Cyberspace Operations

How cyber ops fit within the Marine Corps Planning Process

by Maj Arun Shankar

>Maj Shankar is the MAGTF Plans Officer, MAGTF Staff Training Program in Quantico, VA. He has served a combined 28 months in Operation Iraqi Freedom/Operation Enduring Freedom as a counter-improvised explosive device analyst, assessments analyst, and communications officer. He holds a PhD in Operations Analysis, George Mason University, Fairfax, VA.

The recent explosion of networked devices and computer technology throughout society has provided the fuel for a new emphasis on a concept called "cyberspace operations" within the Department of Defense (DOD). Cyberspace operations are actions conducted within the computer network world known as cyberspace with the goal of achieving a particular objective.[1] The effects of military actions in this unfamiliar domain can have far-reaching consequences that extend beyond geographic boundaries. The execution of such an operation requires careful, methodical, and integrated planning steps prior to execution. Conveniently, the Marine Corps already has a process—the Marine Corps Planning Process (MCPP)—with the necessary structure to achieve these planning goals. The proper input of cyberspace operations throughout the MCPP can result in the optimal integration of warfighting capabilities that best achieve the mission. The purpose of this article is to define this input in each of the six steps of the MCPP.

Background

Cyberspace is simply a set of networks, nodes, configurations, and users. It includes hardware, software, rules, resources, and people. It is one of the five interdependent warfighting domains. The remaining four are the physical domains of air, land, sea, and space. Cyberspace operations encompass three specific missions. These are offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), and DOD Information Network (DOD IN) operations. OCO is focused on power projection against the adversary; DCO is focused on defending the friendly network; and DOD IN operations involve operating and maintaining DOD networks.[2]

The MCPP is the formal process that staffs within the Marine Corps use to plan operations. It contains the essential elements to formulate a desired course of action and distribute it in a way that subordinates can understand and execute effectively. If a cyberspace operation is used to support a MAGTF operation, its effective incorporation within the MCPP is essential. Within a MAGTF, cyberspace operations will most likely emerge as a supporting function to a greater mission rather than a main effort in and of itself. Consequently, cyberspace operations will appear as a concept of support within the steps of the MCPP when planning a MAGTF operation.

The MCPP is the formal process that staffs within the Marine Corps use to plan operations.

There are six steps within the MCPP. The first step, problem framing, exists to gain an understanding of the problem and develop a mission statement. The next step, course of action (COA) development, results in options for the commander to accomplish the mission. The third step, COA wargaming, is essentially meant to improve each of the COAs and determine gaps, shortfalls, or missing links that were not identified earlier. The next step, COA comparison and decision, leads to an evaluation of each COA against predetermined criteria and an informed choice by the commander. Once the COA is chosen, the order is drafted in the fifth step and transitioned to execution in the final step.[3]

Problem Framing

The main goal of problem framing is to gain an understanding of the problem; therefore, a comprehension of the cyberspace environment should be comprised within this. This includes a grasp of the physical and logical network structure as well as its users. The complexities of cyberspace extend this analysis beyond continuous battlespace in its conventional sense. Instead, the focus is placed on portions of a worldwide network that affect both enemy and friendly forces. An appreciation for how the enemy might use his capabilities within cyberspace to achieve his goals or hinder friendly actions is essential. Depending on available information, the fidelity of this information

could range from historical intelligence reports about enemy computer and website usage to a detailed map of both the physical and logical topology within the enemy's cyber area of influence. Such a map could include not only computer terminals and internet cafes, but also satellite transmission towers, cellular phone towers, and wired closed networks.[4]

Cyberspace operations can also play a role in both enemy and friendly center of gravity (CoG) analysis developed during problem framing. An ability to conduct cyberspace operations could emerge as a critical capability during CoG analysis. It could also present itself as a critical vulnerability. In some cases, it may be the CoG itself. It may even impact the characterization of the various critical elements within CoG analysis. For example, an enemy unit with a highly capable cyberspace attack capability might promote that unit to the enemy's CoG. Though CoG analysis is often a contentious exercise within an operational planning team (OPT), the use of a structured model to conduct the analysis will greatly assist in discovering a CoG with adequate rigor and agreement among staff members. The analysis will increase the collective understanding of both enemy and friendly capabilities and orient the staff toward a common objective.

Task analysis within problem framing is the itemization of specified and implied tasks to determine essential tasks and an eventual mission statement. In the context of MAGTF operations, cyberspace operations are not likely to surface as essential tasks, but they will appear as implied and specified tasks. Many believe that the purpose of task analysis is only to develop the mission statement from the essential tasks, but it is actually the steps of task analysis that assist in the collective understanding of the problem that truly achieve the purpose. Ensuring that OCO, DCO, and DOD IN operations are included in the analysis will improve the staff's comprehension of how cyberspace operations can support the main effort.

The development of assumptions is another integral output of problem framing. Key assumptions about friendly and enemy uses of cyberspace operations are crucial to the continuation of planning in the absence of validated requests for information. For instance, it may be necessary to assume that the enemy's use of cyberspace is his primary mode of communications to coordinate ground attacks against friendly forces. It may also be required to assume the effects of an enemy cyberspace attack against friendly networks in various phases on an operation. Even more vital are the limitations (constraints and restraints) placed on the friendly force. One key limitation in the realm of cyberspace operations is the capability of a local commander to execute a given cyberspace operation. In many cases, commanders may not possess the equipment or personnel to do so and will require assistance from supporting commands.

Cyberspace readiness must be tested during training exercises. *(Photo by MCS3 Declan Barnes.)*

Commander's critical information requirements (CCIR) are events that prompt a commander to make a decision, and a proposed list is created during problem framing. Ensuring that cyberspace operations are considered within this list of CCIRs is essential. Indications and warnings of a cyberspace attack are an obvious choice, but events within DOD IN operations may also fit this category. In that regard, a typical communications service outage may also be a CCIR.

Course of Action Development

After problem framing, COA development presents its own opportunities for the integration of cyberspace operations. Once the outline of a maneuver COA is developed, a concept of support is required from each support staff section within the command. In this setting, cyberspace operations support would be included. Similar to logistics, fires, and intelligence, a cyberspace operations concept of support defines how such operations would enable the main effort.

Cyberspace operations should not only limit support to aviation and ground combat units. A logistics convoy could register a requirement for increased cyber security measures during a vulnerable attack sequence. Perhaps an increased friendly cyber defensive posture would be executed during the phase of an operation where a friendly command post's network is more vulnerable to a cyberspace attack. Cyberspace operations also include DOD IN operations, so the details about the phased installation, management, and operation of the MAGTF communications architecture may also be developed during this portion of the MCPP.

The synchronization matrix is one of the outputs of the COA development step. This matrix outlines the key activities of units within the MAGTF over a

time scale. These might include when the main effort will cross the line of departure, or when to expect a supporting effort to land at a specified beach. Cyberspace operations can also be outlined within this matrix just as many other supporting functions. DCO, OCO, and DOD IN operations that are key events within the overall operation should be specified within this matrix so that the activities can be synchronized for the conduct of the wargame.

COA Wargaming

COA wargaming exists to make the plan better.[5] In this step, the friendly actions of each COA are wargamed against anticipated adversary COAs. The results are studied to understand these interactions and identify gaps in the plan. They eventually form the basis for the commander's COA comparison and decision. The cyberspace operations events identified in the synchronization matrix for each COA should be examined during COA wargaming. It should be evident that each cyberspace operation is placed in the correct sequence to support the overall MAGTF concept of operations. The wargaming step should also highlight resource shortfalls or risks related to cyberspace operations. This includes shortages of people or equipment as well as risks to the mission caused by weather, terrain, or the adversary. As these considerations are identified, the overall concept of cyberspace operations support should be refined to improve each COA.

COA Comparison and Decision

Once each COA is wargamed, the commander compares each COA and chooses one to proceed with planning. The comparison is based on evaluation criteria provided by the commander. The comparison can be qualitative, quantitative, or a combination of both. The criteria might include friendly casualties, tempo, simplicity, or how well the MAGTF shapes the battlespace. Cyberspace operations that support (or hinder) these criteria should be highlighted in the comparison for the commander to better understand the circumstances. For instance, the use of a cyberspace operation in support of a maneuver unit could prove to decrease friendly casualties during wargaming. Conversely, maybe the lengthy process for the execution of a cyberspace operation resulted in a loss of tempo. The commander is likely to make the best choice when he is most informed of the critical circumstances surrounding the employment of each COA.

Orders Development

Once the COA is chosen, the operations order is developed. It is composed of a base order and a series of associated annexes. The order is written with the intent of communicating the plan effectively to subordinate leaders. Cyberspace operations that are part of the plan should be portrayed in a detailed fashion within this operation order. Typically, DOD IN operations and DCO are detailed in Annex K (Communications), while OCO is found within Appendix 19 of Annex C (Operations) along with information operations and MAGTF fires. Annexes R (Spare) and Y (Spare) are extra sections that can also be used for various elements of cyberspace operations. Regardless, the chief of staff or the executive officer is the authority on how the operation order should be organized, so his direction will determine where cyberspace operations are specified within the operation order.

COA wargaming exists to make the plan better.

Transition

Once the order is signed and written, it should be transitioned to the current operations cell and the subordinate units. A key element of transition is the assurance that the order is understood by those executing it. This can be accomplished through various types of transition briefs, including rehearsals, face-to-face meetings, and map exercises. Concepts of support are often overlooked during these transition briefs, and cyberspace operations are no exception. However, it is essential for commanders to understand how cyberspace operations synchronize with other warfighting elements across time and space. A clear explanation of DCO, OCO, and DOD IN operations at every phase of the operation is necessary for a successful transition to execution.

Conclusion

The MCPP offers an existing, flexible structure with opportunities for cyberspace operations to inject support in a way that staffs can easily understand. By using this well-known methodology, planners can comprehend the benefits of cyberspace operations and the functions they provide. The details provided within this article suggest an application of cyberspace operations at each step of the MCPP. As a staff gains fluency with cyberspace operations, adaptations and SOPs can be developed to speed this process and improve the planning timeline.

Though MAGTF operations will likely use cyberspace operations as a supporting effort in the near term, future warfare may dictate them as a main effort with maneuver forces as the supporting effort. This paradigm shift is not far from reality, and research should begin on how to plan such operations. Future leaders should consider such a scenario within the MCPP.

Notes

1. Department of Defense, *Joint Publication 3-12, Cyberspace Operations,* (Washington, DC: Joint Staff, 2013).

2. Ibid.

3. United States Marine Corps, *Marine Corps Warfighting Publication 5-1, Marine Corps Planning Process,* (Quantico, VA: 2010).

4. United States Army, *Army Cyber Operations Planner's Course,* (Fort Gordon, GA: 2015).

5. *Marine Corps Planning Process.*