resource Defensive Cyber Forces (DCF),[30] optimizing employment of these limited resources by matching the requirement with the right-sized DCF element and skill set. The MTA is not designed to be Army specific, it was designed to be service and department agnostic. MTA also identifies remaining gaps requiring mitigation or acceptance of risk at by the appropriate decision-mak-ing authority. Appropriate prioritization allows ARCYBER to apply limited capacity against the highest concerns and risks from the Army's perspective. Effective optimization of the Cyber Protection Force (CPF) allows ARCYBER to apply the right capabilities against appropriate prob-lem sets, which sometimes requires significant training or even certification prior to mission execution. For example, training personnel to defend data appropriately in the Amazon Web Services (AWS) cloud requires X months of training and certification, while training personnel to defend Microsoft (MS) Azure cloud requires separate training lasting Y months. Finally, the combination of prioritization and optimization better positions ARCYBER to recommend which forces to re-mission during crises when emerging requirements dictate a shift in resources.

Different cultures and lexicons of customers (operations and mission commanders), cybersecurity and cyberspace security providers (like those across the DoD), Inter-Agency (IA) partners, the private sector, and non-federal jurisdictions all create friction that negatively impacts the government's ability to contend with the effects caused by Malicious Cyber Actors (MCA). MTA helps translate the needs and requirements among the cultures by providing a framework that utilizes definitions used in common that are easily understood by all cultures and varying levels of cyber expertise. To overcome this friction, ARCYBER is incorporating concepts from the DoD Mission Engineering Guide, Carnegie Mellon University's Software Engineering Institute's "Introduction to the Mission Thread Workshop," and RAND Corporation's "Cyber Mission Thread Analysis: A Prototype Framework for Assessing Impact to Missions from Cyber Attacks to Weapon Systems," to inform and establish MTA as a formal process in support of HQDA EXORD 211-22 "Army Support to Defensive Cyberspace."

ARCYBER's Operational Lessons Learned

This ARCYBER depiction of Mission Thread Analysis takes the original model established within the DoD Mission Engineering Guide and expands Mission Engineering Threads into an abstraction that depicts the detail required to support Defensive Cyberspace Operation planning and execution. A detailed abstraction requires Mission Owners to start identifying, defining, and depicting Mission Relevant Terrain – Cyber both on and off DODIN required for the successful completion of a mission.

Textbox 3

Based on ARCYBER's operational lessons learned over the past several years,[31] a thorough MTA enables a common framework to facilitate discussions, establish common understanding of the problem across cultures, and establish priorities of work for conducting DCO, with impacts on cybersecurity and cyberspace security efforts writ large. Establishing MTA as a common framework to facilitate DCO planning and execution allows cyber and non-cyber

Data Rationalization Effort as a Way of Understanding MTA

In the summer of 2023, ARCYBER commissioned a study to provide an end-to-end visualization and analysis of the DoDIN-A enterprise information systems data environment, including DoDIN Operations and Defensive Cyberspace Operations processes. The process generated a complex diagram depicting the "ARCYBER Data Ecosystem Current State." The undertaking involved surveying and mapping hundreds of data feeds being ingested and used across the ARCYBER Enterprise considered mission essential for operating and defending the DoDIN-A. The exhaustive effort included nearly 300 interviews across 13 organizations within the ARCYBER Enterprise. The deliverable included a current state, high-level visual overview of ARCYBER's data ecosystem. To achieve this outcome, planners researched the following questions:

1) What data does ARCYBER have?
2) Where are the data going?
3) What decisions are made with the data?
4) Who uses the data?
5) What are the data gaps?

The results provided the ARCYBER Commander with a mission commander's understanding of various MPT, along with seven actionable recommendations, which included improvement to empower cyber defenders to defend critical networks and associated mission process threads more proactively. The power of the "ARCYBER Data Ecosystem Current State" visualization has led the ARCYBER Commander and Technical Warfare Center leadership team to brief the findings to the Secretary of the Army, the Chief of Staff of the Army, the Principal Cyber Advisor, the Army Chief Information Officer, and the HQDA G-6, as well as numerous Congressional Delegations.33

ARCYBER Example

stakeholders to have a common understanding of the problem and effectively communicate priorities and identify risk. More importantly, MTA helps leaders more clearly sense and better understand[32] threats and vulnerabilities within the cyberspace domain, enabling well-informed decisions, and allowing the optimal employment of cyber protection forces as they act in partnership with Inter-Agency, industry, and allied partners.

Mission Thread Origins

Various definitions of "Mission Threads" are in use within systems engineering, mission engineering, and software engineering disciplines to describe and depict processes. While the disciplines share a common use of process maps, they differ radically in how they depict the processes they describe. While acknowledging the differences in the definitions used by the disciplines, the ARCYBER MTA process is grounded in the Mission Thread and Mission Engineering Thread definitions found within the DoD Mission Engineering Guide. The Mission Engineering approach recognizes the cross-disciplinary nature of the systems within a system-of-systems required to execute and accomplish a mission. Mission Engineering also shows the distinction between accounting for the steps required to achieve a mission and the technical details behind the systems that support the data flow within and between systems to support a mission. Given this background, Mission Thread Analysis uses the terms Mission Process Thread and Mission Engineering Thread to capture both the operational and the technical process details to better support DCO planning and execution in support of mission owners.

ARCYBER's Cyber Protection Brigade has been performing mission analysis based on Mission Threads with mission owners for several years. One of the benefits of MTA is that earlier mission analysis enables optimization of limited DCO capacity. Advanced analysis prior to mission execution allows the CPT to focus on mission planning rather than having to research the technical details of the mission environment, enabling significant time savings. This optimization of resources makes it possible for Defensive Cyber Forces (DCF) to perform more missions over a given period.

Mission Thread Analysis Process

The MTA starts with the identification of a Mission Process Thread. Developing Mission Process Threads is a G3/S3/Mission Owner responsibility and is based on the commander's prioritization of missions/key processes (see Textbox 4). Without established priorities from the commander/G3/S3/Mission Owner, the G6/S6/Chief Information Officer (CIO) and supporting Information Technology Department must make educated guesses about the criticality and potential risk to mission processes and associated systems. Conversely, if the commander focuses protection requirements on missions, a G6/S6/CIO will gain a better understanding of potential vulnerabilities and protection requirements. Moreover, asset-focused requirements obscure the entirety of mission requirements, particularly those that *reside off-DoDIN or outside*

Elements of Mission Thread Analysis

"Developing..." is an iterative process of Identifying, Defining, and Depicting Mission Process Threads and Mission Engineering Threads collaboratively.

Identify, Define, and Depict, cover an ever-increasing amount of detail:

- **Identify** is only the name of the task or system requiring further analysis.
- **Define** covers answering basic questions in words that include, but not limited to the steps of the process, where MRT-C resides, who is responsible for the MRT-C, etc...
- **Depict** provides the most detail and the term is used for the final graphics or network map that show a MT and/or MEngT.

This stratification establishes the different levels of details required to make certain decisions, making clear this is an iterative process to increase understanding. Previously, directives tasked organizations to engage in the daunting task of creating comprehensive network maps without any priorities. Progressing iteratively provides priorities of work for mapping/depicting efforts. Additionally, the stratification provides for a demarcation where the effort must stop if it starts to identify MRT-C that resides off-DDIN. For off-DDIN MRT-C, the task is to identify and define resources only to the extent that it is useful for conversations with IA Partners. The intent is not to depict off-DDIN MRT-C and run afoul of Intelligence Oversight concerns or to violate limitations of authorities.

Textbox 4

the span of control or responsibility of the commander/mission owner. Focusing on a Mission Process Thread, rather than specific assets, assists in more accurately identifying MRT-C outside of a unit's responsibilities and/or off DoDIN. In other words, focusing on assets that an organization owns versus focusing on what it uses as a customer, omits potential vulnerabilities and systems required for operations/mission execution.

Once the G3/S3 or a commander approves final MPT products, the development of Mission Engineering Threads (MEngT) can begin in earnest. An MEngT describes and depicts the processes and systems that handle data connecting the operational steps outlined in the Mission Process Thread. An MPT will have more than one MEngT and those MEngTs are likely to grow in complexity as analysis continues into further steps of the MTA. MEngTs include, but are not limited to systems, information exchanges, nodes, and data storage. In the context of relevant cyber capabilities, the MEngTs include the Persona, Logical, and Physical layers of cyberspace as defined by JP 3-12[34] and within FM 3-12.[35] *In simpler terms, a MEngT is comprised of the programs and pathways that the data take to move from one step to the next within the MPT.*[36] Developing MEngTs is an iterative process, increasing technical detail with each iteration. For the sake of understanding how much detail is within an MEngT, ARCYBER uses the term "Identify, Define, and Depict" to measure the amount of detail at hand. "Identify" is simply the naming convention of processes or systems requiring protection. "Define" covers the answers to the "5Ws" and captures "who" is responsible for the system (and how to contact them) and "where" the system is physically located. "Depict" covers the network map of the processes and systems requiring protection. These three levels of detail help measure progress, support prioritization decisions, support force allocation decisions, and capture technical details required by DCF to plan and execute DCO.

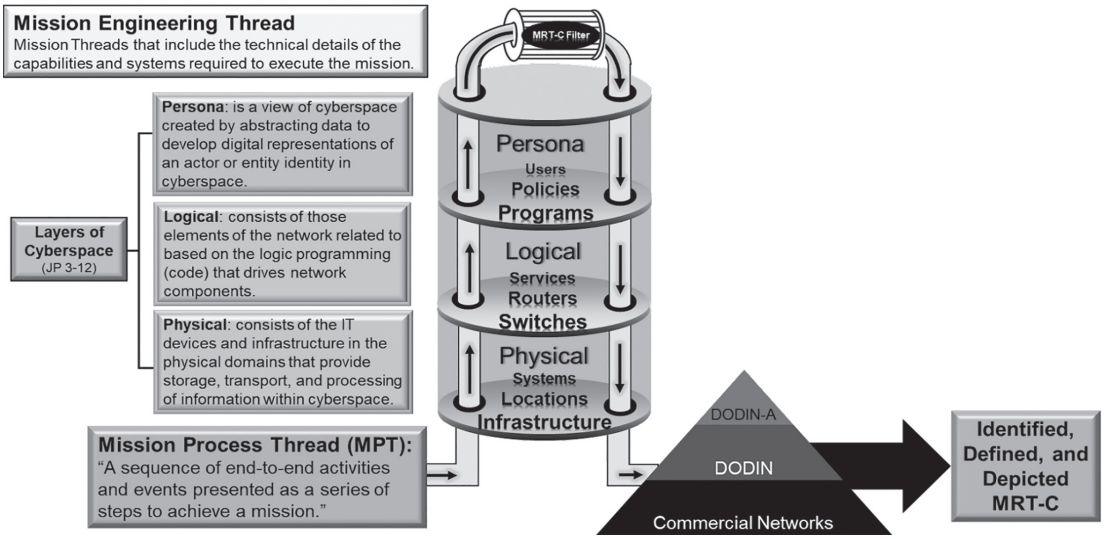


Figure 3. ARCYBER Mission Thread Analysis Framework

For the sake of Mission Thread Analysis, the first iteration of developing MEngTs should identify, in broad terms, what MRT-C[37] is required to complete a step and move to the next step within an MPT across the three layers of cyberspace (physical, logical, and Persona) and where the MRT-C resides (in terms of DoDIN-A, elsewhere on DoDIN, or within Commercial Networks). The first iteration of MEngT development also identifies the responsible organization for those programs/networks and their physical location.

Before going further, it is important to cover and reconcile the different definitions of MRT-C. Failure to reconcile these MRT-C definitions used by Defensive Cyberspace Operations and Mission Assurance has created confusion and considerable friction in the conduct of DCO over the past six years. Different from asset-focused approaches, MTA efforts focus on identifying MRT-C more broadly. The current definition of MRT-C is contained in USCYBERCOM Cyber Warfare Publication 3-0.1 – "Identification of Mission Relevant Terrain in Cyberspace (MRT-C)," 20 August 2021. It defines MRT-C as "All devices, internal/external links, operating systems, services, applications, ports, protocols, hardware, and software on servers, required to enable the function of a critical asset; may exist external to the DoD cyberspace."[38] This definition of MRT-C is in keeping with the original intent of the various series of orders that originally coined the term back in 2017 by acknowledging MRT-C can exist off-DoDIN,[39] and overcomes the friction caused by truncated versions of the MRT-C definition that have emerged since.

MRT-C Depiction

Compromises occur across all the three layers of cyberspace (Physical, Logical, and Persona). A portion of MTA is to determine what MRT-C exists before employment of any DCF and to capture information about MRT-C. Example: Where does the MRT-C reside physically, who is responsible for the MRT-C, and contract information. Determining where MRT-C resides and who is responsible for said MRT-C is critical for determining who within the federal government has the authorities for responding to threats to MRT-C.

Textbox 5

Mission Assurance professionals define MRT-C as "Cyber analysis that includes documenting devices, internal and external links, operating systems, services, applications, ports, protocols, hardware, software, and other technical aspects of a system required for the function of a critical asset."[40] The omission of "may exist external to DoD cyberspace" within the Mission Assurance definition of MRT-C leads planners to focus solely on assets owned by an organization (or only on/within DoDIN), but overlook what MRT-C exists elsewhere, specifically off-DoDIN. The unintended consequence of this omission is that units limit their Mission Assurance analysis to the MRT-C under their direct control. Such analysis comes at the expense of overlooking MRT-C that is within the commander's Area of Interest that the unit requires to accomplish its mission. This has unwittingly created a gap in understanding what processes or systems require consideration for protection and what is needed to frame that understanding in a way that allows mutual support with the interagency in a crisis.

Using different definitions of MRT-C in Mission Assurance and Defensive Cyberspace Operations results in units duplicating efforts and creates a gap between identified unit-owned MRT-C protection requirements and protection requirements for MRT-C used by a unit to accomplish its mission that reside elsewhere, whether on or off DoDIN. What follows is an attempt to reunify both efforts by providing one definition across both Mission Assurance and Defensive Cyberspace Operations. To overcome friction caused by differing definitions, we define MRT-C as, "All devices, internal/external links, operating systems, services, applications, ports, protocols, hardware, and software on services required to enable the function of a critical asset *and/or for the completion of a mission;* ***may exist external to DoD Cyberspace***." Inclusion of the emphasized portion of the definition of MRT-C accounts for both Mission Assurance and DCO requirements, enabling more effective planning and reduction of cybersecurity related

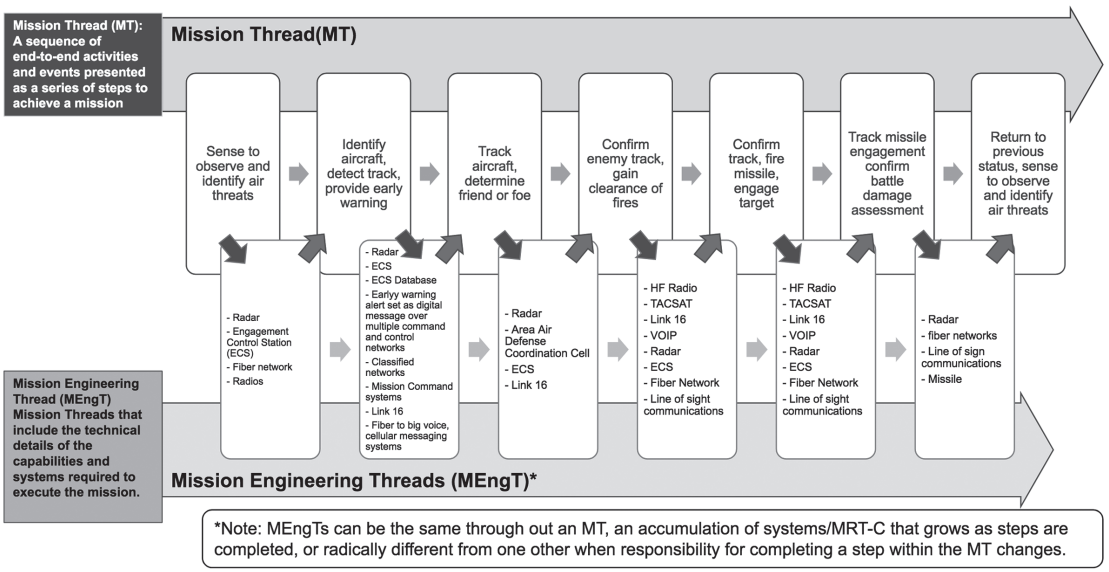


Figure 4. Visualization of Table 1 Mission Thread Analysis of Air Defense Kill Chain Engagement.[41]

risk. Following ARCYBER's back-brief on HQDA EXORD 211-22, Army senior leaders approved this definition during an Army Synchronization Meeting in October 2022 for socialization with other stakeholders and for incorporation into future doctrine and policy.

The completion of MTA triggers the initiation of Mission Thread Defense (MTD) by the Cyber Protection Brigade based on its priorities of work. MTD is the deliberate defense of MEngT (including MRT-C) to support a Mission Owner's designated MPT or critical operational missions by another name (e.g., air defense kill chain). The process identified as MPTs (e.g. detect, provide early warning, track, engage, BDA) during the MTA are those processes, that if compromised, would lead to overall mission failure (e.g. failure to destroy air threat). A successful MTA establishes priorities of work for DCF (by prioritizing excess demands against limited capacity), the details required for a successful MTD (analytics, threat, MRT-C), where (and if) IA support is required (beyond DoD authorities or access), and the identification of risk and authority of risk acceptance if the volume of requirements exceeds the capacity of USCYBERCOM and the IA.

CONCLUSION

MTA enables military organizations and private-sector companies to articulate their cybersecurity and cyberspace security needs more effectively to cyberspace security professionals across the DoD, the Interagency, and private cybersecurity partners. Using clear and concise terms in a manner designed to overcome institutional and cognitive biases enables more effective support and greater potential for optimizing limited resources. As organizations develop MPTs and MEngTs they translate their cyber protection needs across operational and technical frames of reference that can be used by ARCYBER, elsewhere within USCYBERCOM, and by the Interagency when and where appropriate. The MTA approach is also useful when the cyber protection function is performed by allies, sister service defensive cyber forces, Inter-agency partners, the private sector, or any other party – regardless of whether the protection teams are familiar with the process they are protecting. The Army's use of Mission Thread Analysis informs critical training requirements, force management decisions, and helps establish priorities of work for Cyber Mission Forces. A unit's completion of a Mission Thread Analysis helps gather technical details that support DCO execution and gives the unit an opportunity to articulate their priorities more effectively for protection. By encouraging the use of Mission Thread Analysis across the Army, ARCYBER intends to increase efficiency and optimize employment of limited resources, while addressing the different approaches by various stakeholders to counter or mitigate the efforts of Malicious Cyber Actors. These benefits will also accrue to others who implement MTA or a suitable adaptation.

DISCLAIMER

The views expressed in this work are those of the authors and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, or the Department of Defense.

NOTES

1. George W. Bush, "National Security Presidential Directive-54," and "Homeland Security Presidential Directive-23," (January 2008). Cybersecurity is defined as the "Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. More commonly, "The process of protecting information by preventing, detecting, and responding to attacks. See also NIST: https://csrc.nist.gov/glossary/term/cybersecurity.
2. Department of Defense Dictionary of Military and Associated Terms (2023): 49. Department of Defense, Joint Publication 3-12 (December 2022): II-6. Department of the Army Field Manual 3-12 (August 2021): 2-6. Note: Each of these publications define "Cyberspace Security" as: "Actions taken within protected cyberspace to prevent unauthorized access to, exploitation of, or damage to computers and networks, including platform information technology."
3. Department of Defense, "Joint Publication 3-12 Joint Cyberspace Operations" (December 2022): II-6. Note: Cyberspace Defense: actions are taken during DCO-IDM missions, within protected cyberspace, to discover and defeat specific threats that breach, threaten to breach, or are suspected to have breached the cyberspace security measures, to include actions that detect, characterize, fix, contain, clear, and recover/restore from Malicious Cyber Activity, including malware or the unauthorized activities of authorized users.
4. Department of Defense, "Joint Publication 3-12 Joint Cyberspace Operations," (December 2022): II-4. Note: Cyber Protection Forces conduct "Defensive Cyberspace Operations," or "DCO missions," to defend blue cyberspace from imminent or active threats in cyberspace. Specifically, DCO missions preserve the ability to utilize blue cyberspace capabilities and protect data, networks, cyberspace-enabled devices, and other designated systems by defeating ongoing or imminent malicious cyber activities.
5. Donald Firesmith, "Mission thread Analysis Using End-to-End Data Flows – Part I," SEI Blog, Software Engineering Institute, Carnegie Mellon University. https://insights.sei.cmu.edu/blog/mission-thread-analysis-using-end-to-end-data-flows-part-1/
6. ARCYBER lessons learned in operational archives 2015-2022, from named, classified operations: UTMOST GOLF (Logistics), UTMOST CHESS (Power Projection), ROMAN GUARDIAN (Mission Partner Environment), UTMOST SASQUATCH (Critical Production Lines). Authors' note: The classified reports associated with each of these operations (and others) are not available publicly. Where appropriate and necessary, the authors can provide real-world examples based on clearance and need-to-know.
7. Department of the Army, "Field Manual 3-90 Tactics" (May 2023): 6-7.
8. Department of the Army, "Field Manual 3-12 Cyberspace Operations and Electromagnetic Warfare," (August 2021): 2-7.
9. Department of Defense, "Joint Publication 3-12 Joint Cyberspace Operations," (December 2022): II-7
10. Mark Esper, "Definition of 'Department of Defense Cyberspace Operations Forces (DoD COF)'" (official memorandum, Washington, DC, Department of Defense) 2019. NOTE: The term Defensive Cyber Forces (DCF) captures Cybersecurity Service Providers (CSSPs), Cyber Protection Teams (CPTs), CPT Mission Elements, USAF Mission Defense Teams (MDTs), and other forces whose primary functions are to protect or defend Department of Defense Information Networks. Commonly used terminology within USCYBERCOM and Cyber Mission Forces, but not included in the Department of Defense Dictionary of Military and Associated Terms.
11. ARCYBER Lessons Learned in Operational Archives 2015-2022, from named, classified operations: UTMOST GOLF (Logistics), UTMOST CHESS (Power Projection), ROMAN GUARDIAN (Mission Partner Environment), UTMOST SASQUATCH (Critical Production Lines).
12. United States Congress, National Defense Authorization Acts 2015-2024, Congress.gov | Library of Congress: FY2024 HR 2670 (PUBLIC LAW 118-31—DEC. 22, 2023), Sections 1511, 1512, 1517, and 1553; FY2023 HR 7776 (PUBLIC LAW 117–263—DEC. 23, 2022), Sections 1504, 1509,1510, 1511, 1559, 1636, and 1656; FY2022 S 1605 (PUBLIC LAW 117–81—DEC. 27, 2021), Sections 1505, 1525, 1542, and 1543; FY2021 HR 6395 (PUBLIC LAW 116–283—JAN. 1, 2021), Sections 1721, 1724, and 1736; FY2020 S1790 (PUBLIC LAW 116–92—DEC. 20, 2019), Sections 1638, 1660, and 6504; FY2019 HR 5515 (PUBLIC LAW 115–232—AUG. 13, 2018), Sections 1642, 1647, 1648 and 1650; FY2018 HR 2810 (PUBLIC LAW 115–91—DEC. 12, 2017), Sections, 1638, 1643, and 1651; FY2017 S 2943 (PUBLIC LAW 114–328—DEC. 23, 2016), Sections 1645 and 1650; FY2016 S1356 (PUBLIC LAW 114–92—NOV. 25, 2015), Section 1647; FY2015 HR 3979 (PUBLIC LAW 113–291—DEC. 19, 2014), Sections 1632 and 1634. Each of these National Defense Authorization Acts directed United States Cyber Command and the military services to conduct a variety of cyber security related assessments and defensive cyber operations activities that the Army and USCYBERCOM routinely assign to ARCYBER for execution by Defensive Cyber Forces, specifically Cyber Protection Teams, their analytic support elements, and network operators.

NOTES

13. Dina Temple-Raston, "A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack," National Public Radio. https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack
14. Department of the Army, "HQDA EXORD 211-22 Army Support to Defensive Cyberspace," (Jun 2022): 6. A classified document outlining the process to optimize Defensive Cyber Operations and assess risks to the force.
15. George Corbari, Paul Stanton, and John Popiak, "ARCYBER Confirmation Briefing" provided to Army Synchronization Meeting September 2022 and multiple follow-on Army Senior Leader briefings to the Secretary of the Army, Army Chief of Staff, Army Principal Cyber Advisor, and Army Chief Information Officer between October 2022 and October 2023.
16. Michael Gagliardi, William Wood, Timothy Morrow, "Introduction to the Mission Thread Workshop," Software Engineering Institute, Carnegie Mellon University. https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=63148
17. Donald Firesmith, "Mission thread Analysis Using End-to-End Data Flows – Part I," SEI Blog, Software Engineering Institute, Carnegie Mellon University. https://insights.sei.cmu.edu/blog/mission-thread-analysis-using-end-to-end-data-flows-part-1/.
18. ARCYBER Lessons Learned in Operational Archives 2015-2022, from named, classified operations: UTMOST GOLF (Logistics), UTMOST CHESS (Power Projection), ROMAN GUARDIAN (Mission Partner Environment), UTMOST SASQUATCH (Critical Production Lines). Authors' note: The classified reports associated with each of these operations (and others) are not available publicly. Where appropriate and necessary, the authors can provide real-world examples based on clearance and need-to-know.
19. Department of Defense, "The DoD Mission Engineering Guide," (NOV 2020): 38. Note: The guide defines a Mission Thread as, "A sequence of end-to-end activities and events presented as a series of steps to achieve a mission."
20. Department of Defense, "The DoD Mission Engineering Guide," (NOV 2020): 38. Note: The guide defines a Mission Thread as, "A sequence of end-to-end activities and events presented as a series of steps to achieve a mission."
21. US Army Cyber Command, Internal Lessons Learned from After Action Reports from deliberate, named Defensive Cyberspace Operations (2014-present). ARCYBER lessons learned including classified operations: UTMOST GOLF (Logistics), UTMOST CHESS (Power Projection), ROMAN GUARDIAN (Mission Partner Environment), UTMOST SASQUATCH (Critical Production Lines). These specific operations enabled ARCYBER planners to identify gaps and apply lessons learned in the development and validation of the concepts Mission Process Thread and Mission Thread Analysis.
22. Department of Defense, "The DoD Mission Engineering Guide," (NOV 2020): 14-19. Note: Authors adapted Figures 2-5 and 2-9 (pages 14 and 19) when creating these proposals.
23. Department of Defense, "The DoD Mission Engineering Guide," (NOV 2020): 37. Note: Defines Mission Engineering Threads as "Mission threads that include the technical details of the capabilities and systems required to execute the mission."
24. Department of Defense, "The DoD Mission Engineering Guide," (NOV 2020): 37. Note: The authors use MEngT as an acronym to prevent confusion with Mission Essential Task and its acronym "MET."
25. Department of Defense, "The DoD Mission Engineering Guide," (NOV 2020): 37. Note: Defines Mission Engineering threads as "Mission threads that include the technical details of the capabilities and systems required to execute the mission."
26. US Army Cyber Command, Internal Lessons Learned from After Action Reports from deliberate, named Defensive Cyberspace Operations (2014-present). ARCYBER lessons learned including classified operations: UTMOST GOLF (Logistics), UTMOST CHESS (Power Projection), ROMAN GUARDIAN (Mission Partner Environment), UTMOST SASQUATCH (Critical Production Lines). These specific operations enabled ARCYBER planners to identify gaps and apply lessons learned in the development and validation of the concepts Mission Process Thread and Mission Thread Analysis.
27. United States Cyber Command, "(U) CFMAP Info Paper – DCO Requirements," (8 June 2022): 2-4. Authors Note: "Defense Requirements Statement" is an ARCYBER an attempt to translate the information requested by USCYBERCOM into a sentence for easier development of DCO needs and leader understanding of the requirement. Example: (fill in the blank) I*n support of [Plan] and [Sector] to perform [Objective/Effect], assist [Terrain Owner] within [DoDIN AO] by performing CPT functions upon [System/MRT-C] in order to protect [JMET/Mission] from [Threat].*
28. United States Cyber Command, "(U) Relationship between the Cyberspace Forces Mission Alignment Process (CFMAP) and the Global Force Management Allocation Plan," 5 March 2021: 1. NOTE: Cyber Force Mission Allocation Process (CFMAP) is a bi-annual USCYBERCOM process of assessing CCMD and Service requirements in cyberspace and, if or when necessary, recommends to the Secretary of Defense, the adjustment or re-allocation of capacity and missions of Cyber Mission Force.

NOTES

29. United States Cyber Command, "Cyber Warfare Publication 3-0.1 – Identification of Mission Relevant Terrain in Cyberspace (MRT-C)," (August 2021): GL-3.
30. Mark Esper, "Definition of 'Department of Defense Cyberspace Operations Forces (DoD COF)'" (official memorandum, Washington, DC, Department of Defense) 2019. NOTE: The term Defensive Cyber Forces (DCF) captures Cybersecurity Service Providers (CSSPs), Cyber Protection Teams (CPTs), CPT Mission Elements, USAF Mission Defense Teams (MDTs), and other forces whose primary functions are to protect or defend Department of Defense Information Networks. Commonly used terminology within USCYBERCOM and Cyber Mission Forces, but not included in the Department of Defense Dictionary of Military and Associated Terms.
31. US Army Cyber Command, Internal Lessons Learned from After Action Reports from deliberate, named Defensive Cyberspace Operations (2014-present). ARCYBER lessons learned including classified operations: UTMOST GOLF (Logistics), UTMOST CHESS (Power Projection), ROMAN GUARDIAN (Mission Partner Environment), UTMOST SASQUATCH (Critical Production Lines). These specific operations enabled ARCYBER planners to identify gaps and apply lessons learned in the development and validation of the concepts Mission Process Thread and Mission Thread Analysis.
32. Sydney Freedberg, "Army's New Aim is Decision Dominance," Breaking Defense, https://breakingdefense.com/2021/03/armys-new-aim-is-decision-dominance/. Note: Reports the ongoing work of the Combined Arms Center, Fort Leavenworth, ARCYBER and others; based on Army Senior Leader statements and guidance supporting the establishment of "Information Advantage Detachments" and "Information Advantage Task Forces. See also "Army Doctrinal Publication 3-13, Information," (November 27, 2023): 1-1 – 1-12.
33. Paul Son (US Army) and Michelle Paul (IT Cadre), "ARCYBER Data Rationalization Current State Visualization Report," (December 8, 2023): 1-5. NOTE: This report is classified as *Controlled Unclassified Information* and as such not publicly released.
34. Department of Defense, "Joint Publication 3-12 Joint Cyberspace Operations," (December 2022): I-2 – I-4.
35. Department of the Army, "Field Manual 3-12 Cyberspace Operations and Electromagnetic Warfare," (August 2021): 1-5.
36. Department of Defense, "The DoD Mission Engineering Guide," (NOV 2020): 37
37. United States Cyber Command, "Cyber Warfare Publication 3-0.1 – Identification of Mission Relevant Terrain in Cyberspace (MRT-C)," (August 2021): GL-3.
38. United States Cyber Command, "Cyber Warfare Publication 3-0.1 – Identification of Mission Relevant Terrain in Cyberspace (MRT-C)," (August 2021): GL-3.
39. Chairman of the Joint Chiefs of Staff PLANORD, "Identification of Mission Relevant Cyberspace Terrain Supporting Critical Assets," (18 April 2017); United States Strategic Command, "USSTRATCOM PLANORD 17-05, Identification of Mission Relevant Cyberspace Terrain Supporting Critical Assets, (17 May 2017); United States Cyber Command. "USCYBERCOM OPORD 17-0106, Identification of and Mapping of Mission Relevant Cyber Terrain Supporting Critical Assets," (29 July 2017).
40. Department of Defense Instruction (DoDI), "DoDI 3020.45, Mission Assurance Construct," (August 2018), Change 1, May 2, 2022: 72.
41. ARCYBER lessons learned in operational archives 2015-2022, from named, classified operations: UTMOST GOLF (Logistics), UTMOST CHESS (Power Projection), ROMAN GUARDIAN (Mission Partner Environment), UTMOST SASQUATCH (Critical Production Lines). Authors' note: Providing an accurate or real-world example of a complete Mission Thread Analysis would increase the classification of this article. To facilitate the widest possible dissemination of this document, the authors created an example to illustrate what an MTA might look like based on lessons learned from actual operations. By design, some details were left out to reduce potential targeting or threats to industry or systems within the example. Where appropriate and necessary, the authors can provide real-world examples based on clearance and need-to-know.