A Case for a Cyberspace Combatant Command

Blending Service and Combatant Command Responsibilities and Authorities

Lt Col Shawn M. Dawley, ANG

The next draft of the *Unified Command Plan* should redesignate US Cyber Command as a functional combatant command (COCOM). In much the way that significant contingents of leadership in the US Army wished to relegate the Army Air Corps to a mere supporter of land warfare operations, today's military routinely exercises cyberspace capabilities in supporting roles that enable operations in other domains. Placing US Cyber Command (USCYBERCOM) on the same level as other geographic and functional COCOMs and granting it authority to organize, train, and equip its subordinate forces will allow it to more readily build, harness, and exploit capabilities within this newest field of warfare.

Although man-made, cyberspace remains a domain in which participants can act and react, thus resembling the air, space, maritime, and land domains. As in preceding conflicts, back to antiquity, any tribe, criminal element, or nation-state that fails adequately to weaponize its abilities in the available war-fighting domains may find itself unable to wage combat successfully across the spectrum of warfare. Because of the principally nonkinetic nature of cyberspace, institutional and doctrinal battles over the organization and employment of US cyber's capabilities have tended to focus on its enabling characteristics rather than its offensive capacity. The Department of Defense's (DOD) organizational, procurement, and deployment policies place airpower in the air domain, sea power in the maritime domain, and land power in the land domain. As articulated by Gen Peter Pace, USMC, retired,

former chairman of the Joint Chiefs of Staff, "the integration of offensive and defensive cyberspace operations, coupled with the skill and knowledge of our people, is fundamental" to ensuring strategic superiority in the cyber domain.[1]

Whereas the other war-fighting domains existed long before people's ability to operate within them, an inexorable link exists between the cyber domain and the capabilities within it—just as the tools and doctrine evolve, so does the medium. This evolutionary component likely will cause cyber to become the most unpredictable area within the full spectrum of conflict. Embracing this reality possibly requires an approach and organizational structure that not only accepts but also encourages nonconformity and less-than-conventional warriors.

Large-scale kinetic warfare typically rewards forces that are steadfastly disciplined and grounded in sound doctrine (given the number of combatants involved and the close coordination necessary for execution). A much smaller force, however, can prosecute cyber warfare, rewarding speed and agility in the cyber domain on a magnitude greater than in traditional battlespaces. Thus, if these assumptions are valid, a cyber enterprise may call for operators less inclined to stand firm in established doctrine *and* for an entity to organize and employ them unlike traditional service or COCOM constructs. The current organizational model within the *Unified Command Plan* places the newly formed joint USCYBERCOM as a subunified command under US Strategic Command. The military needs a construct that blends service and war-fighting authorities into a single body *and* elevates that organization to a level where it can fully exploit cyberspace. Toward that end, it should make USCYBERCOM a full, functional COCOM *and* grant the command budgetary authorities under title 10, *United States Code*, to organize, train, and equip its unique contingent of warriors.

Strategy and Execution

Although long-standing customs, international norms, and armed conflicts have established nearly universal recognition of physical sovereignty, the nation-state notion of physical dominion is less exacting in discussions of the cyber domain. Since the Peace of Westphalia in the mid-seventeenth century, sovereignty has been viewed as a legitimate authority over territorial possessions.[2] Thus, for over 300 years, governments, whether monarchies or republics, could physically delineate encroachments on their territories by land, sea, and—eventually—air forces. Further, physical destruction of a fortress or financial institution inarguably constituted an act of war. In the cyber domain, nonkinetic actions produce the same effects, leaving the aggrieved without the same sense of hostile activity. But a computer network attack rendering a fire-brigade command post unable to fix targets or a virus "zeroing out" a banking system's accounts is not *completely* unlike munitions leveling either one. The principal distinction is that a kinetic attack provides for a tangible "CNN effect" while one that simply uses binary code lacks the appeal to passion so critical to calls for retaliation.

Because attacks or probes can (and do) happen within the cyber domain—but not in the same way they occur in the other domains—nation-states must update the doctrinal tradition of just war theory. Particularly as it relates to *jus ad bellum*, "which concerns the justice of resorting to war in the first place," many international affairs scholars hold that only in the aftermath of a threat, existential or otherwise, should a nation-state resort to conflict.[3] To date, such threats have typically been directed against physical possessions. The presence of every computer, cellular telephone tower, and communications grid on the front line in any cyber war prevents defense in depth.[4] Principally, since cyber's vulnerabilities include its reliance on nonproprietary, civilian-operated, and interconnected network systems, "we have no early warning radar system or Coast Guard to patrol the borders in cyberspace."[5] Therefore, consistent with the Bush doctrine, which sees preemptive warfare as the necessary counter to asymmetric threats

posed by hostile actors leveraging weapons of mass destruction, a successful approach to cyber melds defensive posturing with offensive, preemptive capabilities.

Cyber Operations and Strategic Guidance

Most of the attention given to cyber and cyber warfare in strategic planning guidance addresses threats posed to the United States and its allies rather than the necessity of weaponizing friendly cyber capacity. In the most recent *National Security Strategy*, *National Defense Strategy*, and *National Military Strategy of the United States of America*, senior government and military leaders strongly emphasize the dangers posed by state and nonstate actors capable of conducting cyber attacks against the United States and its allies. They pay less attention to developing a robust "strike" capability. Naturally, since these publications are available to both a domestic and international audience, one would not expect them to contain any specifics regarding offensive capabilities. At the same time, the degree to which these documents explore our nation's vulnerabilities in the cyber domain far exceeds the attention paid to generating combat power.

In the *National Security Strategy* (2010), President Barack Obama acknowledges the importance of cybersecurity, listing it as one of just six strategic imperatives for safeguarding US national interests: "In addition to facing enemies on traditional battlefields, the United States must now be prepared for asymmetric threats, such as those that target our reliance on space and cyberspace."[6] This and other excerpts prepared by his national security staff and presented in that document deal for the most part with US vulnerabilities. The strategy accurately captures and portrays the nature of future cyber threats as existing across the continuum of potential adversaries. However, it presents the facilitating role of cyber exclusive of its offensive ability: "The threats we face range from individual criminal hackers to . . . terrorist networks to advanced nation states. . . . Our digital infrastructure, therefore, is a strategic national asset. . . . We will deter,

prevent, detect, defend against, and quickly recover from cyber intrusions and attacks."[7]

Like the *National Security Strategy*, the *National Defense Strategy* (2008) acknowledges that the susceptibility of cyberspace to malicious operations is a strategic vulnerability. Further, it also lacks strong and significant guidance in the way of furthering offensive engineering of cyber capabilities: "The United States . . . and our partners face a spectrum of *challenges*, including . . . emerging space and cyber threats" (emphasis added).[8] Cyber dangers are rightly grouped with the array of potential nonconventional threats, but the *National Defense Strategy* presents them solely as a *challenge*—not as an opportunity for exploitation. Further, the strategy has a tendency to think even more narrowly than the president's strategic guidance in that it more readily associates cyber threats with asymmetric warfare against the United States by a weaker adversary: "Small groups or individuals . . . can attack vulnerable points in cyberspace . . . causing economic damage, compromising sensitive information and materials, and interrupting critical services such as power and information networks."[9]

Finally, the *National Military Strategy of the United States of America* (2011) contemplates cyberspace not simply as a prospective "Achilles' heel" but as a domain in which the United States can and should *prosecute* operations. It readily accepts the impending challenges to the enabling capability of cyber when it stipulates that "assured access to and freedom of maneuver within the global commons—shared areas of sea, air, and space—and globally connected domains such as cyberspace are being increasingly challenged by both state and non-state actors."[10] However, the strategy departs from its parent documents issued by the president and secretary of defense when it establishes that "enabling *and war-fighting domains* of space and cyberspace are simultaneously more critical for our operations, yet more vulnerable to malicious actions" (emphasis added).[11] Here, a reader of senior strategic policy guidance gets a first mention of cyberspace as an arena in which warfare, albeit principally nonkinetic, takes place. This dual-purpose con-

text is comparable to that of any other domain. For example, in the air domain, one can perform aerial resupply of forward operating bases (an enabling function) or bombing strikes of armored columns (a war-fighting function). More to the point, the *National Military Strategy* declares that "space and cyberspace enable effective global war-fighting in the air, land, and maritime domains, *and have emerged as war-fighting domains in their own right*" (emphasis added).[12]

Further downstream from the chairman of the Joint Chiefs of Staff's strategy document, the outlook in the *Joint Operating Environment* makes comparable assessments about the unfolding dynamics of cyberspace. It addresses threats *within* cyber, such as its becoming a "main front in both irregular and traditional conflicts," as well as the range of *adversaries* from "states and non-states . . . from the unsophisticated amateur to highly trained professional hackers."[13] One finds a more direct call to action, however, in the *Universal Joint Task List* (under "Manage Cyberspace Operations"), which charges "services and agencies [to] ensure *offensive* and defensive capabilities are fielded and ready to further DOD and United States . . . national security objectives in cyberspace" (emphasis added).[14] Although lacking the *Joint Task List*'s demand for offensive capability within cyberspace, the *Joint Operating Environment* does issue a challenge—as does the *National Military Strategy*—to rethink the organizational and doctrinal construct of the DOD's cyber enterprises.

In the *Joint Operating Environment*, one reads that "while progress toward defining requirements and advocating for Service cyberspace forces has been made, cyber threats will demand a new mindset to ensure agility in adapting to new challenges."[15] Similarly, but with more emphasis on the organizational issues ahead, the *National Military Strategy* posits that "we will carefully review legacy personnel systems. . . . The emerging war-fighting domain of cyberspace requires special attention in this regard."[16] Within the parameters of these strategic vectors of "new mindset," "agility," and manpower, there is latitude to approach cyber capabilities, roles, and missions *not* as extrapolations of

existing organizations and doctrines but as unique problems worthy of innovative solutions.

At the COCOM and service levels, bottom-up approaches to cyber warfare have been divided more appropriately between maintaining access to the enabling functions of cyber (defense) and the ability to exploit and attack adversary networks (offense):

> USCYBERCOM is responsible for planning, coordinating, integrating, synchronizing, and directing activities to operate and defend the Department of Defense information networks and when directed, conducts full-spectrum military cyberspace operations . . . in order to ensure U.S. and allied freedom of action in cyberspace, *while denying the same to our adversaries*.[17] (emphasis added)

The phrase "denying the same" conveys a deliberate and active application of cyber capability against an enemy to create effects in a manner consistent with effects-based operations, which are "planned, executed, assessed, and adapted to influence or change systems or capabilities in order to achieve desired outcomes."[18] Linking actions to objectives, one can generate effects either kinetically or nonkinetically. The utilization of cyber capabilities to affect nodes within a system—especially within a system-of-systems—can create effects whose outcomes far exceed the inputs. Especially because warfare is complex and nonlinear, a small cyber action against a nodal construct can produce disruptive consequences.

A Combatant Command Model

According to Joint Publication 1, *Doctrine for the Armed Forces of the United States*, functional COCOMs are "responsible for a large functional area requiring single responsibility for effective coordination of the operations therein. These responsibilities are normally global in nature."[19] Beyond this operational orientation, US Special Operations Command (USSOCOM) also merges *service-like* authorities and responsibilities with those typically associated with other functional COCOMs. Like a hybrid of a service and a COCOM (e.g., the US Navy and

US Central Command), USSOCOM prepares forces for fielding and then plays a role when they go into battle.

Following the passage of the Defense Reorganization Act of 1986, USSOCOM was established as a four-star unified command "responsible for preparing Special Operations Forces to carry out assigned missions and, if directed by the President or Secretary of Defense, to plan and conduct special operations."[20] The first charge, "preparing Special Operations Forces," is comparable to that of any service; the second, "to plan and conduct special operations," falls within the realm normally associated with a COCOM.

The *Unified Command Plan* of 2004 "assigned USSOCOM responsibility for synchronizing Department of Defense plans against global terrorist networks and, as directed, conducting global operations [against those networks]."[21] To do so, the command "receives, reviews, coordinates and prioritizes all DoD plans . . . and then makes recommendations to the Joint Staff regarding force and resource allocations to meet global requirements."[22]

If USSOCOM performs both service-like duties to build a force and COCOM-like authorities to employ it, then the command provides for an organization that

1. develops strategy and doctrine to address unique challenges;
2. has budgetary authority to recruit, organize, train, and equip select personnel;
3. can provide resources to COCOMs in a supporting role; and
4. can conduct operations worldwide in a supported role.

This blending of service-style title 10 responsibilities with COCOM-style authorities allows for an organization with a worldwide mandate that can marry the right personnel to its mission; develop nimble tactics, techniques, and procedures; and wage war against the enemy along the spectrum of conflict. USCYBERCOM should adopt this model.

Recommendations

A functional COCOM that recruits, organizes, trains, equips, and employs cyber capabilities as weapons in warfare's newest domain is essential to contemporary conflict. Just as Air Force Special Operations Command, Marine Special Operations Command, Army Special Operations Command, and Navy Special Warfare Command are component commands of USSOCOM, so would Army Forces Cyber Command, Twenty-Fourth Air Force, Fleet Cyber Command, and Marine Forces Cyber Command retain their affiliations as service components of USCYBERCOM.[23] Like the components currently comprising USSOCOM, the components of the elevated USCYBERCOM should include personnel uniquely and thoroughly suited to its core mission.

Existing manpower models demonstrate the effectiveness of a long "tooth-to-tail" ratio for certain force constructs. Of the nearly 60,000 members of USSOCOM, only about 20,000 of them are "operators"—individuals recruited, trained, and retained as special forces.[24] Looking at another community for context, that of remotely piloted aircraft, one sees that the number of pilots and sensor operators represents but a fraction of the overall required manpower. This model reinforces the concept of a centrally controlled cyber operations center, given that mission operators of these aircraft can perform global functions from a geographically separated garrison installation.

The ratio of support personnel to cyber operators needs further research, but, more than likely, the operators would receive support from a larger number of administrative and technical specialists. Similar to the US Army's "SOF [special operations forces] Truths" that "quality is better than quantity" and that "humans are more important than hardware," not every "cyber soldier" need be a hunter-killer.[25] Rather, the majority of USCYBERCOM would include the various administrative and logistics support personnel that make up any other command, with emphasis on deliberately recruiting, training, equipping, and retaining those select men and women best suited to the dual missions of cyber defense and cyber attack.

Following, or in conjunction with, a revision of the *Unified Command Plan*, legislative action would provide budgetary authority to USCYBERCOM—like that of the services and USSOCOM—and would specify roles and missions, necessitating a change to title 10 *United States Code* (Armed Forces), part 1 (Organization and General Military Powers), chapter 6 (Combatant Commands). Aside from devising regulations to incorporate the above-mentioned statutory change in the status of USCYBERCOM, the DOD would need to revise its planning, programming, budgeting, and execution process.[26] Like Major Force Program 11, Special Operations (MFP-11) in the *Future Years Defense Program*, the DOD should establish a dedicated major force program (e.g., "MFP-12 Cyber Operations"), along with a budgetary entry for USCYBERCOM (similar to what USSOCOM, the services, and DOD agencies currently have).[27]

Finally, to wage cyber warfare, a standing joint cyber task force (JCTF) should be established within USCYBERCOM. Acting as both a fusion cell for worldwide monitoring of cyber threats and a command authority through which the secretary of defense, in communication with the Joint Chiefs of Staff, can direct USCYBERCOM to conduct its COCOM mission, this JCTF would plan for and direct offensive and counterattack operations within cyberspace against the spectrum of adversaries threatening US national interests, cyber or otherwise.

Conclusion

A USCYBERCOM empowered to organize, train, and equip its forces *and* employ them against adversaries can more fully build and exploit capabilities within warfare's newest domain. So long as a cyber force remains subordinated to potential service or traditional war-fighting parochialism, it will be hindered in weaponeering its capacity to inflict effects in the battlespace. By providing its leaders more freedom of movement within the DOD bureaucracy, USCYBERCOM will allow them to develop and maintain combat power in a way that is less hampered by the conventional focuses of their respective branches—just as

airpower underwent reexamination as a capability that transcended its supporting effects to the Army's battlefield doctrine. Once its forces are fully developed and available, a USCYBERCOM with functional COCOM authority to conduct operations against nodal systems is positioned to create disproportional and potentially catastrophic effects. These effects—some of which can be "undone," given their often nonkinetic nature—can be produced through surgical application by a standing JCTF. ✪

Notes

1. Chairman of the Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations* (Washington, DC: Chairman of the Joint Chiefs of Staff, December 2006), vii, http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf.
2. Eleonore Kofman and Gillian Youngs, eds., *Globalization: Theory and Practice* (New York: Pinter, 1996), 111.
3. *Stanford Encyclopedia of Philosophy*, Fall 2008 ed., s.v. "War," http://plato.stanford.edu/archives/fall2008/entries/war/.
4. US Joint Forces Command, *The Joint Operating Environment* (Suffolk, VA: US Joint Forces Command, Joint Futures Group, 18 February 2010), 34–36, http://www.jfcom.mil/newslink/storyarchive/2010/JOE_2010_o.pdf.
5. Forrest Hare, "Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security?," in *The Virtual Battlefield: Perspectives on Cyber Warfare*, ed. Christian Czosseck and Kenneth Geers, Cryptology and Information Security Series, vol. 3 (Fairfax, VA: Ios Press, 2009), 5.
6. President of the United States, *National Security Strategy* (Washington, DC: White House, May 2010), 17, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.
7. Ibid., 27.
8. Department of Defense, *National Defense Strategy* (Washington, DC: Department of Defense, June 2008), 1, http://www.defense.gov/news/2008%20national%20defense%20strategy.pdf.
9. Ibid., 7.
10. Joint Chiefs of Staff, *National Military Strategy of the United States of America* (Washington, DC: Joint Chiefs of Staff, 2011), 3, http://www.jcs.mil//content/files/2011-02/020811084800_2011_NMS_-_08_FEB_2011.pdf.
11. Ibid.
12. Ibid., 9.
13. US Joint Forces Command, *Joint Operating Environment*, 36.

14. *Universal Joint Task List*, version 7.1, 17 July 2012, [244], http://www.dtic.mil/doctrine/training/ujtl_tasks.pdf.

15. US Joint Forces Command, *Joint Operating Environment*, 36.

16. Joint Chiefs of Staff, *National Military Strategy*, 17.

17. "U.S. Cyber Command," United States Strategic Command, December 2011, http://www.stratcom.mil/factsheets/Cyber_Command/.

18. Air Force Doctrine Document 2, *Operations and Organization*, 3 April 2007, 13, http://www.e-publishing.af.mil/shared/media/epubs/afdd2.pdf.

19. Joint Publication 1, *Doctrine for the Armed Forces of the United States*, 2 May 2007 (Incorporating Change 1, 20 March 2009), I-14, http://www.dtic.mil/doctrine/new_pubs/jp1.pdf.

20. "U.S. Special Operations Command—SOCOM," US Department of Defense, accessed 9 November 2012, http://www.defense.gov/OrgChart/office.aspx?id=62.

21. "About USSOCOM," United States Special Operations Command, accessed 9 November 2012, http://www.socom.mil/Pages/AboutUSSOCOM.aspx.

22. Ibid.

23. "U.S. Cyber Command Fact Sheet," US Department of Defense, 25 May 2010, http://www.defense.gov/home/features/2010/0410_cybersec/docs/cyberfactsheet%20updated%20replaces%20may%2021%20fact%20sheet.pdf.

24. Senate, *Hearings before the Committee on Armed Services to Authorize Appropriations for Fiscal Year 2012 for Military Activities of the Department of Defense and for Military Construction, to Prescribe Military Personnel Strengths for Fiscal Year 2012, and for Other Purposes*, 112th Cong., 1st sess., http://www.gpo.gov/fdsys/pkg/CHRG-112shrg68084/html/CHRG-112shrg68084.htm. In this document, see US Special Operations Command and US Central Command, 1 March 2011, and posture statement of Adm Eric T. Olson, USN, commander, US Special Operations Command.

25. "SOF Truths," US Army Special Operations Command, accessed 9 November 2012, http://www.soc.mil/USASOC%20Headquarters/SOF%20Truths.html.

26. "Planning, Programming, Budgeting & Execution Process (PPBE) (Biennial Driven)," Defense Acquisition University, 27 September 2012, https://dap.dau.mil/acquipedia/Pages/ArticleDetails.aspx?aid=10fdf6c0-30ca-43ee-81a8-717156088826.

27. Department of Defense, *Future Years Defense Program (FYDP) Structure* (Washington, DC: Department of Defense, Office of the Director, Program Analysis and Evaluation, April 2004), 6, http://www.dtic.mil/whs/directives/corres/pdf/704507h.pdf; and Maj Robert Siau, commander, 143rd Combat Communications Squadron Detachment, Washington Air National Guard, discussion with the author, March 2011.

Lt Col Shawn M. Dawley, ANG

Lieutenant Colonel Dawley (BS, MBA, Embry-Riddle Aeronautical University; MA, Marine Corps University; MA, American Military University) is commander of the 165th Airlift Squadron, Kentucky Air National Guard. A C-130 pilot who has flown combat and combat-support sorties in support of Operation Enduring Freedom, Operation Iraqi Freedom, Operation Joint Forge and Joint Guard, and Operation Southern Watch, he most recently served as commander of the 737th Expeditionary Airlift Squadron in Southwest Asia. Lieutenant Colonel Dawley has completed Squadron Officer School, Air Command and Staff College, Marine Corps Command and Staff College, Air War College, and the Joint Force Staff College's advanced joint professional military education.

Let us know what you think! Leave a comment!