Military Cyber Affairs

Volume 4
Issue 1 *Command and Control of Cyberspace Operations*

Article 3

2019

Prioritizing Strategic Cyberspace Lethality

Andrew J. Schoka
United States Cyber Command, andrew.j.schoka@gmail.com

Prioritizing Strategic Cyberspace Lethality

Cover Page Footnote

The views and opinions expressed in this paper are those of the author alone and do not reflect the official policy or position of the U.S. Department of Defense, U. S. Cyber Command, or any agency of the U. S government.

Abstract:

The primary concern of United States national security policy, as detailed in the 2018 National Defense Strategy, has shifted from asymmetrical counter-insurgency operations to countering inter-state strategic competition by rogue regimes and revisionist powers. This doctrinal shift has prompted an increased emphasis on military lethality, particularly in strategic-level cyberspace operations intended to counter open challenges to the global security environment and United States preeminence. Drawing from the theory of constraints in industrial engineering and Bayesian search theory in operations research, this paper identifies the key organizational constraints that hinder the lethality of the Department of Defense's strategic-level cyberspace operations units in light of a continued struggle for available cyberspace personnel. Current force structure paradigms and command and control policies are identified as the key limiting factors of military lethality in cyberspace. This paper argues for ruthlessly prioritizing the elimination and improvement of these constraints in order to align Department of Defense policies with efforts to project strategic power in and through cyberspace.

When U.S. Secretary of Defense Jim Mattis announced the nation's new National Defense Strategy, he emphasized that "inter-state strategic competition, not terrorism, is now the primary concern in U.S. national security".[1] This change in U.S. strategic thinking has marked a dramatic doctrinal shift away from asymmetrical counter-insurgency operations to long-term symmetrical warfare between nuclear powers. It is a recognition of the increasingly entropic nature of the global strategic environment, in which a *de facto* state of open conflict exists between numerous nations across the globe, and an acknowledgement of increased military and economic development by rivalling powers. The unclassified version of the National Defense Strategy characterizes the greatest threat to U.S. prosperity and security to be the "reemergence of long-term strategic competition by...revisionist powers and rogue regimes".[2] Predatory economic policy and strategic brinkmanship, not jihadist extremism, are now of principal strategic interest. The revised strategic posture of the U.S. seeks to address the influence operations, information campaigns, and diplomatic maneuverings of rival nation states seeking increasingly greater degrees of regional hegemony and global influence.

Of particular importance to the U.S.'s efforts to successfully adapt to a changing global operating environment is the ability to operate effectively in and through the cyberspace domain. Increased military lethality, particularly in the realm of cyberspace operations, is highlighted as the first and most important strategic priority in the 2018 National Defense Strategy.[3] Addressing his vision and priorities for the nascent U.S. Cyber Command in light of the strategic shift to competition between nuclear superpowers, General Paul Nakasone posited that "the locus of the struggle for power has shifted to cyberspace".[4] In light of the acknowledged strategic need for increased lethality in the cyberspace domain, the Department of Defense must address several critical challenges that impede the nation's strategic-level cyberspace efforts. A lack of unity of command amongst Cyber Command's mission teams is a key issue affecting strategic cyberspace lethality, and is exacerbated by systemic recruiting and retention challenges across the military cyber workforce. In order to meet the challenges of a changing global strategic environment, the Department of Defense should ruthlessly prioritize strategic cyberspace lethality by modernizing Cyber Command's force structure, unifying the multiple chains of command that presently exist across its formations.

The concept of ruthless prioritization is an idea borrowed from the theory of constraints, a management and process improvement methodology developed in the field of industrial engineering.[5] The management philosophy behind the theory of constraints suggests that manageable processes are limited from achieving significantly greater efficiency by a disproportionately small number of constraints, or bottlenecks.[6] After identifying a system's bottlenecks, the theory of constraints dictates that an organization ruthlessly subjugate all decisions to the systematic improvement of that constraint until it is no longer the limiting factor of the system.[7] From a standpoint of accomplishing an organization's objectives, the greatest level of overall organizational progress is achieved through the elimination of these critical constraints first, prior to addressing other impediments. Considering inter-state strategic competition in cyberspace within the context of the theory of constraints, it is important to characterize issues facing the cyberspace operations workforce as constraints to achieving strategic-level success in cyberspace.

Another important factor to consider in the process of systematically identifying and improving a system's bottlenecks is the feasibility of accomplishing the improvement of individual constraints. This concept is based in Bayesian search theory, a form of statistics applied in operations research to identify a mathematically optimized search order based on probabilistic modeling. In Bayesian search theory, the locations that should be searched first are not necessarily the locations where an object is most likely to be, but also where it is most likely that an object could be found if it is actually located there.[8] Applied in an organizational context, it is not only the criticality of a constraint that should be considered, but also the feasibility of addressing and improving that constraint.

Considering bureaucracy at the scale of the U.S. Department of Defense, there are a large number of organizational constraints that potentially have a detrimental effect on achieving strategic success in cyberspace. However, the focus should be narrowed to those policies, authorities, and decisions that can be feasibly addressed within a reasonable time frame and without considerable expense or disruption. For instance, consolidating all military cyberspace personnel to a new and separate branch of military service would likely eliminate a great deal of organizational constraints associated with a joint force the size of

U.S. Cyber Command.[9] However, the amount of time, resources, and legislation required for such a change make it infeasible to achieve from a practical, present-oriented standpoint. In order to bring about impactful change in the nation's strategic cyberspace forces, it is critical that the solutions proposed are not only related to the system's most critical constraints, but also feasible in terms of time, resources, and authorities.

Military and political leaders have recognized, rightfully, that the U.S. military no longer holds the advantage of uncontested superiority across all warfighting domains.[10] As acknowledged in the National Defense Strategy, the U.S. has "no preordained right to victory.".[11] Instead, military forces operating in all domains must adapt to fighting in a highly contested environment, in which unilateral superiority across all warfighting domains is not always guaranteed. Looking ahead to potential future conflicts between nation-states, the inherently accessible and asymmetric nature of the global information environment may form an operating environment in which it is impossible to ever operate uncontested in the cyberspace domain.[12] The realities presented by a rapidly-changing and technologically interconnected global operating environment are in sharp contrast to the military's doctrinal assumptions for the better part of the last half-century. In response to this, the Department of Defense has rapidly stood up U.S. Cyber Command, now a full unified combatant command, and charged it with the responsibility for unifying, coordinating, and executing the nation's cyberspace operations.

Cyber Command's force structure is based on the Cyber Mission Force (CMF), a team-based construct consisting of 133 cyber teams, each specializing in offense, defense, or operational support. The majority of CMF teams are aligned to support the various Combatant Commands, or retained directly by each separate service branch.[13] Additionally, a small number of these teams are organized under the Cyber National Mission Force (CNMF) as a direct subordinate unit of U.S. Cyber Command.[14] Each branch of the military is responsible for providing a set number of these teams to Cyber Command through their respective cyber component command (ARCYBER, AFCYBER, MARFORCYBER, and FLTCYBER), and is responsible for training, manning, and equipping the CMF teams in order to conduct their respective missions.[15]

The CMF is the primary force responsible for the conduct of cyberspace operations at the strategic level. When nation-states present a significant threat to U.S. infrastructure, systems, or interests, it is Cyber Command's teams that are charged with the responsibility of conducting full-spectrum cyberspace operations to defeat and deter that threat. This responsibility includes combating large-scale influence operations and dis-information campaigns targeting democratic processes, problem sets that are of tremendous national importance and visibility.[16] Cyber Command's offensive mission teams are the U.S.'s main instrument of projecting strategic power in cyberspace, and are the on-call force responsible for national-level priorities and objectives in cyberspace.

In the coming years, the daunting challenges faced by Cyber Command in recruiting and retaining the cyber personnel assigned to the CMF are projected to continue to increase in scale and severity.[17] Manpower studies and projections of future job demand in cyber-related work roles suggest there simply aren't enough qualified cyberspace operations personnel to fully meet the anticipated cyber personnel needs of all the services.[18] Coupled with the significant time and expense required to train, clear, and certify new cyberspace operations personnel, there will continue to be an unavoidable shortage of available personnel in the CMF.[19] Without novel, and potentially controversial, changes to recruiting criteria and enlistment methods, this constraint is unlikely to change in the foreseeable future. This problem is further perpetuated by an injurious manning cycle that leaves offensive CMF teams struggling to maintain operationally effective levels of trained and experienced personnel.

In light of an acknowledged lack of cyber personnel, Cyber Command's effective employment of available resources is of critical importance to the U.S's strategic success in cyberspace. However, despite the advantage gained through fostering a highly collaborative joint command environment, Cyber Command's current force structure fosters a lack of command unity for teams assigned to support a command outside of their service. This introduces a critical constraint that hinders strategic cyberspace lethality, bottlenecking Cyber Command's operational efforts.

Unity of command is a critical axiom inherent to joint-level military operations, and is meant to ensure that a subordinate has a clear chain of

command above them from which to receive orders and direction.[20] Unity of command is utilized in virtually every military organization across the services; a Navy submarine, an Air Force fighter squadron, a Marine infantry platoon, and an Army tank company all share one characteristic in common: a single commander responsible for both the administrative and operational functions of that unit during execution of its mission. While it is common for units to often be tasked to support other commands, and may even be detached from their "owning" command to do so, they will always maintain a command element that is responsible for the overall administrative and operational aspects of that unit.

Because of the manner in which legislation has dictated the Department of Defense to construct Cyber Command, the various teams from each service remain under administrative control (ADCON) of their providing service, while being assigned under operational control (OPCON) of Cyber Command.[21] ADCON responsibilities primarily revolve around providing a trained and ready force, and encompass anything pertaining to the unit's administrative functions, including personnel management, training, and readiness. OPCON responsibilities center around the execution of the unit's mission, and consists of the direction and employment of the team's members during the conduct of operations. Neither OPCON nor ADCON can operate fully without the other's support, and a unit fundamentally depends on the effective and timely support of both OPCON and ADCON responsibilities in order to function.

The bifurcation of command responsibilities between multiple leaders produces competing sets of priorities wherein multiple commanders each maintain control over critical functions of a single unit.[22,23]In Cyber Command's current force structure, a member of an Army National Mission Team reports administratively to their service's ADCON unit commander and operationally to their CMF team leader. The result of the services filling a force-supplying supporting role to Cyber Command is that service members are subordinate to separate administrative and operational chains of command.[24] This harmful dichotomy manifests regularly when operational and administrative commanders find themselves at odds over a unit's priorities and function.[25]

In addition to hindering mission accomplishment, having multiple sources of command authority also complicates career progression and talent management

for cyberspace operations personnel. The responsibilities of an Air Force flight commander, for example, are easily understood across the service regardless of career field, whereas the responsibilities of a Cyber Support Team Lead are less well-known. However, under current implementation of the Defense Officer Personnel Management Act (DOPMA), officer promotions are handled by centralized selection boards, and positions like Air Force flight or Army company command, typically associated with operational authority, tend to be considered more favorable for promotion.[26] This creates a difficult choice for officers in cyber career fields, who are often forced to decide between career-benefitting administrative roles with little operational applicability, or technically demanding operational roles at the expense of promotion potential.[27] The administrative commander who fights to pull personnel away from mission for a unit-mandated training event is not acting in the wrong, as their metrics of success and chance of promotion rely on the completion of administrative tasks mandated by the next step in the administrative chain of command. Likewise, the operational commander's success is determined by the completion of mission-related tasks, even at the expense of administrative requirements. This tug-of-war between an administrative commander and an operational commander will continue to exist for as long as unity of command is not implemented in Cyber Command's command-and-control structure.

The lack of unity of command in the current CMF force structure is a key constraint hindering strategic cyberspace lethality, and the Department of Defense must ruthlessly prioritize the elimination of this bottleneck. With significant attention dedicated in extant research to the retention of experienced cyberspace personnel, the vestigial split of administrative and operational control in the CMF ought to be considered as not only a critical mission accomplishment factor, but also a key issue for retention. If the main recruiting message of the Department of Defense is the ability to contribute to a unique cyberspace mission, it should expect continued struggles in retention if it fails to employ personnel in a way to meaningfully contribute to that mission.[28] This requires vesting operational CMF commanders with administrative command authority for their units, unifying the two chains of command that currently exist across Cyber Command. Ruthless prioritization of strategic-level cyberspace operations would dictate that the services be required to designate CMF team leaders additionally as the command authority for the teams' corresponding administrative formations.

The strategic global security environment continues to rapidly evolve, and open challenges to the established international order and national sovereignty will continue. U.S. interests will be increasingly challenged abroad, and the U.S. military will continue to operate in heavily contested warfighting domains without the decisive overmatch it has grown accustomed to for much of the last half-century. Russia will continue to engage in deliberate influence operations intended to undermine fundamental democratic functions of American society and further ideological divisions in the population.[29] China will continue its predatory economic policies and targeting of U.S. intellectual property and personal information through vulnerable networks.[30] Iran will continue to pursue development of destructive capabilities to increase its regional standing, and persist in its sponsorship of terrorist organizations to destabilize neighboring regions.[31] North Korea will continue to seek coercive influence over the U.S. and its allies through pursuit of weapons of mass destruction.[32]

These threats will continue to develop unchecked so long as there is no legitimate deterrence to the actions of revisionist powers and rogue regimes. Put more simply by Senate testimony of General Nakasone, because these rivaling nation states "do not fear us".[33] It is the stated mission of the Cyber National Mission Force to defend the nation against threats of significant consequence in cyberspace by imposing cost on adversaries seeking to undermine U.S. influence and interests. Inter-state strategic competition will continue to pose an existential threat to U.S. safety and security, necessitating deterrence of hostile actors. Legitimate deterrence through increased cyberspace lethality demands the ruthless prioritization of U.S. strategic efforts in cyberspace, and nothing less.

References:

1. 2018 National Defense Strategy of the United States of America. Unclassified summary retrieved from: https://admin.govexec.com/media/20180118173223431.pdf
2. Ibid.
3. Ibid.
4. GEN Paul Nakasone, Remarks at the 9th Billington Cybersecurity Summit, 6 September 2018.
5. Eliyahu M. Goldratt, "The Goal: A Process of Ongoing Improvement". Great Barrington, MA. North River Press. 2004.
6. Ibid.
7. Ibid.
8. Lawrence D. Stone, "Theory of Optimal Search". New York, New York. Academic Press. 1975
9. James Stavridis and David Weinstein, "Time for a U.S. Cyber Force". *Proceedings*, U.S. Naval Institute. January 2014.
10. GEN Paul Nakasone, Remarks at the 9th Billington Cybersecurity Summit, 6 September 2018.
11. 2018 National Defense Strategy.
12. Brett T. Williams, *The Joint Force Commander's Guide to Cyberspace Operations*, Joint Force Quarterly 73, 2014.
13. Ibid.
14. Mark Pomerleau, "The New Cyber Leader Focused On National Defense", *Fifth Domain*. June 2018.
15. Mark Pomerleau, "Here's How the Cyber Service Component Mission Sets Differ From Cybercom", C4ISRNet. July 2017.
16. Jim Garamone, "National Security Agency, Cybercom Defend Against Election Meddling", Defense Media Activity. August 2018.
17. Arthur Macdougall and Michael Myers, "Pentagon Faces Array of Challenges in Retaining Cybersecurity Personnel", The Hill. June 2018.
18. Morgan Chalfant, "Pentagon Faces Slew of Cyber Challenges in New Year", The Hill. January 2018.
19. Andrew Schoka, "Training Cyberspace Maneuver", Small Wars Journal, June 2018.
20. "Joint Publication 3-0: Joint Operations". January 2017
21. Ibid.
22. Josh Lospinoso, "Fish Out of Water: How the Military is an Impossible Place for Hackers and What to Do About It", War on the Rocks. July 2018.

23. Leonard Wong and Stephen J. Garras. “Lying to Ourselves: Dishonesty in the Army Profession”. Carlisle Barracks, PA. United States Army War College Press. 2015.
24. Table 3-2: Army Support Relationships, “Army Field Manual 4-95: Logistics Operations”. April 2014.
25. Ibid.
26. DOPMA Policy Reference Tool, The RAND Corporation. Available at: http://dopma-ropma.rand.org/
27. Lospinoso, “Fish Out of Water”.
28. Jared Serbu, “More Authorities Could Help Army Recruit Cyber Officers From Silicon Valley”, Federal News Radio. August 2018.
29. Alyza Sebenius, “NSA Chief Forms Group to Counter Russian Cyber Threat”, Bloomberg. July 2018.
30. Kathleen McInnis, “The 2018 National Defense Strategy”, Congressional Research Service. February 2018
31. Collin Anderson and Karim Sadjadpour, “Iran’s Cyber Threat: Espionage, Sabotage, and Revenge”, Carnegie Endowment for International Peace. January 2018.
32. Dorothy Denning, “North Korea’s Growing Criminal Cyberthreat”, Scientific American. February 2018.
33. GEN Paul Nakasone, Testimony to the Senate Armed Services Committee, March 2018.