2022 LtCol Earl “Pete” Ellis Essay Contest: Honorable Mention

Offensive Cyberspace Operations

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

by LtCol Arun Shankar

>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.

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 warfighting 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 warfighting 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]

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.

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 audience understood risk and capabilities. Citing this precedent, one could argue the same for OCOs.

Boundaries and fires deconfliction can also be defined for OCO scenarios if the environment is constrained and well-understood. Contrarians persist that this is impossible and that cyberspace is so abstract and dimensionless that every OCO has the risk of undesired catastrophic effects.[6] However, even an amateur understanding of networks will reveal that this premise is likely exaggerated. Though it is acknowledged that the network structures often do not correspond with physical space, they do have a logical space defined by IP addresses. This logical space can be assigned to a MAGTF battlespace owner, much like airspace, sea lanes, and battlefields. Designated as a restricted operating zone, it could also constrain maneuver to reduce collateral damage.

In addition to logical boundaries, the *probability of success* should also influence the OCO launch authority. A failed OCO is a costly loss of time and resources because it is also a zero-day attack.[7] Such an attack is the first of its kind, where it exploits a publicly unknown network vulnerability. The code to develop an OCO can take years to script, so its usage should be judicious. Moreover, once an OCO launches, the enemy can likely deconstruct and harvest intelligence from it. Artificial intelligence models are developed specifically for such scenarios, and they can provide credible insight into the probability of an OCO's success.

Once these parameters and constraints are defined within the battlespace, the MAGTF commander could have the authority to navigate within it, using a direct support asset or an organic force. In either event, the decision to act would lie with the MAGTF commander, decentralizing decision making and improving tempo, both of which are vital tenets of conventional maneuver warfare.[8]

Artificial Intelligence Model - Cyber Kill Chain

AI refers to a machine's ability to think and perform tasks like a human. Machine learning is a subset of AI that denotes a machine's predictive and pattern recognition ability.[9] AI is not spreadsheet automation or macro-scripting; instead, its algorithms follow an endless cycle of inputting data and outputting predictions. The predictions are checked against new data, and the algorithm parameters improve accordingly (i.e., machine learning). Typical examples of AI include facial recognition software and grammar editing applications.

The code to develop an OCO can take years to script ...

OCO can be framed by a cyber kill chain—a sequence of regular events for every cyber-attack operation.[10] Depending on the circumstances, they can be in series, parallel, or a combination of both. This decomposition of the cyber-attack process into a probabilistic network of events allows the decision maker to understand better the system's dynamics, rather than an oversimplified, binary scoring system that plagues most military decision support tools. This framework is modeled by assigning probabilities of success to each event, feeding an overall probability score for the success of the kill chain.[11] A commander's appetite for risk can determine a launch threshold for this probability.

Figure 1 portrays a simple kill chain that can be adapted for many scenarios.[12] This kill chain encompasses the actions of reconnaissance, scanning, gaining access, maintaining access, and clearing tracks. Reconnaissance is the act of studying the target and gathering general information such as login information, passwords, IP addresses, and physical locations. Scanning includes using software tools to determine open ports and other vulnerabilities. An attacker gains access through these vulnerabilities and maintains access by escalating privileges and installing backdoors for future access. Once the purpose of the attack is complete, the attacker covers his tracks upon exit by deleting created objects and clearing logs. A successful attack is defined by sequential success at each of these steps of the kill chain.

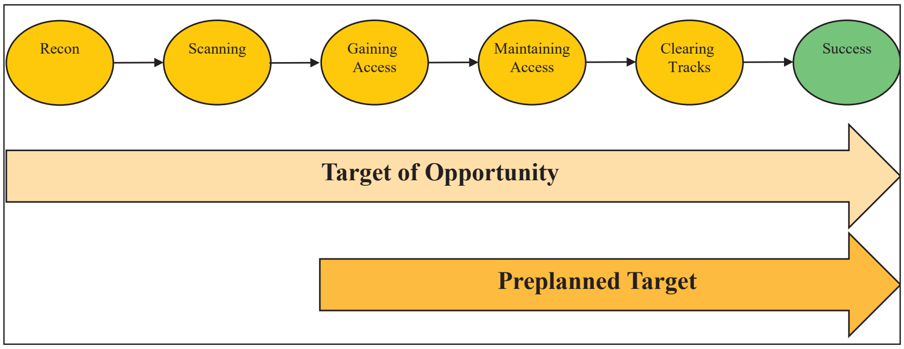


Figure 1. Cyber kill chain. *(Figure provided by author.)*

This five-phase OCO process can also be decomposed into a Markov Chain, a mathematical matrix of probabilities characterizing transitions between these phases.[13] 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

	Reconnaissance	Scanning	Gaining Access	Maintaining Access	Clearing Tracks	Success
Reconnaissance	0.5	0.5	0	0	0	0
Scanning	0.5	0	0.5	0	0	0
Gaining Access	0.5	0	0	0.5	0	0
Maintaining Access	0.5	0	0	0	0.5	0
Clearing Tracks	0.5	0	0	0	0	0.5
Success	0	0	0	0	0	1

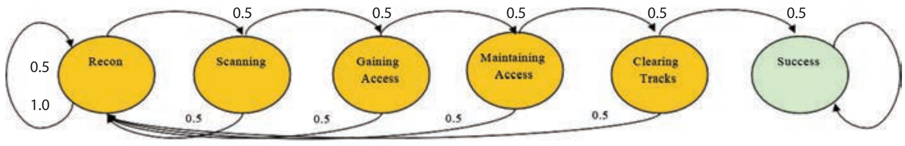


Figure 2. Markov Diagram and Markov Chain. *(Figure provided by author.)*

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.[14] 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—preplanned or a target of opportunity.[15] 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

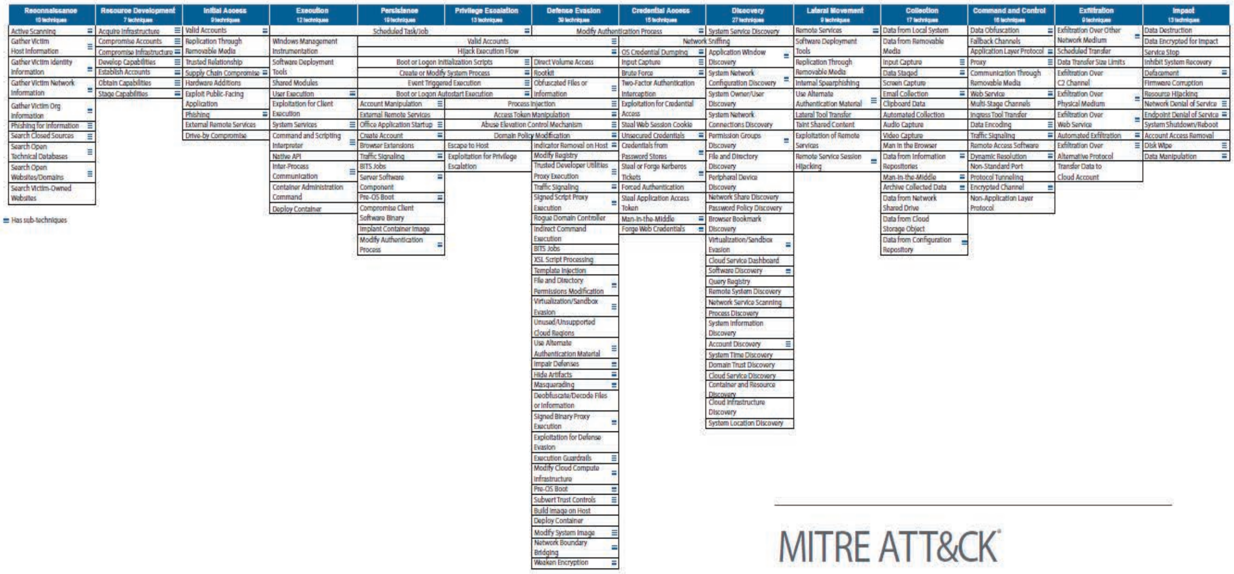
A MAGTF commander will execute a raid of a near-peer enemy stronghold in 36 hours. He knows his enemy primarily depends on a military cellular phone network to control his forces. He wants to attack the network with the end state of manipulating chat messages to cause chaos and confusion. His intelligence says the adversary is likely monitoring friendly satellite communications, so 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.[16] 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.

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.



Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques
Active Scanning ≡	Acquire Infrastructure ≡	Valid Accounts ≡	Scheduled Task/Job ≡			Modify Authentication Process ≡
Gather Victim Host Information ≡	Compromise Accounts ≡	Replication Through Removable Media	Windows Management Instrumentation	Valid Accounts ≡		
Gather Victim Identity Information ≡	Compromise Infrastructure ≡	Trusted Relationship	Software Deployment Tools	Hijack Execution Flow ≡		
Gather Victim Network Information ≡	Develop Capabilities ≡	Supply Chain Compromise ≡	Shared Modules	Boot or Logon Initialization Scripts ≡		Direct Volume Access
Gather Victim Org Information ≡	Establish Accounts ≡	Hardware Additions	User Execution ≡	Create or Modify System Process ≡		Rootkit
Phishing for Information ≡	Obtain Capabilities ≡	Exploit Public-Facing Application	Exploitation for Client Execution	Event Triggered Execution ≡		Obfuscated Files or Information ≡
Search Closed Sources ≡	Stage Capabilities ≡	Phishing ≡	System Services ≡	Boot or Logon Autostart Execution ≡		
Search Open Technical Databases ≡		External Remote Services	Command and Scripting Interpreter ≡	Account Manipulation ≡	Process Injection ≡	
Search Open Websites/Domains ≡		Drive-by Compromise	Native API	External Remote Services	Access Token Manipulation ≡	
Search Victim-Owned Websites			Inter-Process Communication ≡	Office Application Startup ≡	Abuse Elevation Control Mechanism ≡	
			Container Administration Command	Create Account ≡	Domain Policy Modification ≡	Indicator Removal on Host ≡
			Deploy Container	Browser Extensions	Escape to Host	Modify Registry
				Traffic Signaling ≡	Exploitation for Privilege Escalation	Trusted Developer Utilities Proxy Execution ≡
				BITS Jobs		Traffic Signaling ≡
				Server Software Component ≡		Signed Script Proxy Execution ≡
				Pre-OS Boot ≡		Rogue Domain Controller
				Compromise Client Software Binary		Indirect Command Execution
				Implant Container Image		BITS Jobs
				Modify Authentication Process ≡		XSL Script Processing
						Template Injection
						File and Directory Permissions Modification ≡
						Virtualization/Sandbox Evasion ≡
						Unused/Unsupported Cloud Regions
						Use Alternate Authentication Material ≡
						Impair Defenses ≡
						Hide Artifacts ≡
						Masquerading ≡
						Deobfuscate/Decode Files or Information
						Signed Binary Proxy Execution ≡
						Exploitation for Defense Evasion
						Execution Guardrails ≡
						Modify Cloud Compute Infrastructure ≡
						Pre-OS Boot ≡
						Subvert Trust Controls ≡
						Build Image on Host
						Deploy Container
						Modify System Image ≡
						Network Boundary Bridging ≡
						Weaken Encryption ≡

Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
	System Service Discovery	Remote Services ≡	Data from Local System	Data Obfuscation ≡	Exfiltration Over Other Network Medium ≡	Data Destruction
Network Sniffing		Software Deployment Tools	Data from Removable Media	Fallback Channels	Scheduled Transfer	Data Encrypted for Impact
OS Credential Dumping ≡	Application Window Discovery ≡	Replication Through Removable Media	Input Capture ≡	Application Layer Protocol ≡	Data Transfer Size Limits	Service Stop
Input Capture ≡	System Network Configuration Discovery ≡	Internal Spearphishing	Data Staged ≡	Proxy ≡	Exfiltration Over C2 Channel	Inhibit System Recovery
Brute Force ≡	System Owner/User Discovery	Use Alternate Authentication Material ≡	Screen Capture	Communication Through Removable Media	Exfiltration Over Physical Medium ≡	Defacement ≡
Two-Factor Authentication Interception	System Network Connections Discovery	Lateral Tool Transfer	Email Collection ≡	Web Service ≡	Exfiltration Over Web Service ≡	Firmware Corruption
Exploitation for Credential Access	Permission Groups Discovery ≡	Taint Shared Content	Clipboard Data	Multi-Stage Channels	Automated Exfiltration ≡	Resource Hijacking
Steal Web Session Cookie	File and Directory Discovery	Exploitation of Remote Services	Automated Collection	Ingress Tool Transfer	Exfiltration Over Alternative Protocol ≡	Network Denial of Service ≡
Unsecured Credentials ≡	Peripheral Device Discovery	Remote Service Session Hijacking ≡	Audio Capture	Data Encoding ≡	Transfer Data to Cloud Account	Endpoint Denial of Service ≡
Credentials from Password Stores ≡	Network Share Discovery		Video Capture	Traffic Signaling ≡		System Shutdown/Reboot
Steal or Forge Kerberos Tickets ≡	Password Policy Discovery		Man in the Browser	Remote Access Software		Account Access Removal
Forced Authentication	Browser Bookmark Discovery		Data from Information Repositories ≡	Dynamic Resolution ≡		Disk Wipe ≡
Steal Application Access Token	Virtualization/Sandbox Evasion ≡		Man-in-the-Middle ≡	Non-Standard Port		Data Manipulation ≡
Man-in-the-Middle ≡	Cloud Service Dashboard		Archive Collected Data ≡	Protocol Tunneling		
Forge Web Credentials ≡	Software Discovery ≡		Data from Network Shared Drive	Encrypted Channel ≡		
	Query Registry		Data from Cloud Storage Object	Non-Application Layer Protocol		
	Remote System Discovery		Data from Configuration Repository ≡			
	Network Service Scanning					
	Process Discovery					
	System Information Discovery					
	Account Discovery ≡					
	System Time Discovery					
	Domain Trust Discovery					
	Cloud Service Discovery					
	Container and Resource Discovery					
	Cloud Infrastructure Discovery					
	System Location Discovery					

≡ Has sub-techniques

MITRE ATT&CK

Figure 3. MITRE ATT&CK framework. ***(Figure provided by author.)***

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.

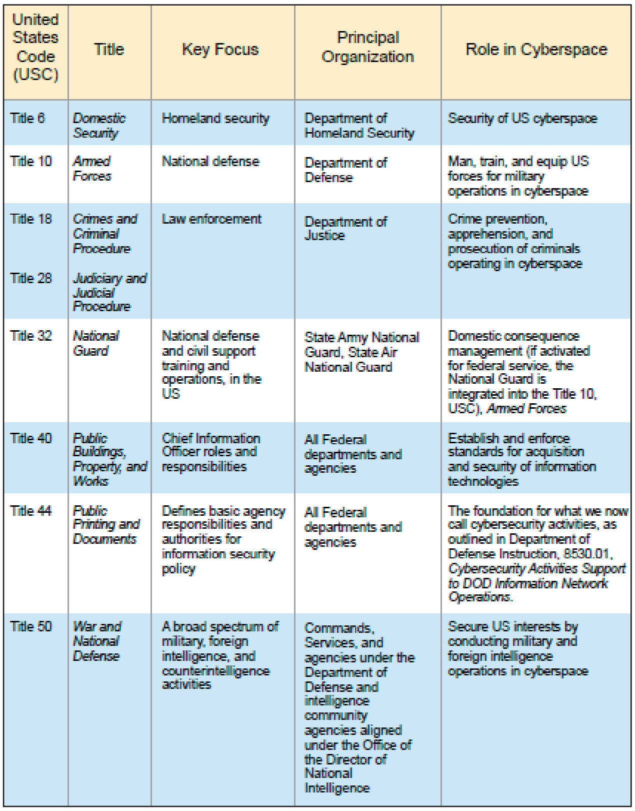
Military cyberspace operations are primarily bounded by two specific elements of* U.S. Code Title 10 *and* Title 50 *...

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*, shown in Figure 4.[17] *Title 10* largely governs military operations in a general sense, including those in cyberspace. *Title 50* focuses on intelligence gathering and allows for cyberspace operations' covert, clandestine nature. Unlike the use of many physical weapons, the U.S. military will not advertise an OCO before it is executed for fear the attack will be thwarted and the precious code deemed useless. Therefore, because of this peculiarity of cyberspace, *Title 50* plays a role in this authorization.[18] Conveniently, the director of the National Security Agency, an intelligence agency, and the commander of USCYBERCOM, a functional combatant command, are the same person, so the dual usage of *Title 10* and *Title 50* is supported by the command structure.

Delegating OCO execution authority to the MAGTF level would require two modifications to this apparatus. First, the National Security Agency and the USCYBERCOM organizations must be commanded by different people and staffs.[19] Despite the overlap in *Title 50* characteristics, cyberspace operations should be planned and characterized as military operations in cyberspace, not as covert operations run by the intelligence community.[20] Intelligence operations are often risk-averse, overclassified, and laden with mounds of analysis. Its agencies are deliberate and methodical, built for long-term strategic outcomes rather than quick, tactical gains. Most of the U.S. intelligence community is manned



United States Code (USC)	Title	Key Focus	Principal Organization	Role in Cyberspace
Title 6	*Domestic Security*	Homeland security	Department of Homeland Security	Security of US cyberspace
Title 10	*Armed Forces*	National defense	Department of Defense	Man, train, and equip US forces for military operations in cyberspace
Title 18 Title 28	*Crimes and Criminal Procedure* *Judiciary and Judicial Procedure*	Law enforcement	Department of Justice	Crime prevention, apprehension, and prosecution of criminals operating in cyberspace
Title 32	*National Guard*	National defense and civil support training and operations, in the US	State Army National Guard, State Air National Guard	Domestic consequence management (if activated for federal service, the National Guard is integrated into the Title 10, USC), *Armed Forces*
Title 40	*Public Buildings, Property, and Works*	Chief Information Officer roles and responsibilities	All Federal departments and agencies	Establish and enforce standards for acquisition and security of information technologies
Title 44	*Public Printing and Documents*	Defines basic agency responsibilities and authorities for information security policy	All Federal departments and agencies	The foundation for what we now call cybersecurity activities, as outlined in Department of Defense Instruction, 8530.01, *Cybersecurity Activities Support to DOD Information Network Operations.*
Title 50	*War and National Defense*	A broad spectrum of military, foreign intelligence, and counterintelligence activities	Commands, Services, and agencies under the Department of Defense and intelligence community agencies aligned under the Office of the Director of National Intelligence	Secure US interests by conducting military and foreign intelligence operations in cyberspace

Figure 4. United States Code. ***(Figure provided by author.)***

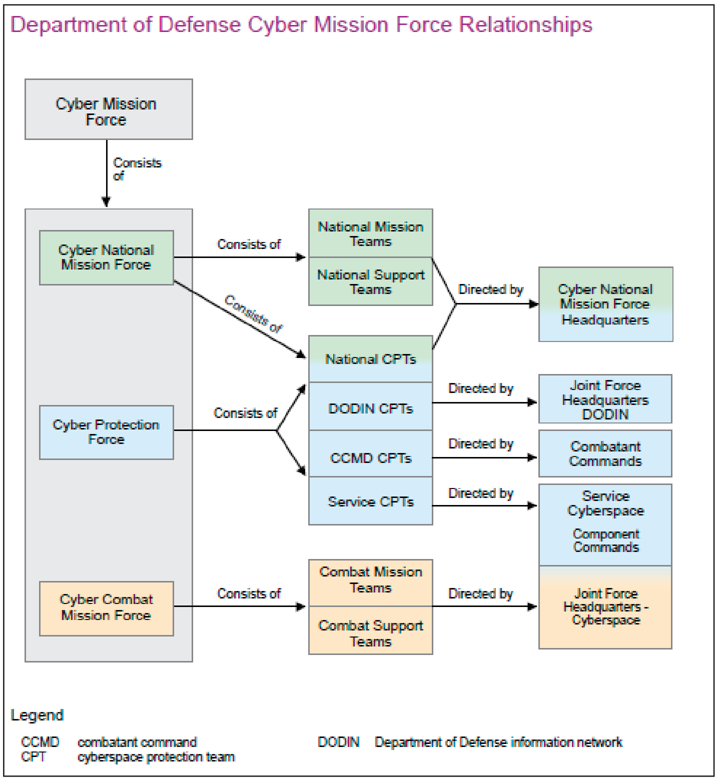

Department of Defense Cyber Mission Force Relationships
Cyber Mission Force
Consists of
Cyber National Mission Force
Consists of
Consists of
National Mission Teams
National Support Teams
Directed by
Cyber National Mission Force Headquarters
National CPTs
Directed by
Joint Force Headquarters DODIN
Cyber Protection Force
Consists of
DODIN CPTs
CCMD CPTs
Directed by
Combatant Commands
Service CPTs
Directed by
Service Cyberspace Component Commands
Cyber Combat Mission Force
Consists of
Combat Mission Teams
Combat Support Teams
Directed by
Joint Force Headquarters - Cyberspace
Legend
CCMD combatant command
CPT cyberspace protection team
DODIN Department of Defense information network

Figure 5. Command and Control relationships (present-day). ***(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 overlayed 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.

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

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

1. Department of Defense, *JP 3-60, Joint Targeting,* (Washington, DC: 2013).

2. Blake Strom, Andy Applebaum, Douglas Miller, Kathryn Nickels, Adam Pennington, Cody Thomas, "MITRE ATT&CK: Design and Philosophy," *MITRE,* March 31, 2020, https://www.mitre.org/news-insights/publication/mitre-attck-design-and-philosophy.

3. Department of Defense, *JP 3-12, Cyberspace Operations,* (Washington, DC: 2018).

4. R. Axelrod and R. Iliev, "Timing of Cyber Conflict," *Proceedings of the National Academy of Sciences of the United States of America* 111, No. 4. (2014).

5. Peter Feaver and Kenneth Geers, *When the Urgency of Time and Circumstances Clearly Does Not Permit: Pre-delegation in Nuclear and Cyber Scenarios From Understanding Cyber Conflict: Fourteen Analogies*, (Washington, DC: Georgetown University Press, 2017).

6. Giorgio Bertoli and Lisa Marvel, "Cyberspace Operations Collateral Damage-Reality or Misconception?" *The Cyber Defense Review*, July 31, 2018, https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1588897/cyberspace-operations-collateral-damage-reality-or-misconception.

7. Tommaso Zoppi, Andrea Ceccarelli, and Andrea Bondavalli, "Unsupervised Algorithms to Detect Zero-Day Attacks: Strategy and Application," *IEEE Acces 9*, (2022).

8. Headquarters Marine Corps, *MCDP 6, Command and Control*, (Washington, DC: 1996).

9. S. Aziz and M. Dowling, "Machine Learning and AI for Risk Management," in *Disrupting Finance* (New York: Springer International Publishing, 2019).

10. W. Zeng and Vasileios Germanos, "Modelling Hybrid Cyber Kill Chain," *Research Gate,* June 2019, https://www.researchgate.net/publication/335753886_Modelling_Hybrid_Cyber_Kill_Chain.

11. William J. Farrell III and Dean Wilkening, "Modeling Kill Chains Probabilistically," *Military Operations Research* 25, No. 3 (2020).

12. Muhammed Mudassar Yamin et al., "Mapping Tools for Open Source Intelligence with Cyber Kill Chain for Adversarial Aware Security," *Mathematics 10, No.* 12 (2022).

13. Kishor S. Trivedi and Andrea Bobbio, "Continuous-Time Markov Chain: Reliability Models," in *Reliability and Availability Engineering* (Cambridge: Cambridge University Press, 2017).

14. Boualem Rabta, Bart van den Boom, and Vasco Molini, "A Continuous-time Markov Chain Approach for Modeling of Poverty Dynamics: Application to Mozambique," *African Development Review* 28, *No.* 4, (2016).

15. *JP 3-60, Joint Targeting,*

16. "MITRE ATT&CK."

17. *JP 3-12, Cyberspace Operations,*

18. Andru Wall, "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action," *Presidents and Fellows of Harvard College*, 2011, https://harvardnsj.org/wp-content/uploads/sites/13/2012/01/Vol-3-Wall.pdf.

19. Frank Cilluffo and Joseph Clark, "Repurposing Cyber Command," *Parameters* 43, No.4 (2013).

20. Benjamin Leitzel and Gregory Hillebrand, *Strategic Cyberspace Operations Guide*, (Carlisle: U.S. Army War College, 2022).

21. Jack Goldsmith and Alex Loomis, "'Defend Forward' and Sovereignty," *Hoover Institution*, April 29, 2021, https://www.hoover.org/research/defend-forward-and-sovereignty.

22. M. Emre Celebi, *Supervised and Unsupervised Learning* (New York: Springer, 2020).

23. William Farrell III and Dean Wilkening, "Modeling Kill Chains Probabilistically," *Military Operations Research* 25, No. 3 (2020).