Battlefield Development Plans: Threat Analysis Enabling Multi-Domain Operations

by Mr. Earl S. Bittner

Introduction

During this next decade, each of the U.S. Military Services will transition to the new multi-domain operations (MDO) joint warfighting doctrine. The genesis for this new doctrine arose as adversaries, who studied U.S. warfighting doctrine and its applications closely for the past 20 to 30 years, developed concepts and capabilities designed to undermine our strengths and seize upon our weaknesses. In response, the Army and joint forces examined these new threats and developed MDO as a counter. Just as intelligence drives operations, these new threats drove the development of MDO—a divergence from previous capabilities-based doctrines. The sophistication of the threats' capabilities and warfighting concepts meant we had to use a variety of analytical methods to derive the knowledge necessary to defeat adversaries. Understanding how the Army and joint force acquired this knowledge remains important for intelligence professionals because as the threat evolves, the Army must continue this analysis so that we maintain our ability to defeat these adversaries.

Background

During the counterinsurgency wars from 2001 to 2015, the U.S. Army and joint forces became adept at targeting personnel and terror/insurgent organizations. However, as our military reoriented from predominantly counterinsurgency operations to that of large-scale combat operations, it became clear that adversaries had made advances that necessitated a change in how we evaluated threats. This fact became even more evident in the 2016 *Russian New Generation Warfare Study,* for which the U.S. Army performed an in-depth analysis of this new threat.[1] To do the study, the Army referred back to the 1970s and 1980s when it used the battlefield development plan to visualize how the Army would fight the Soviets in particular scenarios.[2] We then combined guidance from the National Defense Strategy, assessments about the future operational environment, and information concerning the new near-peer great power competition to modernize the battlefield development plan and used it to support MDO.[3] In developing the new battlefield development plan, we discovered the force could no longer just identify the threat's centers of gravity and high-payoff targets and then strike them with overwhelming force from a relative sanctuary. The threat now protected their centers of gravity with redundant, integrated, highly capable systems that made their destruction difficult. They also improved their capability to neutralize our fires capabilities (air and ground) that we use to attack their centers of gravity. Furthermore, threats had developed new capabilities and concepts that enabled them to contest us across the length of the battlefield, in all domains and phases, in layered, networked systems with near-real-time responses. This meant we could no longer analyze one system and figure out how to attack and destroy it as we traditionally had done in the past. We now had to understand much more complex systems of systems (also known as complexes) with which we had limited practical experience.

Battlefield Development Plan Books

Book 1: Red Forces

Book 2: Blue Capabilities

Book 3: MDO Options "Blue vs Red"

Our Analytical Approach

To comprehend these new threats, we had to examine how they operated in all domains, how the new systems functioned, and how they were nested. We also had to gain an understanding of how the threats' networks operated and how redundancies were built into these networks. Another challenge was comprehending how our adversaries were using a whole-of-nation approach to war beginning in the competition phase. Further exacerbating these difficulties was the new level and sophistication that information operations brought to warfare. These are just some of the challenges posed by our adversaries that the Army and joint forces studied, and continues to study, and why we needed to analyze the threat using additional and new methods.[4]

We used analytical methods described in ATP 2-33.4, *Intelligence Analysis,* to analyze the problem set. However, given the complex nature of the threat, we had to build upon, modify, and combine analytical methods to achieve the threat comprehension required for the battlefield development plan.

We call the method we used to perform this activity *threat systems analysis*. It combines nodal/network; systems; criticality, accessibility, recuperability, vulnerability, effect, and recognizability (also called CARVER); and kill chain analytic methods with operational environment data across all domains and warfighting echelons to achieve an understanding of the threat's capabilities and vulnerabilities, and potential means for mitigation and exploitation, respectively. The method first involves understanding the system(s) and then applies that understanding to the specific operational environment.

The Concept

Since many of the emerging threats base their means of warfighting on systems warfare, our analysis began with gaining an understanding of the individual combat systems. These individual systems are normally integrated; therefore, we also viewed these systems as networks. Given the Army's recent experience and expertise in dissecting insurgent and terrorist networks, it was natural to apply counterinsurgency network analysis to this process. As in counterinsurgency network analysis, we identified nodes in the systems and networks, gained an understanding of the relationship between the nodes, and then sought to identify the strengths and weaknesses within the system and network. However, the increased complexity of systems networks over insurgent networks meant additional collection and analysis were required. With the built-in redundancies and nesting of these systems into systems of systems (or complexes), simply neutralizing select nodes would be insufficient.

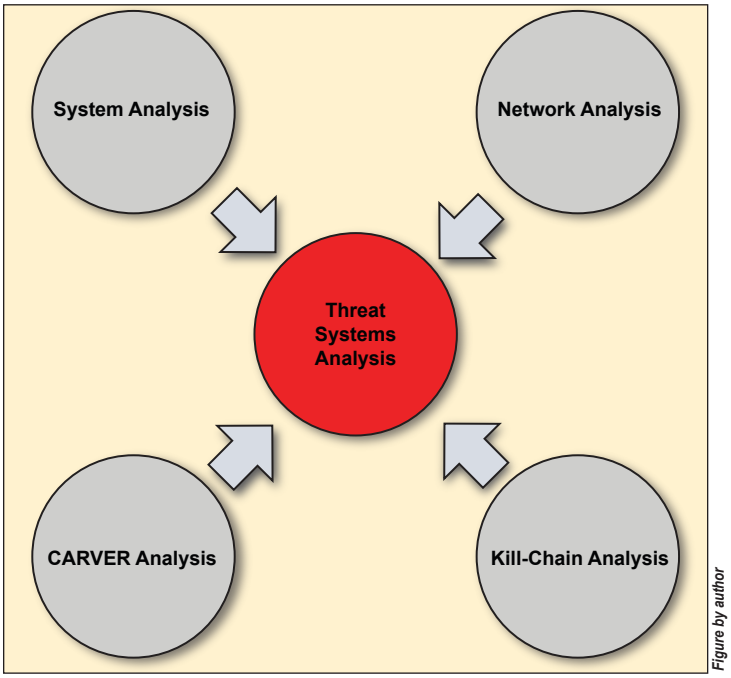
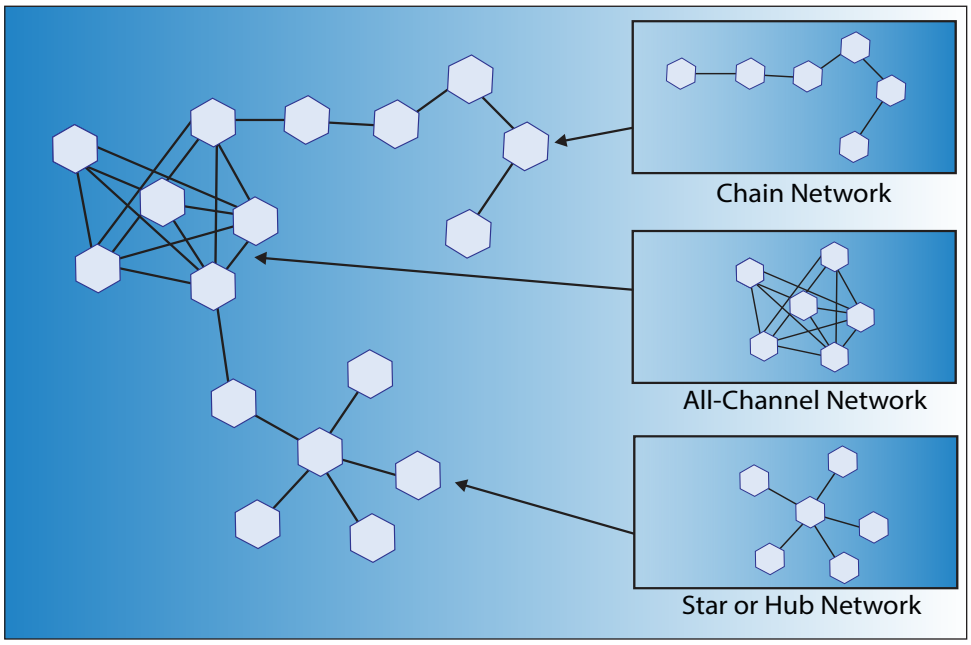


Figure by author

Threat Systems Analysis

Next, we had to understand the process by which the systems performed their missions—the kill chain. We examined how systems went through the process from target detection, to engagement, to end of mission. This effort typically involved drawing more and more systems into the study. For instance, to understand the kill chain process of a multiple rocket launcher means you also need to understand how the unmanned aerial vehicle performs target acquisition, the communications system passes the data, the fire direction performs the fire mission calculations, and the command and control system makes a decision. Each one of these systems involved in the multiple rocket launcher's kill chain has its own respective kill chain or information processes that needed to be examined to identify the best node or high-payoff target to neutralize. As part of this analysis of systems/complexes, it usually was not enough to simply strike one node; it was necessary to strike selected targets in a particular order. This is similar to how targets would be struck in counterinsurgency to achieve the greatest effect. Some targets must be struck simultaneously, others sequentially, and still others with a combination of both. In each step of the process, we looked for opportunities to disrupt the system's kill chain processes and identified strengths to circumvent.



Networked Organization and Structure Analysis[5]

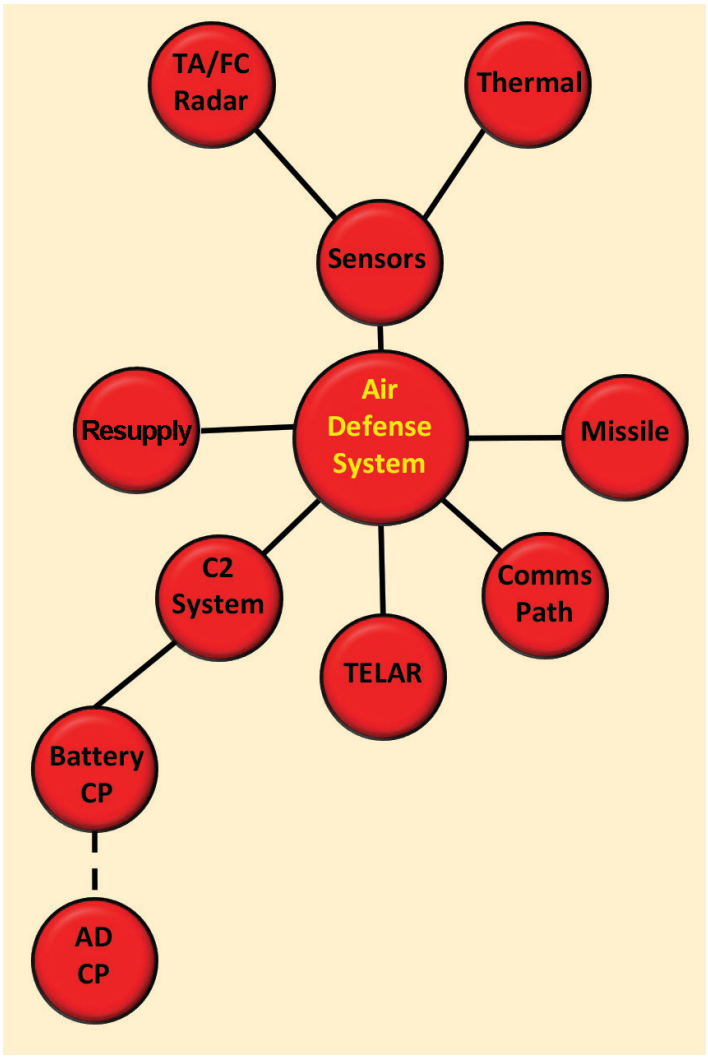


Figure by author

Threat System Nodal Analysis Example

Within this context, we next examined how each of these system complexes operated within the larger battlefield framework at the tactical, operational, and strategic levels. We identified the threat's means of integrating the force, and contingencies should their primary means be disrupted or neutralized. Once we gained a strong understanding of the threat's systems, networks, and processes, we identified potential areas in which the force could affect the threat.

At this point, the process of analyzing the threat became interactive between operational and intelligence personnel. The operational analysts—experts on the future force and capabilities—identified the means to exploit the vulnerabilities, while the intelligence analysts helped refine the best manner of exploitation. In some cases, the operational personnel developed entirely new capabilities and tactics, techniques, and procedures (TTPs), thereby creating vulnerabilities in threat systems not previously identified. Of course, as the threat continues to evolve, so too will the means to address the threat and the need to reexamine the threat.

Resources Used

In performing the analysis, we contacted a large number of organizations to fuse together each organization's expertise. A key starting point for the analysis was the joint country force assessments, which are the Defense Intelligence Agency's estimates of select countries' military forces projected into specific timeframes. This estimate aggregates Department of Defense intelligence organizations' assessments of force structure, capabilities, and disposition of forces over the specific time period. Next, to gain an in-depth understanding of systems, we consulted each Service's intelligence organizations, augmented by other national agencies as needed, to fully understand how a particular threat system operated.

Threat analysts supporting capability development are charged with basing their estimates on the current operational environment and projecting them into the future. Therefore, building off our understanding of current systems, we consulted combatant commands, current threat Army techniques publications, U.S. Army Training and Doctrine Command G-2's Foreign Military Studies Office, think tanks, other organizations with specialized subject matter expertise, and lessons learned from current operations to determine the threat's kill chains and TTPs. We then projected them into the future.

Once we gained as much understanding of the threat systems we could attain, we dissected the components, networks, and nesting of systems to determine the strengths and weaknesses. To perform this examination, we consulted Services' and combatant commands' CARVER target analysis[6] of the projected threat in order to determine prioritization and effectiveness of each target node. As stated earlier, as the threat suffers losses, it will employ contingencies that will have second order effects that can then change CARVER calculations and therefore next targeting plans. It is also in this stage that we had to deeply consider the operational environment. Even if the threat

Kill Chain*

- Indicators and Warnings Intelligence
- Target Detection
- Target Acquisition and Tracking
- Target Assignment
- Target Engagement
- Assess and Re-attack

*Modified as needed to fit the system

TARGET SYSTEMS	Criticality	Accessibility	Recuperability	Vulnerability	Effect	Recognizibility	Total
Bulk Electric Power	5	3	3	5	5	5	26*
Bulk Petroleum	5	3	5	4	3	5	25*
Water Supply	3	5	3	5	5	3	24*
Communications Systems	3	4	5	2	2	2	18
Air Transport	1	1	3	1	2	2	10
Ports and Waterways	1	1	3	1	1	1	8
Rail Transport	2	4	4	1	4	3	18
Road Networks	1	5	3	5	2	5	21
*Indicates target systems suitable for attack. In this example, the Bulk Electric Power target system has been selected.							

Strategic CARVER Matrix Application Example[7]

remained the same, a change in the operational area might necessitate a completely different targeting approach.

Next, we described this new threat to the operational and combat development force to examine how current systems could be used to exploit potential vulnerabilities. Where possible, the operational force applied and modified current capabilities to exploit future threat vulnerabilities. In some cases, this amounted to changing TTPs, and in other cases, it involved networking existing systems differently. For particularly vexing problem sets, it required the capability developers to develop new systems that could take advantage of the system(s) weaknesses.

At this point, the Army performed a series of Army and joint tabletop exercises and experiments to determine whether particular operational capabilities and TTPs would have the desired effects against targeted threat systems. The Army, and other Services, then refined capabilities and TTPs based on lessons learned from these events to best determine the way ahead. This evolution continues as the Services, warfighting functional proponents, and joint force continue to experiment and refine capabilities.

The Future

The process described serves as a baseline analytical method for the battlefield development plans used to support MDO concept and capabilities development and is not intended to be an end-all, be-all solution, but rather a starting point. As mentioned earlier, when the operational environment changes, other approaches to neutralizing the threat may become more suitable—another reason for the continuous process and addition of analytical methodologies.

Systems that must be explored more fully as the future looms are the non-kinetic systems. These systems are the most challenging to replicate, model, and analyze. Some of this difficulty is due to the sophistication of systems in various operational environments, some is due to our lack of information concerning both threat and friendly systems, and some is due to classifications of information. Fortunately, this problem works both ways and is more vexing for potential threats because their understanding of the full effects of non-kinetic weapons is almost certainly much less complete.

Another area requiring greater focus is competition. While the U.S. industrial-defense complex has spent many decades and trillions of dollars studying threats and developing weapons for combat, in comparison, an infinitesimal amount has been applied to analysis, activities, and systems for the competition phase. Since much of our success in MDO is contingent on activities performed during competition, it is important for the intelligence community to study competition and better learn how we may influence events that will affect activities in conflict. This will likely require the incorporation or creation of additional analytic methods.

A more effective and efficient means to perform experimentation and tests will help advance our analytics. Currently, in order to run an experiment to validate capabilities and concepts, one often needs months of preparation and thousands of man-hours to simply test various elements on new concepts and doctrine. This means there is significant lag time between performing our analysis and testing whether our analytical conclusions were valid. On the other hand, when we used less sophisticated means of

experimentation, it is often oversimplified and can lead to incorrect conclusions. Advances in modeling and simulation will enhance our ability to analyze and more rapidly learn.

As the Army, other Services, and joint force continue to gain a better understanding of the threats systems, the threat is doing the same. Therefore, as part of this feedback loop, the intelligence community continues to refine data as the threat's capabilities change and are refined. Ultimately, this threat systems analysis is a living process, and it will aggregate analytical methods into the process in order to solve new problems brought about by the evolving threats.

Endnotes

1. Department of the Army, *Russian New Generation Warfare: Unclassified Summary of the U.S. Army Training and Doctrine Command Russian New Generation Warfare Study* (Fort Eustis, VA: Training and Doctrine Command, n.d.), https://www.armyupress.army.mil/Portals/7/online-publications/documents/RNGW-Unclassified-Summary-Report.pdf?ver=2020-03-25-122734-383.

2. Eric J. Wesley and Jon Bates, "To Change an Army—Winning Tomorrow," *Military Review* 100, no. 3 (May–June 2020): 6-17, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2020/Wesley-Winning-Tomorrow/.

3. Eric J. Wesley and Robert H. Simpson, *Land Warfare Paper 131, Expanding the Battlefield: An Important Fundamental of Multi-Domain Operations* (Arlington, VA: The Association of the United States Army, April 2020), https://www.ausa.org/sites/default/files/publications/LWP-131-Expanding-the-Battlefield-An-Important-Fundamental-of-Multi-Domain-Operations.pdf.

4. Department of the Army, *The Battlefield Development Plan: Field Army, Corps, and Division in MDO 2028* (Army Futures Command, June 2020).

5. Figure is adapted from Figure IV-4, Network Structure, Office of the Chairman of the Joint Chiefs of Staff, Joint Publication 3-25, *Countering Threat Networks* (Washington, DC: The Joint Staff, 21 December 2016), IV-11.

6. Christopher M. Schnaubelt, Eric V. Larson, and Matthew E. Boyer, *Vulnerability Assessment Method Pocket Guide: A Tool for Center of Gravity Analysis* (Santa Monica, CA: RAND, 2014), https://www.rand.org/content/dam/rand/pubs/tools/TL100/TL129/RAND_TL129.pdf.

7. Department of the Army, Army Techniques Publication 3-05.20, *Special Operations Intelligence* (Washington, DC: U.S. Government Publishing Office, 3 May 2013), 2-11 (common access card login required).

Mr. Earl Bittner is an intelligence specialist assigned to the U.S. Army Training and Doctrine Command G-2 Operational Environment Integration Directorate and threat author for the Russian Battlefield Development Plan. He is a retired U.S. Army intelligence officer with 22 years of service, multiple deployments, and experience in a variety of analytical assignments.