Offensive Cyberspace Operations

Using artificial intelligence and kill chains to analyze the effects of MAGTF execution authority

by LtCol Arun Shankar

Offensive cyberspace operations (OCO) play a crucial role in every phase of modern warfare from competition to conflict to stability. Generally, geographic combatant commanders, U.S. Cyber Command (USCYBERCOM), or Service-level components hold the authority to use these weapons. Though there are methods for MAGTF commanders to request OCO support from these agencies, they can be arduous and time-consuming. In practice, this often leads to the assumed unavailability of this resource and suboptimal outcomes at the MAGTF level. This article proposes a simple mathematical model that uses artificial intelligence (AI) to analyze opportunities when a further delegation of this authority might prove fruitful. Implications of these findings to law and policy are also presented.

Background

OCOs are an element of the warfare function termed “fires.” Fires, most commonly known as bombs and rockets, are more accurately defined as lethal and nonlethal capabilities that produce a specific effect on a target.1 Like psychological operations and electronic warfare, OCOs are nonlethal fires. They aim to disrupt or deny an enemy’s capability but generally do not inflict casualties directly. Examples of OCOs could include adversary data manipulation or network denial.2

Though fire support may come from different agencies and various echelons of command, MAGTF battlespace owners typically hold the authority for executing the use of these assets. In fact, this authority is more common in the use of lethal fires than nonlethal fires. In some cases, this approval is delegated even further through the assignment of direct-support relationships. Within this model, a particular fires asset may be tasked to provide priority support to a given MAGTF mission, and the MAGTF commander would retain authority to use it with very few approval parameters. Three-dimensional warfare domains (air, land, sea, space) are well-suited for this construct.

Contrarily, cyberspace is not bound by the standard Cartesian coordinate system.3 Limits and boundaries can be challenging to estimate, increasing the risk of collateral damage and other unintended consequences. Moreover, OCO resources are precious. Unlike the firing of ammunition, if the adversary discovers the computer code of an OCO, its chance of friendly reuse is unlikely.4 For these reasons, conventional leaders in the cyber community argue that the authority to deploy cyber effects in the battlespace must be held at component and combatant command levels, much like the use of large-scale missiles and nuclear weapons.5

A similar premise was first adopted when electronic warfare capabilities became mainstream in the 1970s. The authority to use these non-kinetic fires was held at the highest levels of command.

However, over time, a delegation of authority was eventually given to ground commanders once a wider au-

This article proposes a simple mathematical model that uses artificial intelligence (AI) to analyze opportunities when a further delegation of this authority might prove fruitful.

>**LtCol Shankar is a CMC Fellow at the Hoover Institution, Stanford University. He has served a combined 28 months in Operation IRAQI FREEDOM and Operation ENDURING FREEDOM as a counter-IED Analyst, Assessments Analyst, and Communications Officer, and holds a PhD in Operations Analysis from George Mason University.**
The code to develop an OCO can take years to script...

This five-phase OCO process can also be decomposed into a Markov Chain, a mathematical matrix of probabilities characterizing transitions between these phases. In particular, the probability of residing in one phase only depends upon the previous state. A Markov Chain’s elegant features allow us to estimate the probability of a successful OCO easily. As new data about OCOs is collected, these transition probabilities are updated, and final estimates are improved through machine learning. Hence, the Markov Chain is the backbone of the AI that powers this mathematical model and its conclusions.

Figure 2 overlays the five phases of the cyber kill chain into a Markov Chain and Markov Diagram. In this elementary model, the probability of successfully completing one phase...
and proceeding to the next phase is 50 percent. Conversely, the probability of failing the phase and returning to the first phase is also 50 percent. Moreover, if the fifth phase (clearing tracks) is completed successfully, there is a 100 percent chance of a successful mission.

The initial transition probabilities within the Markov Chain are derived from the exponential statistical distribution. The exponential distribution is ideal for this circumstance because it is often used in reliability and failure analysis in some manufacturing settings. It requires just two inputs to produce an output probability. The first is the rate parameter, or the minimum time needed to complete the execution of a given phase under the current circumstances. The rate parameter is influenced by the type of cyber target—pre-planned or a target of opportunity. Pre-planned targets should require less time to execute (low rate parameter) because reconnaissance and scanning have generally already occurred successfully (Figure 1). In contrast, targets of opportunity may require execution of all steps of the kill chain, with little prior planning, consequently requiring more time than a pre-planned target (high rate parameter).

The second input is the maximum allowed time for each phase of the cyber kill chain, influenced by the tactical mission deadline. This total available time needs to be subdivided for each phase. Once the two inputs are determined for each phase of the process, the probabilities are computed and inputted into the Markov transition matrix. From here, the total probability of success for the mission is determined.

### Hypothetical Scenario

A MAGTF commander will execute a raid of a near-peer enemy stronghold in 36 hours. He knows his enemy primarily depends on a military cellular phone network to control his forces. He wants to attack the network with the end state of manipulating chat messages to cause chaos and confusion. His intelligence says the adversary is likely monitoring friendly satellite communications, and he does not wish to request OCO support from his higher headquarters. Moreover, since the start of this conventional war, national and Service-level cyber teams have been stretched thin, only providing support to decisive missions of national interest. Thankfully, a small OCO element is organic to his unit. He has been delegated authority to execute OCO missions if they meet specific guidelines and their probability of success is greater than 75 percent.

Cyber missions can be characterized as routine (>24 hours), priority (12–24 hours), or urgent (0–12 hours). In this case, the mission is routine since the commander has 36 hours before execution. The target has also been pre-planned, so reconnaissance and scanning are already complete. Historical data reveals the average minimum time to failure is three hours when gaining access, six hours when maintaining access, and five hours when clearing tracks. The commander allows his OCO team a maximum of twelve hours in each of these sequential phases before he aborts the mission. Consequently, the calculations result in a probability of success of 77 percent. If the remaining guidelines for launch are met, the MAGTF commander should be allowed to execute without further approval.

### Discussion

The preceding AI model (hereafter “Markov Kill Chain”), powered by a Markov Chain, can easily be adapted to portray more complex scenarios. For instance, the five-phase cyber kill chain illustrated in Figure 2 can be converted to the well-known MITRE ATT&CK framework in Figure 3. This kill chain has 14 phases and more than 100 subphases, but the Markov Chain foundation of the model remains the same. Subphases can be modeled separately, aggregating results into the greater Markov Kill “Web.” Additionally, phases need not be sequential—the Markov Kill Chain is especially effective in analyzing parallel actions. Scalability is virtually endless.

---

**Figure 2. Markov Diagram and Markov Chain.** (Figure provided by author.)

<table>
<thead>
<tr>
<th>Phase</th>
<th>Success</th>
<th>Clearing Tracks</th>
<th>Maintaining Access</th>
<th>Gaining Access</th>
<th>Scanning</th>
<th>Reconnaissance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Clearing Tracks</td>
<td>0.5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Maintaining Access</td>
<td>0.5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.5</td>
<td>0</td>
</tr>
<tr>
<td>Gaining Access</td>
<td>0.5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Scanning</td>
<td>0.5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Reconnaissance</td>
<td>0.5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

---

**A MAGTF commander will execute a raid of a near-peer enemy stronghold in 36 hours. He knows his enemy primarily depends on a military cellular phone network to control his forces.**
Moreover, the Markov Kill Chain is primarily driven by the rate parameters that influence the output probability from the exponential distribution. These input parameters are developed from historical data and updated as more data is collected, forming the machine learning backbone for artificial intelligence. A concerted data collection effort is essential for any artificial intelligence endeavor to produce reliable results; the Markov Kill Chain is no different. Therefore, this model’s success also relies on military commands mining and storing this data in a readily accessible format.

Like any assessment tool, this Markov Kill Chain should not be the commander’s sole source of risk assessment. Several qualitative and binary conditions should be considered as well. For instance, the OCO should have logical network boundaries for execution, perhaps requiring senior authorization to traverse outside of enemy military networks. Suppose the enemy is using civilian infrastructure as part of his communications network. In that case, this may require a qualitative judgment by the commander on whether tactical execution of the OCO should be authorized. The target effect of the OCO should also be considered. Higher authorities should be consulted if the OCO can cause widespread, unintended disarray that counters the desired friendly end state. Depending on the circumstances and available data, the Markov Kill Chain can be modified to consider all these conditions before producing a recommendation.

Implications to Law and Policy
Military cyberspace operations are primarily bounded by two specific elements of U.S. Code Title 10 and Title 50...

<table>
<thead>
<tr>
<th>Title 10</th>
<th>Title 50</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>Overview</td>
</tr>
<tr>
<td>Current</td>
<td>Current</td>
</tr>
<tr>
<td>Changes</td>
<td>Changes</td>
</tr>
<tr>
<td>Future</td>
<td>Future</td>
</tr>
</tbody>
</table>

Figure 3. MITRE ATT&CK framework. (Figure provided by author.)
by civilians, not the military, and these cultural barriers are apparent to any service member outside of Washington, DC.

On the other hand, a combatant command is generally distributed and decentralized to support tactical military formations. The culture lends itself to accepting risk when it benefits tempo. Ground and air commanders are encouraged to take initiative and be bold. Therefore, OCO authority is more likely to be in the hands of MAGTF commanders in this latter command structure.

USCYBERCOM’s recent “Defend Forward” initiative is a step in the right direction.21 The DOD’s former passive approach of waiting to be attacked before reacting is no more. Today, USCYBERCOM operators are actively hunting for adversaries before they reach our friendly resources. This long overdue, active defense strategy promotes tempo, but not at the tactical level. Nevertheless, GEN Nakasone and his leaders should be commended for taking this prudent step forward.

Second, the military’s cyber mission capability, or “Cyber Mission Force”, needs to be decentralized (Figure 5), with OCO capabilities at the MAGTF level. Doctrine should be revised to permit the dissolution of this empire into a practical, conventional warfare weapon.

**... the military’s cyber mission capability ... needs to be decentralized...**

The counterargument of a cyberspace unity of command does not void the necessity of decentralized authority. A MAGTF commander cannot optimally maneuver in every warfighting domain without the authority to do so.

Granted, the benefit of this delegation of authority does not necessarily reveal itself during today’s low-intensity competition, but it absolutely will when we face a great power in a conventional conflict.

**Conclusion**

OCO authority can be delegated to MAGTF commanders responsibly and effectively. Future warfare will require regular cyber warfare capabilities, and our tactical commanders need the authority to execute these fires when available. Artificial intelligence models exist to optimize this decision-making challenge. Moreover, our ancient cyberspace law and policy apparatus can easily be adapted to promote this new way of thinking.

This interdisciplinary research has both operational and methodological contributions. Operationally, the author portrays a way that a supervised AI algorithm can be used to promote the delegation of OCO authority to the MAGTF command level and highlights necessary changes in law and policy to attain that goal further.22 Methodologically, the Markov Kill Chain can be adapted to any targeting process in military warfare.23 Any kinetic or
non-kinetic fires methodology can be overlaid onto the Markov Kill Chain, and probabilities of success can be computed easily. No longer do these decisions need to be decided solely through qualitative measures. Today, we have the technology and resources to do better. Future efforts should be focused on the unclassified aggregation of historical OCO data.

Concurrently, data scientists should continue the development of more robust decision support tools that observe more inputs and produce better outputs.

Any kinetic or non-kinetic fires methodology can be overlaid onto the Markov Kill Chain, and probabilities of success can be computed easily.

Specifically, models that can digest enemy network architecture designs and produce collateral risk metrics can be instrumental. In the interim, serious research should illuminate the USCYBERCOM empire and why the bulk of its resources remain inside the Beltway, rather than with our warfighters.

Notes


15. JP 3-60, Joint Targeting.

16. “MITRE ATT&CK.”

17. JP 3-12, Cyberspace Operations.


