INSTITUTE FOR DEFENSE ANALYSES

What Is the Purpose of the Cyber Mission Force?

Michael P. Fischerkeller, *Project Leader*

February 2019

IDA Document
D-10466
Copy

INSTITUTE FOR DEFENSE ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

The Institute for Defense Analyses is a non-profit corporation that operates three federally funded research and development centers to provide objective analyses of national security issues, particularly those requiring scientific and technical expertise, and conduct related research on other national challenges.

About This Publication

This work was conducted by the Institute for Defense Analyses (IDA) under contract HQ0034-14-D-0001, Task CB-5-4600, "Supporting and Maturing the Strategy of Persistent Engagement," for USCYBERCOM. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgments

Gen. (retd.) Larry D. Welch

For more information:

Michael P. Fischerkeller, Project Leader
mfischer@ida.org, 703-845-6784

Margaret E. Myers, Director, Information Technology and Systems Division
mmyers@ida.org, 703-578-2782

INSTITUTE FOR DEFENSE ANALYSES

IDA Document D-10466

What Is the Purpose of the Cyber Mission Force?

Michael P. Fischerkeller, *Project Leader*

Executive Summary

General Paul Nakasone, Commander United States Cyber Command (USCYBERCOM), recently and rhetorically posed the following question "What function does U.S. Cyber Command perform that obligates society to assume responsibility for its maintenance?"[1] This question is a variant of a theme that permeated strategic literature emerging after the end of World War II: What is the purpose of U.S. military forces?[2] In spite of its existential leanings, it is an important question for which USCYBERCOM should have a defensible response when queried about the Cyber Mission Force, as less than a year ago, all 133 cyber mission teams achieved Full Operational Capability.[3] This essay both derives an answer by adopting an analytical framework first appearing in post-World War II strategic scholarship – one based on considerations of geography and technology – and reviews recent U.S. strategic guidance to ascertain what U.S. policy maintains (or implies) the purpose should be. The first analysis concludes the chief purpose of the Cyber Mission Force should be to seize the initiative and gain superiority in the cyber strategic competitive space short of armed conflict, whereas the second suggests it should be coercive. This misalignment, should it not be corrected, portends an ineffectual future for the CMF in great power competition.

[1] Nakasone, "A Cyber Force for Persistent Operations," p. 11.

[2] See, for example, Huntington, "National Policy and the Transoceanic Navy"; Schelling, *Arms and Influence*; and Brodie, *The Absolute Weapon: Atomic Power and World Order*.

[3] U.S. Cyber Command Public Affairs, "Cyber Mission Force Achieves Full Operational Capability."

Contents

1. The Importance of Purpose

In his 1954 essay examining the post-war purpose of the U.S. Navy, Samuel Huntington argues that "[T]the fundamental element of a military service is its purpose or role in implementing national policy." "Purpose" is a description of how, when, and where the military service expects to protect the nation against some threat to its security. Without purpose, a service will "wallow about amid a variety of conflicting and confusing goals, and ultimately it suffers both physical and moral degeneration." In this essay, I take the liberty of extending this argument from one that is service-centric to one that is force-centric, confident that it is no less potent from the latter orientation. This allows for its consideration for the Cyber Mission Force (CMF).

2. The Framework: Technology and Geography

A. Pre-World War II

In introducing his concept of coercive diplomacy, Thomas Schelling claims that "To seek out and destroy the enemy's military force, to achieve a crushing victory over enemy armies, was the avowed purpose and the central aim of American strategy in both world wars."[4] He argues the reason behind this purpose is "apparently that the technology and geography of warfare, at least for a war between anything like equal powers during the century up through World War II, kept coercive violence from being decisive before military victory was achieved."[5] The same reasoning, he argues, characterized the great wars of the century preceding World War II – "for reasons of technology and geography, military force has usually had to penetrate, to exhaust, or to collapse opposing military force – *to achieve military victory* – before it could be brought to bear on the enemy nation itself."[6]

Although Schelling does not state it explicitly, if one assumes that purpose flows from national policy, as Huntington argues, it can reasonably be concluded that the purpose of U.S. military forces in the two world wars, as well as that of the forces of the great powers in the century prior to World War II was to defeat an enemy's forces. Regarding the latter, Schelling noted that "[T]the allies in World War I could not inflict coercive pain and suffering directly on the Germans in a decisive way until they could defeat the German army; and the Germans could not coerce the French people with bayonets unless they first beat the Allied troops that stood in their way."[7]

B. Post-World War II

The development of nuclear weapons and the technologies supporting their delivery made geography *strategically less consequential* in determining the purpose of military forces "between anything like equal powers" post-World War II. With these technologies, great powers expect to be able to penetrate an adversary's homeland without first collapsing its military force. Military forces in possession of them are able to levy

[4] Schelling, *Arms and Influence,* p. 16.

[5] Ibid.

[6] Ibid, p. 21.

[7] Ibid, pp. 21–22.

extraordinary violence on an adversary's populace without first achieving military victory – a significant change from the pre-World War II period. And so, with the advent of these technologies, those who possess them no longer require a military victory before coercing an adversary.[8] Consequently, "military victory" no longer adequately expresses what nations who wield such strategy-altering capabilities primarily want the purpose to be of their military forces. Instead, and mostly, Schelling argues, they want the influence that resides in latent force and not the bargaining power that results from direct consequences of military victory.[9] Bernard Brodie captured this most succinctly and, perhaps alarmingly, by saying that "Thus far the chief purpose of our military establishment has been to win wars. From now on its chief purpose must be to avert them. It can have almost no other useful purpose."[10]

Schelling and Brodie argue, then, that with the advent of nuclear weapons and their means of delivery, military strategy between nuclear-armed powers should no longer be thought of as the science of military victory, as it could for some countries in other eras. Schelling argues most persuasively that defeating a near-peer adversary's military forces should, therefore, not be the primary purpose of U.S. military forces. Military strategy for the United States should now be equally, if not more, the art of coercion, of intimidation and deterrence, because the military instruments of war post-World War II are far more punitive than acquisitive.[11]

U.S. policy post-world War II and strategy documents from this century are indicative of this coercive purpose. Regarding the former, Alexander George refers to deterrence as the "handmaiden" of the U.S. Cold War containment policy.[12] More recently, the 2005 National Defense Strategy says that the United States will achieve its strategic objectives by assuring allies and friends, dissuading potential adversaries, deterring aggression and countering coercion, and defeating adversaries should deterrence fail. Similarly, the national military objectives espoused in the 2011 and 2015 U.S. national military strategies are, respectively, to deter and defeat aggression; counter violent extremism; and strengthen international and regional security, and to deter, deny, and defeat state adversaries; disrupt, degrade, and defeat violent extremist organizations; and strengthen the global network of allies and partners.

---

[8] Ibid, p. 22.

[9] Ibid, p. 31.

[10] Brodie, *The Absolute Weapon: Atomic Power and World Order*, p. 76.

[11] Schelling, *Arms and Influence*, p. 34.

[12] George and Smoke, *Deterrence in American Foreign Policy: Theory and Practice*, p. 4.

C. The Advent of Cyberspace

Comprising a vast array of technologies, cyberspace, through its core structural feature of interconnectedness has arguably made geography *strategically inconsequential* among and between great power adversaries (and state and non-state actors, as well). Additionally, this structural feature, its consequent condition of constant contact, and the imperative for persistent action derived from both has shifted the dominant interaction dynamic between states from episodic, militarized crises and war (the strategic space of armed conflict) to continuous competition in the cyber strategic competitive space short of armed conflict.[13] Although adversaries *could* employ cyber campaigns/operations to attack an enemy's military forces for the purpose of military "victory" or *could* attack (or threaten to attack) an enemy nation for coercive purposes, there have been few such incidents to-date between states not already at war.[14] Indeed, Richard Harknett and I have argued that there are both structural incentives and strategic rationales for states to not use cyber campaigns/operations in support of these ends. Due to interconnectedness, strategic targets are accessible in, through, and from cyberspace via cyber operations/campaigns short of armed conflict; and through constant contact, persistent action in the cyber strategic competitive space short of armed conflict holds out the prospect for cumulative change resulting from these campaigns/operations that can really matter – changes that can affect sources of national power.[15]

These arguments lead to conclusions regarding the purpose of the CMF that differ slightly from the post-World War II conclusions of Schelling and Brodie regarding the U.S. military force, writ large. I agree that military strategy (when considering the CMF) should not be thought of as the science of military victory. That is, crushing an adversary's forces (cyber or otherwise) should not be its chief purpose, as the day-to-day cyber competition short of armed conflict is the dominant strategic approach through which states are seeking to make significant gains.[16] However, I differ from Schelling and Brodie by arguing that the military instruments of competition in this cyber strategic competitive space are more exploitative than punitive, and so military strategy in this space should be primarily the art

---

[13] Fischerkeller and Harknett, "Deterrence is Not a Credible Strategy for Cyberspace."

[14] See, for example, Valeriano, Jensen, and Maness, *Cyber Strategy*; Valeriano and Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*; and *Center for Strategic and International Studies' Significant Cyber Events List*, https://csis-prod.s3.amazonaws.com/s3fs-public/180308_Significant_Cyber_Events_List.pdf? Of the few cyber attacks generating effects equivalent with armed attack, nearly all have been between states engaged in armed conflict. Consider for example, the Russian-attributed attacks on the Ukrainian electrical grid. See Greenburg, "How an Entire Nation Became Russia's Test Lab for Cyber War."

[15] Fischerkeller and Harknett, *Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics, and Escalation.*

[16] Moreover, there are significant limitations to how much destructive, physical damage cyber operations/campaigns could do to an adversary's forces.

of competition, not coercion – of seizing the initiative and gaining cyber superiority through persistence in competition. It follows that the chief purpose of the CMF should be the pursuit of these military objectives through persistence in the cyber strategic competitive space short of armed conflict. This is not to say that the CMF has no purpose to support coercive operations/campaigns in the strategic space of armed conflict. Indeed, Joint Task Force ARES was established in 2016 to counter ISIL in cyberspace.[17] Rather, it is to say that purpose is subsidiary to, and actually is often supported by, its chief purpose in competition.

[17] See Martelle, "Joint Task Force ARES and Operation GLOWING SYMPHONY: Cyber Command's Internet War Against ISIL."

3. The 2018 Department of Defense (DoD) Cyber Strategy and U.S. National Cyber Strategy

It is instructive to compare my conclusions with guidance offered in the 2018 DoD and U.S. National cyber strategies.[18] There are three sections in the former from which one might be able to infer a chief purpose of the CMF. An opening section discussing the strategic competition in cyberspace makes the following argument:

> First, we must ensure the U.S. military's ability to fight and win wars in any domain, including cyberspace. This is a foundational requirement for U.S. national security and a key to ensuring that we deter aggression, including cyberattacks that constitute a use of force, against the United States, our allies, and our partners.[…];
>
> Second, the Department seeks to preempt, defeat, or deter malicious cyber activity targeting U.S. critical infrastructure that could cause a significant cyber incident regardless of whether that incident would impact DoD's warfighting readiness or capability. Our primary role in this homeland defense mission is to defend forward by leveraging our focus outward to stop threats before they reach their targets. The Department also provides public and private sector partners with indications and warning (I&W) of malicious cyber activity, in coordination with other Federal departments and agencies, and;
>
> Third, the Department will work with U.S. allies and partners to strengthen cyber capacity, expand combined cyberspace operations, and increase bi-directional information sharing in order to advance our mutual interests.[19]

The first two points suggest that, at a minimum, the chief purpose of the CMF should be coercion (consider as evidence references to deter, defeat, and preempt). A second section of the document highlighting the Department's cyberspace objectives, however, doesn't necessarily support this argument:

1. Ensuring the Joint Force can achieve its missions in a contested cyberspace environment;

---

[18] See U.S. Department of Defense, *Summary of the Department of Defense Cyber Strategy*, and The White House, *National Cyber Strategy of the United States of America*.

[19] U.S. Department of Defense, *Summary of the Department of Defense Cyber Strategy*, p. 2.

2. Strengthening the Joint Force by conducting cyberspace operations that enhance U.S. military advantages;
3. Defending U.S. critical infrastructure from malicious cyber activity that alone, or as part of a campaign, could cause a significant cyber incident;
4. Securing DoD information and systems against malicious cyber activity, including DoD information on non-DoD-owned networks; and
5. Expanding DoD cyber cooperation with interagency, industry, and international partners.[20]

Frankly, it is difficult to draw any conclusions regarding the CMF's chief purpose from this list of objectives, as they are not of the same format as the national military objectives specified in the national military strategies cited previously. However, a third section of the cyber strategy describing DoD's strategic approach to realizing those objectives aligns more closely with that format.

Of the three lines of effort composing the strategic approach, the second is the most relevant and is entitled "Compete and Deter." Through this line of effort *the Department will prioritize securing sensitive DoD information and deterring malicious cyber activities that constitute a use of force* against the United States, our allies, or our partners; and, should deterrence fail, the Joint Force stands ready to employ the full range of military capabilities in response. In addition, the Department will counter cyber campaigns threatening U.S. military advantage by defending forward to intercept and halt cyber threats and by strengthening the cybersecurity of systems and networks that support DoD missions. This includes working with the private sector and our foreign allies and partners to contest cyber activity that could threaten Joint Force missions and to counter the exfiltration of sensitive DoD information.[21]

By prioritizing deterring malicious cyber activities constituting a use of force, the Department again suggests that the chief purpose of the CMF should be coercion. In sum, were we to draw a conclusion from the DoD cyber strategy, and admittedly it would be a tenuous one, it would be that the chief purpose of the CMF should be coercion. This conclusion is made less tenuous, however, when considering the content of the U.S. National Cyber Strategy.

In the section entitled "Attribute and Deter Unacceptable Behavior in Cyberspace" the national cyber strategy makes clear that that United States will use all instruments of national power to attribute and deter malicious cyber activities with integrated strategies that impose swift, costly, and transparent consequences when malicious actors harm the

[20] Ibid, p. 3.

[21] Ibid, p. 4.

United States or its partners.[22] Moreover, the strategy says the United States will launch an international Cyber Deterrence Initiative to build a coalition of like-minded states and develop tailored strategies to ensure that adversaries understand the consequences of their malicious cyber behavior.[23] The National Cyber Strategy offers no ambiguity regarding strategic approach – deterrence – and, consequently, strongly suggests that the chief purpose of the CMF is coercion. Perhaps it is not surprising that of the CMF's 133 teams not aligned against defending the Department of Defense Information Network (DoDIN), approximately 70% are aligned against coercive missions.[24]

The purpose suggested by both strategies and weight of effort implied in team distribution is at odds with what I've argued in this essay should be the primary purpose of the CMF. Interestingly, however, the closing remarks in both the 2018 National Defense Strategy and the DoD Cyber Strategy have it right, from my perspective, if we're to infer priority from order – both argue that the Department must be prepared to compete, deter, and win.[25] That language may be a leading indicator of upcoming changes ensuring better alignment, but that may merely be wishful thinking. Two obvious remedies for stronger alignment come to mind: select a percentage of the CMF aligned to coercive missions and re-task them to support competition and/or increase the size of the CMF and task the new forces in support of competition. Regarding the latter, General Nakasone recently commented that "as we continue to operate more, as our adversaries continue to improve, there will be requirements that will probably be outside the 133 teams that we have right now", although he did not specify in support of what purpose those additional teams might be aligned.[26]

---

[22] The White House, *National Cyber Strategy of the United States of America*, p. 21.

[23] Ibid.

[24] This value was calculated by first setting aside the 68 Cyber Protection Teams assigned to defend the DoDIN, then assuming (reasonably) the number and size of Combat Support Teams and National Support Teams are equal, and finally assuming (reasonably) the sizes of Combat Mission Teams and National Mission Teams are equal and calculating the relative percentage of each against the total number of mission teams. Combat Mission Teams (27 of 40) primarily conduct military cyberspace operations in support of combatant commander priorities and missions (i.e., their purpose is coercive). National Mission Teams (13 or 40) primarily support competition in the cyber strategic competitive space short of armed conflict. See U.S. Cyber Command Public Affairs, *Cyber Mission Force Achieves Full Operational Capability*

[25] U.S. Department of Defense, *Summary of 2018 National Defense Strategy of The United States of America*, p. 11, and U.S. Department of Defense, *Summary of the Department of Defense Cyber Strategy*, p. 7.

[26] *Congressional Quarterly*, "Senate Armed Services Committee Holds Hearing on U.S. Special Operations and Cyber Command"

4. Conclusion

I noted at the outset of this essay that General Nakasone asked his question about "purpose" rhetorically. I would be remiss to exclude his answer. Recall that his question was framed in the context of USCYBERCOM, not the CMF specifically. That said, I think his answer applies equally well to both. He says he would explain to the nation that CYBERCOM's strategic concept (Huntington's alternative term for "purpose") has evolved from one of a "response force" to one of a "persistence force."[27] A cyber "response force" is a force whose purpose is coercion. A cyber "persistence force" is one that continuously seeks initiative, seeking to gain cyber superiority through persistence in competition. General Nakasone's perspective is consistent with the argument offered in this essay.

Although recent U.S guidance has evidenced marked, positive shifts in identifying a re-emergent great power competition and the significant role the cyber strategic competitive space plays in it, that same guidance continues to be grounded in (and weighted down by) a legacy strategic approach (coercion) that is misaligned with this competitive space. The CMF's chief purpose is to compete short of armed conflict and unless and until U.S. strategic guidance is aligned to that purpose, the potential effectiveness of the CMF in great power competition will not be fully realized.

[27] Nakasone, "A Cyber Force for Persistent Operations," p. 11.

References

Brodie, Bernard. *The Absolute Weapon: Atomic Power and World Order*. New York: Harcourt, Brace and Company, 1946. https://www.worldcat.org/title/absolute-weapon-atomic-power-and-world-order/oclc/2067440

Congressional Quarterly. "Senate Armed Services Committee Holds Hearing on U.S. Special Operations and Cyber Command," February 14, 2019, http://www.cq.com/doc/congressionaltranscripts-5464111?0

Fischerkeller, Michael P. and Richard J. Harknett. "Deterrence is Not a Credible Strategy for Cyberspace." *Orbis* 61, no. 3 (Summer 2017): 381–393. https://www.fpri.org/article/2017/06/deterrence-not-credible-strategy-cyberspace/

Fischerkeller, Michael P. and Richard J. Harknett. *Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics, and Escalation*. Alexandria, VA: Institute for Defense Analyses, 2018. https://www.ida.org/idamedia/Corporate/Files/Publications/IDA_Documents/ITSD/2018/D-9076.pdf

George, Alexander L. and Richard Smoke. *Deterrence in American Foreign Policy: Theory and Practice*. New York: Columbia University Press, 1974.

Greenburg, Andy. "How an Entire Nation Became Russia's Test Lab for Cyber War." *Wired* (June 20, 2017). https://www.wired.com/story/russian-hackers-attack-ukraine/

Huntington, Samuel P. "National Policy and the Transoceanic Navy." *U.S. Naval Institute Proceedings* 80, no. 5 (May 1954): 483–489. https://www.usni.org/magazines/proceedings/1954-05/national-policy-and-transoceanic-navy

Martelle, Michael. "Joint Task Force ARES and Operation GLOWING SYMPHONY: Cyber Command's Internet War Against ISIL." *National Security Archive*. August 13, 2018. https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-13/joint-task-force-ares-operation-glowing-symphony-cyber-commands-internet-war-against-isil

Nakasone, Paul M. "A Cyber Force for Persistent Operations." *Joint Force Quarterly* 92, no. 1 (2019): 10–15.

Schelling, Thomas C. *Arms and Influence*. New Haven: Yale University Press, 2008. https://yalebooks.yale.edu/book/9780300143379/arms-and-influence

U.S. Cyber Command Public Affairs. "Cyber Mission Force Achieves Full Operational Capability." May 17, 2018. https://www.cybercom.mil/Media/News/News-Display/Article/1524492/cyber-mission-force-achieves-full-operational-capability/

U.S. Department of Defense. *Summary of 2018 National Defense Strategy of the United States of America*. Washington, DC: Department of Defense, 2018. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

U.S. Department of Defense. *Summary of the Department of Defense Cyber Strategy*. Washington, DC: Department of Defense, 2018. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

Valeriano, Brandon, Benjamin Jensen, and Ryan Maness. *Cyber Strategy*. Oxford, United Kingdom: Oxford University Press, 2018. https://global.oup.com/academic/product/cyber-strategy-9780190618094?cc=us&lang=en&

Valeriano, Brandon and Ryan C. Maness. *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*. New York, NY: Oxford University Press, 2015. https://global.oup.com/academic/product/cyber-war-versus-cyber-realities-9780190204792?cc=us&lang=en&

The White House. *National Cyber Strategy of the United States of America*. September 2018. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
00-02-19	Final	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
What Is the Purpose of the Cyber Mission Force?	HQ0034-14-D-0001
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)	5d. PROJECT NUMBER
Michael P. Fischerkeller	CB-5-4600
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES	8. PERFORMING ORGANIZATION REPORT NUMBER
Institute for Defense Analyses 4850 Mark Center Drive Alexandria, VA 22311-1882	D-10466

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR'S / MONITOR'S ACRONYM
LTC George Corbari USCYBERCOM/NSA Combined Action Group, Ft. Meade, MD	USCYBERCOM
	11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

This draft has not been approved by the sponsor for distribution and release.

13. SUPPLEMENTARY NOTES

Project Leader: Michael P. Fischerkeller

14. ABSTRACT

General Paul Nakasone, Commander United States Cyber Command (USCYBERCOM), recently and rhetorically posed the following question "What function does U.S. Cyber Command perform that obligates society to assume responsibility for its maintenance?'" This question is a variant of a theme that permeated strategic literature emerging after the end of World War II, i.e., what is the purpose of U.S. military forces? In spite of its existential leanings, it is an important question for which USCYBERCOM should have a defensible response when queried about the Cyber Mission Force as, less than a year ago, all 133 cyber mission teams achieved Full Operational Capability. This essay derives an answer by adopting an analytical framework first appearing in post-World War II strategic scholarship, one based on considerations of geography and technology, and concludes that the chief purpose of the Cyber Mission Force should be to seize the initiative and gain superiority in the cyber strategic competitive space short of armed conflict.

15. SUBJECT TERMS

Cyberspace, cyber mission force, cyber strategy, persistent engagement

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			LTC George Corbari
Unclassified	Unclassified	Unclassified	Unlimited	20	19b. TELEPHONE NUMBER (Include Area Code) 301-688-1744