The US Army War College Quarterly: Parameters

Volume 43
Number 4 *Parameters Winter 2013*

Article 27

Winter 12-1-2013

Repurposing Cyber Command

Frank J. Cilluffo

Joseph R. Clark

Repurposing Cyber Command

Frank J. Cilluffo and Joseph R. Clark

Abstract: Recent debates about the organizational relationship between Cyber Command and the NSA stress political issues over force employment. This article focuses on the latter, making the case that Cyber Command should be split from the NSA, because nations that marshal and mobilize their cyber power and integrate it into strategy and doctrine will ensure significant national security advantage. Cyber Command provides the best route for developing the tactics, techniques, and procedures necessary for achieving these goals.

For twenty years, members of the United States' national security community, including readers of this journal, have debated the potential tactical, operational, and strategic effects of cyber components and capabilities.[1] Recently, these discussions have become intertwined with arguments about the organizational relationships as well as the Title 10 (traditional military) and Title 50 (intelligence and covert) authorities that exist under the Unified Command Plan. Because of this expanding controversy, there is a growing chorus calling for a split between the National Security Agency (NSA) and US Cyber Command.

These debates are important. Yet they subsume the pivotal issue —how cyber components and capabilities will affect US national security—beneath more transient legal and political issues generated in the wake of Edward Snowden. Furthermore, past and current debates often overlook a basic truth: battlefield outcomes and strategic effects are the product of *actual* force employment, not theoretical arguments or proving-ground tests.

Cyber Command should be cleaved from NSA, but not for reasons of political expediency. Cyber Command should be split from NSA because the United States needs an organizational arrangement that provides for the development and normalization of Title 10 and Title 50 cyber capabilities, while maintaining a focus on how such will affect the use of military force and US national security. Cyber Command should be split from the NSA because nations that marshal and mobilize their cyber power and integrate it into strategy and doctrine will ensure significant national security advantage, and Cyber Command currently provides the best route for achieving such.[2]

Cyber Command should be removed from under US Strategic Command and established as a unified combatant command. That action

1 The debate began with John Arquilla and David Ronfeldt, "Cyberwar is Coming!" *Comparative Strategy* 12, no. 2 (Spring 1993): 141-165. The phrase "cyber components and capabilities" is used to denote computer network attacks (CNA), computer network exploits (CNE), and computer network operations (CNO), as well as future developments both within and beyond these categories.

2 Frank J. Cilluffo and J. Richard Knop, "Getting Serious About Cyberwarfare," *The Journal of International Security Affairs* (New York: Jewish Institute for National Security Affairs, 2009).

represents the most effective means for developing and maturing the tactics, techniques, and procedures that will allow US cyber components and capabilities to be employed for military purposes and to generate strategic effects. Currently, there are two primary reasons why the establishment of a unified combatant command presents a better solution than tasking existing branch and service structures. First, speed is of the essence. Tasking an existing branch or service, or even establishing a new service, would open up organizational and bureaucratic rivalries likely to slow (if not cripple) the development of cyber components and capabilities. Second, in the near term, Title 10 and Title 50 concerns, vagueness in the cyber rules of engagement, concerns about political blowback, and fears that US cyber weapons could be reverse engineered and used against the United States, all highlight the importance of an organizational solution that synchronizes and deconflicts activities across the whole of government. In short, the United States needs a combatant command that can do two things: (1) craft the tactical, operational, and strategic cyber capabilities US national security will need in the decades to come; and, (2) oversee their application, integration, and execution. Cyber Command is the best choice and now is the time to act.

Operationalizing Cyber

When Cyber Command was established in 2009, it made sense that it be stood up as a sub-unified command under Strategic Command. Until recently the line between computer network attacks and computer network exploits was chiefly one of intent (i.e., if you had the ability to exploit, you had the ability to attack). The use of cyber was largely constrained to information collection and intelligence. Kinetic effects and battlefield uses were essentially theoretical, not practical. In addition, because of the scarcity of manpower and materials, it made sense that Cyber Command and the NSA be joined by the dual-hatting of their commander, General Keith Alexander. This allowed the two organizations to pool resources and avoid redundancy.

Today, the situation is different. The kinetic potential of cyber components and capabilities have been demonstrated, attempts to employ them for strategic effect have been undertaken. The use of cyber in support of operational or strategic objectives is becoming increasingly common. Three examples in a growing universe of cases illustrate this point. The 2009 Stuxnet attack against Iran's nuclear-fuel centrifuges temporarily halted Tehran's enrichment program. The 2011 distributed denial of service attacks against government and media websites slowed the counterconcentration of Georgian forces in response to Russia's military invasion.[3] The 2012 distributed denial of service attacks against American banks, launched in retaliation for the US-led sanctions against Iran, exposed a weak point that potentially could be used to coerce the US government.[4]

These cases suggest future conflicts will contain cyber elements at both the operational and strategic levels. Such is the new reality. Regardless of asymmetries in other capabilities, cyber components and capabilities

3 David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, January 6, 2011, http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008.

4 Richard Davies, "Iran Suspected in Bank Site Hacking," *ABC News*, January 9, 2013, http://abcnews.go.com/blogs/business/2013/01/iran-suspected-in-bank-site-hacking/

are now part of the battlefield and the strategic environment writ large. At the same time, there are important differences between the use of tactical and operational level cyber in conjunction with activities on the physical domains, and strategic activities occurring solely within the cyber domain itself. The result is a growing divergence between the missions of the NSA and Cyber Command—as well as a growing divergence in the skills and capabilities each needs to fulfill its respective mission.

The increasing use of cyber at the operational and strategic levels creates impetus for all military forces, from those of powerful nation-states to those of weak insurgent movements, to acquire cyber components and capabilities. Cyber is not an instrument of the weak or the strong, it is an instrument—period. It is becoming conventional wisdom that "the ability to use cyberspace to create advantages and influence events in all other operational environments and across the instruments of power" will ensure significant advantage.[5] America's adversaries are preparing for the operationalization of this conventional wisdom; the United States must do so as well.

Still, the acquisition of new technologies is not enough. Stephen Biddle argues that technology magnifies the effects of force employment.[6] Technology makes capable forces more capable. If integrated properly, technology enhances how military units execute or react to actions born out of the principles of war: mass, maneuver, surprise, security, simplicity, objective, offensive, economy of force, and unity of command. Biddle warns, however, that technology is not a substitute for good force employment. It will not make a "bad" force better.[7] This suggests that if cyber components and capabilities are to have actual strategic effect, careful thought must be given to their application, integration, and execution. What is needed is an entity that can:

- Think through these issues in regard to computer network attacks and the defense of Department of Defense (DOD) systems.
- Mature the cyber components themselves as well as the tactics, techniques, and procedures for their use.
- Deconflict efforts across the whole of the US government.

Cyber Command represents the best entity for accomplishing all of the above.

To allow Cyber Command to fulfill these roles, the Unified Command Plan should be modified. Cyber Command should be cleaved from the NSA, taken out from under Strategic Command, and established as a functional combatant command. Cyber Command, like US Special Operations Command, should receive direct Congressional funding as a major force program, with the services free to make additional investments (as they do with Special Operations Command).[8] Unlike Special Operations Command, Cyber Command should have

5 Franklin Framer, Stuart Starr, and Larry Wentz, *Cyberpower and National Security* (Washington, DC: National Defense University, 2009); Cilluffo and Knop, "Getting Serious About Cyberwarfare."

6 Stephen Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle* (Princeton, NJ: Princeton University Press, 2004), 146.

7 Ibid., 164.

8 Eric Olson, "The Future of Special Operations: Proposed Changes in the Unified Command Plan," Comments at the *Global Security Forum* (Washington, DC: Center for Strategic and International Studies, 2012).

operational authority and the ability to initiate a request that forces be attached to a geographic combatant command in response to identified threats. In short, it is time to let Cyber Command come into its own.

At present Cyber Command exists, much as Special Operations Command did in the wake of the 9/11 attacks, in the organizational shadows unable to contribute its full potential to the security of the United States. Establishing Cyber Command as a combatant command would allow it to leverage its existing capabilities and organizational relationships to develop US cyber capabilities through the fulfillment of two missions. One mission would be to act as an incubator for operational cyber capabilities. The other mission would be to act as *the* designated operator for offensive actions within the cyber domain itself.

In its incubator role, Cyber Command should act as facilitator for the development of cyber components and capabilities to enhance modern force employment and integrate cyber components and capabilities into the combined arms framework. In this role, Cyber Command should work with the Defense Advanced Research Projects Agency (DARPA), the services' various combat training directorates, academic programs, and other private and public sector entities. Cyber Command would, as the other combatant commands do, task the NSA for information and capabilities in support of its primary mission. The goal would be to develop, demonstrate, and disseminate capabilities for cyber enhanced combat operations on the terrain of the physical domains. Cyber Command should act as a client and partner for activities such as DARPA's Project X, which seeks to map enemy networks, develop mission scripts for the use of cyberweapons, and develop techniques for assessing battle damage to cyber components and capabilities.[9] Cyber Command should act as a repository for lessons learned about the operational employment of cyber and the lead for activities regarding how cyber components and capabilities should be folded into the Joint Munitions Impact Modeling System (JMIMs). Cyber Command would then be able to provide war planners with more robust tools for understanding the likely effects of cyber attacks, yielding as much confidence about the effects of computer network attacks, as about the use of traditional munitions. Its incubator role would allow Cyber Command to refine tactics, techniques, and procedures based on actual battlefield experiences—including those from the use of cyber in Afghanistan—so that cyber is operationalized on the basis of combat experience rather than just theoretical or proving-ground tests.[10] In short, Cyber Command should be charged with finding out how US forces could employ cyber to better execute the principles of war within mission, enemy, terrain, troops, time, and civilian (METT-TC) constraints.

In its operational role, Cyber Command should remain the entity for operations that occur within the networks and systems that make up cyberspace. In fact, Cyber Command ought be designated at *the* combatant command for the cyber domain. It should *own* all offensive or defensive cyberborne operations not related to intelligence collection.

---

9 Tom Gjelten, "First Strike: US Cyber Warriors Seize the Offensive," *World Affairs* (January/February 2013), http://www.worldaffairsjournal.org/article/first-strike-us-cyber-warriors-seize-offensive.

10 Sterling C. Beard, "Marine officer says US using cyberwarfare in Afghanistan," *The Hill* (Washington, DC: Capitol Hill Publishing Corporation, August 24, 2012), http://thehill.com/blogs/defcon-hill/marine-corps/245421-marine-officer-says-us-using-cyberwarfare-in-afghanistan.

Making one entity responsible for the use of components and capabilities in the cyber domain will protect American assets. It will ensure their cautious use, reducing opportunities adversaries might have to copy and reverse engineer them.[11] Cyber Command should continue to field cyberwarfare teams, like those General Alexander discussed before the Senate Armed Services Committee in March 2013.[12] Cyber Command, through a sub-unified command within it, should play a role analogous to the one Joint Special Operations Command (JSOC) plays in regard to counterterrorism. Once the intelligence community identifies a target and the national command authority makes the decision to act, Cyber Command should "pull the trigger." To ensure accountability and deconflict efforts across the whole of the US government, this process should occur through a Title 10 and Title 50 synchronization process similar to that of JSOC. Cyber Command should have responsibility for this process, and then responsibility for implementing computer network attacks. Cyber Command should continue to be responsible for synchronizing and coordinating the actions of the service components: US Army Cyber Command, the US 10th Fleet, the 24th Air Force, US Marine Corps Force Cyber Command, and US Coast Guard Cyber Command.[13] This operational role, in addition to being vital in itself, would support Cyber Command's incubator mission through the constant development of new cyber components, capabilities, and skill sets.

Making the above happen requires a greater division of labor between the NSA and Cyber Command. The use of cyber as an intelligence asset should be separated from the use of cyber as a military asset. The NSA should continue to be responsible for and have authority to execute cyberborne operations related to intelligence collection. More specifically, the NSA should continue to be responsible for capturing information from potential or existent US adversaries via computer networks and operations; and support efforts to protect American networks from similar attempts on the part of foreign governments, criminal organizations, and others. In essence, this separation would make Cyber Command responsible for Strategic Initiative 1 and the NSA for Strategic Initiative 2, with each entity taking responsibility

11 Frank J. Cilluffo and Sharon L. Cardash, "Cyber Domain Conflict in the 21st Century," *The Whitehead Journal of Diplomacy and International Relations* 14, no. 1 (January 2013).

12 Richard Lardner, "US forming cyber teams to take offensive," *The Boston Globe*, March 13, 2013. http://www.bostonglobe.com/news/nation/2013/03/12/pentagon-forming-cyber-teams-prevent-attacks/UcUxkq95wj2FCXTQ3LJsvM/story.html.

13 United States Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Arlington, VA: United States Department of Defense), 5, http://www.defense.gov/news/d20110714cyber.pdf.

for the remaining three as outlined in the July 2011 "Department of Defense Strategy for Operating in Cyberspace":

- *Strategic Initiative 1.* "Treat cyberspace as an operational domain to organize, train, and equip so that [DOD] can take full advantage of cyberspace's potential."
- *Strategic Initiative 2.* "Employ new defense operating concepts to protect [DOD] networks and systems."
- *Strategic Initiative 3.* "Partner with other [US] government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy."
- *Strategic Initiative 4.* "Build robust relationships with [US] allies and international partners to strengthen collective cybersecurity."
- *Strategic Initiative 5.* "Leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation."

This division would allow each entity to develop and refine the particular cyber techniques and skills most likely to bring about success within their respective realms.

The need to separate Cyber Command from NSA, and to establish it as a functional combatant command goes beyond force employment or operations within the cyber domain onto itself. Cleaving Cyber Command from NSA also addresses the need to balance (and rebalance) Title 10 and Title 50 authorities. The convergence of traditional military missions with intelligence and covert action is not new. General Edward Meyer, Army Chief of Staff from 1979 to 1983, recognized the need for such. General Meyer argued that America's "adversaries were affecting us below the threshold of war," necessitating the development of new capabilities. The result was the birth of special operations as a community that could blend combat capabilities, intelligence, and covert action. In response to world events of the last three decades—including the Iranian hostage crisis, the rise of Hezbollah and the bombing of the Marine barracks in Beirut, and later al Qaeda and 9/11—this convergence of military, intelligence, and covert activities has continued. Yet, in some areas, even when operationally necessary, convergence has clouded authorities. It has made it unclear as to which parts of the government are responsible and accountable for various actions. Given how they permeate modern life, cyber components and capabilities raise new issues. Cyber adds concerns about privacy to those about force employment and intelligence. Separating Cyber Command from NSA would support the synchronization of Title 10 and Title 50, where necessary, and alleviate privacy concerns by clarifying the authorities for conducting various cyber operations within specific contexts.[14]

Three additional issues must be resolved to establish Cyber Command as a functional combatant command charged with maturing the US cyber capabilities and executing operations within the cyber domain.

14 Robert Chesney, "Military-Intelligence Convergence and the Law of Title 10/Title 50 Debate." *Public Law and Legal Theory Research Paper Series Number 212*, (Austin, TX: The University of Texas School of Law, October 17, 2011), http://ssrn.com/abstract=1945392; Andru Wall, "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action." *Harvard National Security Journal* 3, no. 1 (Cambridge, MA: Harvard University, 2011), http://harvardnsj.org/wp-content/uploads/2012/01/Vol.-3_Wall1.pdf.

First, Cyber Command must have budgetary independence to ensure its needs are not squeezed out by bureaucratic competition with the service components, other combatant commands, or weapons systems. For this reason, Cyber Command should receive direct funding from Congress as a major force program. The other services should be free to make investments in Cyber Command, but the command must have a budget insulated from the concerns or needs of the services themselves, the other combatant commands, or the DOD itself. Second, unlike Special Operations Command, Cyber Command must be granted the ability to initiate a request that specific cyber components and capabilities be attached to geographic combatant commands in response to identified threats. Because of the unique nature of Cyber Command's expertise, especially in the near term, the command is likely to possess greater understanding of the cyber threats and opportunities faced by other combatant commands. The fulfillment of such requests should require input from the receiving command before being decided by the national command authority. Third, Congress and the executive branch must make significant investments in the personnel needs of both NSA and Cyber Command. The size of the cyber work force should be increased, and training of individuals tailored to the missions and requirements of their respective command. It is imperative that Congress and the executive branch supply the resources necessary to accomplish this. The United States must avoid a situation in which Cyber Command and the NSA are left operationally anemic by a lack of qualified personnel and a need to compete with one another for the highly skilled individuals each needs to fulfill their respective missions.

Today, there are three broad reasons to undertake the above proposal. First, it would facilitate the integration of cyber components and capabilities into the combined arms framework, and provide an effective mechanism for the crafting of cyber tactics, techniques, and procedures. Second, it represents the most efficient, and most likely, path for achieving the strategic initiatives outlined in the 2011 Department of Defense Strategy for Operating in Cyberspace.[15] Third, it keeps cybersecurity discussions, policy, and practice focused on the fact that the central issues—even in regard to the potential for cyberwarfare—are inherently about grand strategy and human conflict, not technical capability.

To be clear, the establishment of Cyber Command as a functional combatant command does not represent a panacea. It leaves unaddressed important issues regarding the security of the US private sector cyber assets and resources, including jurisdictional issues among the NSA, the Department of Homeland Security, and the Federal Bureau of Investigation. It also leaves unaddressed important issues about the rights and responsibilities of the US private sector regarding the ability to engage in the active defense of their computer networks and systems from the efforts of organized crime, foreign attacks, and state-sponsored espionage. Still, doing so represents the best means (at present) for developing and normalizing Title 10 and Title 50 cyber capabilities for offensive action and in defense of DOD computer networks and systems. It also represents the logical mechanism for attempting to

15 *Department of Defense Strategy for Operating in Cyberspace.*

achieve the Presidential Policy Directive-20 goal of using cyber to dissuade, deter, or compel US adversaries.[16]

Conclusion

It is critically important that the United States act now to integrate cyber fully into operational level force employment. Evidence suggests America's adversaries are doing just that. Given America's greater reliance on cyber, and thus greater vulnerability, US national security necessitates it maintain a dominant position in regard to cyber. Dominance comes through application, integration, and execution. At this point, the United States needs to designate one entity to take lead in the development and maturing of the tactics, techniques, and procedures that will allow cyber components and capabilities to be employed for military purposes, establish dominance, and generate strategic effects. For these reasons, it is time to establish Cyber Command as a functional combatant command.

Frank J. Cilluffo

Mr. Cilluffo is an Associate Vice President at George Washington University where he directs university-wide Cybersecurity Initiative and the Homeland Security Policy Institute. He previously served as Special Assistant to President George W. Bush for Homeland Security.

Joseph R. Clark

Dr. Clark is a policy analyst at The George Washington University's Homeland Security Policy Institute and Adjunct Professor at Virginia Commonwealth University.

16 Robert O'Harrow and Barton Gellman, "Secret cyber directive calls for ability to attack without warning," *The Washington Post*, June 7, 2013, http://articles.washingtonpost.com/2013-06-07/world/39817439_1_cyber-tools-president-obama-directive.