Time for a U.S. Cyber Force | U.S. Naval Institute
www.usni.org

Instead of each armed service having its own version of a cyber command, why not create a separate entity altogether that would serve all branches?

In November 1918, U.S. Army Brigadier General Billy Mitchell made the following observation: "The day has passed when armies of the ground or navies of the sea can be the arbiter of a nation's destiny in war." General Mitchell's comments came in the context of a vigorous debate involving a then-new domain of warfare: the skies. Nearly a century later, we are confronted with yet another contested domain. Cyberspace, like airspace, constitutes a vital operational venue for the U.S. military. Accordingly, it warrants what the sea, air, and land each have—an independent branch of the armed services.

Eight months before Mitchell's clairvoyant statement, President Woodrow Wilson had signed two executive orders to establish the U.S. Army Air Service, replacing the Aviation Section of the U.S. Signal Corps as the military's aerial warfare unit. This small force served as a temporary branch of the War Department during World War I and looked much like the Pentagon's joint task forces of today. It was relatively small and consisted of personnel on assignment from the different services. In 1920, the Air Service's personnel were recommissioned into the Army. The decision was backed by the popular belief that aviation existed exclusively to support ground troops.

A significant debate was under way within the armed services. The minority camp, led by Mitchell, advocated on behalf of establishing an independent service for aerial warfare. He contended that air power would serve a purpose beyond supporting the Army's ground movements, and that gaining and maintaining preeminence of the skies required an entirely autonomous branch with indigenous manning, personnel, logistics, and acquisition duties. His opponents, on the other hand, favored integrating aviation into the existing services. Budgets were tight, and Army brass were eager to garner additional funding streams.

Ultimately, the politics of the day prevailed, and the Army's forceful lobby succeeded in preserving the status quo. Mitchell was court-martialed and subsequently demoted for insubordination, and in 1926 the Air Corps Act created the U.S. Army Air Corps. The legislation mandated few substantive reforms, but nonetheless solidified the Army's control over military aviation, ostensibly ending the debate for two decades. Mitchell's wisdom prevailed 20 years later when President Harry S. Truman signed the National Security Act of 1947. The postwar legislation created the Department of the Air Force and at 65 years old, that force is the most formidable aerial warfare branch in the world.

Today we find ourselves in an almost identical situation with cyberspace. In 2005, the Pentagon reacted to the emerging virtual domain by establishing a joint task force of sorts, much like the old Signal Corps. Known as the Joint Functional Component Command for Network Warfare, it was tasked with "facilitat[ing] cooperative engagement with other national entities in computer defense and offensive information warfare." The Fort Meade–based unit sequestered personnel from the Army, Navy, Marine Corps, Air Force, and Coast Guard to support its mission.

A year later, the Air Force took a page from the Army's 1920 playbook and established its own cyber headquarters. The Air Force Cyber Command's mission statement described it as a "provider of forces that the President, combatant commanders, and the American people can rely on for preserving the freedom of access and commerce in . . . cyberspace." Unlike the Army of the 1920s, though, the Air Force lost the bureaucratic battle for control of cyberspace. In 2008, the Defense Department denied its permanent activation in favor of a joint organization, and in 2010 the Pentagon officially stood up the U.S. Cyber Command (CYBERCOM) and designated it at initial operational capability status. Most recently, in September 2013, CYBERCOM activated the Cyber Mission Force, which is composed of the National Missions Teams, Combat Mission Teams, and Cyber Protection Teams—all of which have different missions and will be staffed by the five services.

Currently, each of the five services possesses a cyber component. For example, the Navy has Fleet Cyber Command, the Air Force has Air Force Cyber Command, and the Marine Corps has Marine Forces Cyber Command. The Army and Coast Guard also have similar units. Each component, although technically subordinate to CYBERCOM, supports service and joint missions. In other words, Fleet Cyber Command answers to both the Chief of Naval Operations and the CYBERCOM commander. When push comes to shove, though, the Navy dictates the criterion by which the 10th Fleet manages its cyber sailors. After all, the Navy, not CYBERCOM, is footing the bill.

Not only does this construct threaten unity of command and foster at times unhealthy competition among the services, but it also inhibits the establishment of universal standards that transcend the DOD's cyber community. With so many different appropriation vehicles, CYBERCOM lacks sufficient influence over the services' priorities, and in the event that CYBERCOM and its components do not share mission interests, conflicts inevitably arise. A stand-alone force would eliminate both the unity-of-command problem and the interservice rivalries. It would prevent the inefficiencies associated with disparate personnel standards while allocating resources based on objectively adjudicated priorities.

Some supporters of CYBERCOM's organizational structure cite U.S. Special Operations Command, or SOCOM, as a replicable model. Like CYBERCOM, SOCOM is a functional (as opposed to geographic) command with representation from all five services. Put simply, if CYBERCOM's function is cyberspace operations, then SOCOM's function is special operations. The problem with drawing parallels between the two, however, is that SOCOM's functions span multiple domains, whereas CYBERCOM's functions only involve one domain—cyberspace. Therefore, SOCOM indeed requires the core competencies of all the services to carry out its missions in the sea, air, and on land. Cyberspace operations, by contrast, do not require any of the core competencies of the five services; in fact, the cyber domain requires precisely the core competencies that none of the other branches possesses.

Despite their differences, an independent cyber branch could be positively informed by the experience of SOCOM. SOCOM's official history cites the opposition of Admiral William Crowe, then Chairman of the Joint Chiefs of Staff, to a combatant command specifically dedicated to special operations. Furthermore, special operators have navigated an interagency environment alongside intelligence-community counterparts since their founding. Those who fear redundancy between a distinct cyber branch within

the armed services and its closest intelligence-community partner, the National Security Agency (NSA), should look no further than SOCOM's relationship with the Central Intelligence Agency (CIA). While military special operators have established their own organic intelligence-gathering capabilities, and the CIA has recently enhanced its kinetic capabilities, the two organizations enjoy a mutually symbiotic relationship. Further, a dedicated cyber branch would assuage the tension that SOCOM endures between administrative and operational control of its personnel. In this respect, a single branch for cyber warfare would better facilitate manning, training, and equipping forces for the conduct of operations.

Operational art is achieved through the convergence of otherwise opposing worldviews. The joint environment facilitates this healthy ideological clash by mandating the cohabitation of diverse military disciplines for the purpose of tactical, operational, and strategic planning. Wargaming, course-of-action development, center-of-gravity analysis, and strategic design are most effective with a room full of different-colored uniforms. Currently, in the joint world, the Army offers its perspective from land operations, just as the Navy does the sea and the Air Force the air. This forced meshing of domain-related views has proven highly valuable for meeting combatant commanders' intent for planning in all domains. Anyone who has worked in a joint environment—from the Joint Staff scripting strategic doctrine down to a Joint Operations Center churning out tactical orders—would agree that intellectual diversity is paramount to mission success.

The problem, however, is that no one service specializes in cyberspace operations. Because cyberspace is now an established military domain, combatant commanders are eager to integrate a new institutional perspective into military plans. Today, cyber planners from the Army, Navy, Marine Corps, Air Force, and Coast Guard fill the institutional gap. At a time when the doctrine for cyberspace operations is still immature, these personnel are not only ideologically biased by their operational past—be it on land, at sea, or in air—but they are also extremely new to the domain. In this respect, as long as America's cyber warriors belong to big Army, Navy, or Air Force, they will always be at least partially influenced by their experiences in another domain, thus depriving joint operations of an institutionally untainted warfighter. Further, having cyber assets in each branch produces unnecessary redundancy; in an era of increasing threats amidst austerity, having a branch dedicated to cyber with streamlined financial accountability makes economic sense. Cyber warriors across the military equipped with institutional cohesion amongst one another better serves U.S. national-security objectives than those same cyber warriors maintaining institutional allegiance to an existing branch.

Before we can fully modernize the joint environment, though, it is critical to recruit and train America's military to operate on the 21st century's digital battlefield. As with any battlespace, the case for a U.S. Cyber Force starts with people—and America's cyber warriors demand more than just their own uniforms. Perhaps surprisingly, the vast majority of CYBERCOM's military personnel are experiencing cyberspace for the first time in their careers. Helicopter pilots, chemical officers, B-2 navigators, tank drivers, infantry soldiers, and acquisition specialists occupy CYBERCOM's ranks. These personnel enter the cyber trenches at all levels of leadership with little to no related experience, so the command invests heavily in expensive training regimens to mitigate gaping proficiency holes. The long-term return on investment is strikingly minimal, however, as most personnel rotate out after three years to an entirely different discipline.

The lucky few who received prior training from their respective branches are typically influenced by their service's legacy doctrine, thus inducing confusion among the joint ranks. For example, cyber soldiers typically default to information-operations doctrine, whereas cyber sailors often view cyberspace operations through the lens of electronic warfare.

In addition to military personnel, civilians also occupy the cyber trenches. While the Air Force failed to take ownership of the cyber domain in 2008, it did gain the majority stake of civilian personnel management. Through no fault of its own, though, the Air Force lacks the requisite human-resources capacity to acquire and retain the nation's best technical talent. Doing so necessitates an effective advertising effort to build and market a brand that attracts an entirely different civilian than the Air Force is accustomed to targeting. To compete with the private sector in an increasingly lucrative field, the DOD must offer attractive incentives. In this respect, the Pentagon's uptight and hierarchical culture is hardly preferable to the free-spirited and flat cultures that characterize the sunny offices of Palo Alto's technology start-ups. Today, the Air Force does not even offer Senior Executive Service (the civilian equivalent to generals and admirals) positions at CYBERCOM, so upward mobility is capped.

Recruiting the appropriate military personnel is equally important. "The Few, The Proud, The Marines," is a great slogan for attracting young infantry candidates seeking to tackle a specific mission and share in a storied heritage of elite warriors, but it hardly appeals to the wily hacker types who must populate the cyber trenches. Therefore, the Corps' cyber component, Marine Forces Cyber Command, is compelled to choose cyber warriors from among its existing ranks of Devil Dogs—the same Marines who were enticed to enlist by flashy television commercials of men in dapper uniforms donning shiny swords. As a general proposition,

Marines are of course much more accustomed to navigating amphibious terrain than global highways of fiber-optic cables or the Washington Beltway's network of bureaucrats. Imagine, though, if the U.S. Cyber Force landed a commercial spot during the Super Bowl—or better yet, an advertising deal with World of Warcraft? How about 30-second ads on YouTube videos from the Black Hat hacker convention? Even Don Draper of Mad Men fame could not resist the creative potential of such a brand. Today, CYBERCOM does not even have a public-facing website, let alone a Twitter or Facebook account to target the 20-somethings who never knew a world without computers. Only a new service is capable of generating enough brand appeal to recruit and retain America's next-generation warfighter.

The U.S. Cyber Force would be a drastic but timely innovation for America's military. A dedicated branch would be smaller in size than the Marine Corps with comparatively low physical-fitness standards and noticeably relaxed grooming standards. Make no mistake about it, America's cyber warriors would not bear the likeness of G.I. Joe. The uniform of the day might resemble that of a conservatively dressed Googler—the branch's motto artfully inscribed across the chest in MD5 hash.

With the other services looking to downsize, technically apt military personnel would get first dibs on populating the new ranks. In addition to absorbing existing people, raising the new cyber branch's profile would attract a diverse pool of patriotic technologists, ranging from high school hackers to Silicon Valley's computer scientists. The cyber trenches must include pure geeks, with an unparalleled command of coding, and

emotionally intelligent social scientists who are equally comfortable with technology and policy. Operating in cyberspace necessitates deft maneuvering to navigate the dizzying ambiguities of a virtual domain while overcoming the stifling stovepipes of Washington's bureaucratic behemoths. Shunning divergent personalities from the military apparatus is a parasitic posture; by engendering commonality in wearing the cloth of our nation, all military branches will be better suited to integrate cyberspace capabilities. Accordingly, the U.S. Cyber Force's non-techies are critical to facilitating the convergence of intellectually divergent disciplines, each of which is collectively indispensable to advancing the America's interests in cyberspace.

As with any major organizational revision, the skeptics will inevitably voice concerns. Antiwar activists will warn of provoking the militarization of cyberspace, and privacy advocates will object on the basis of recent accusations of domestic surveillance. Other opponents will tacitly acknowledge the sound logic but will be intimidated by the daunting prospect of change. In reality, the path to a new service would be gradual. The next logical step is dividing the bureaucratic relationship between CYBERCOM and NSA, principally by appointing exclusive leaders for each organization and then cementing the command's autonomy by granting it unified combatant command status, thereby releasing it from the oversight of the Omaha-based U.S. Strategic Command. A fully empowered and independent functional combatant command is a halfway house on the way to an independent service branch.

Of course, the U.S. Cyber Force's mission would be strictly governed by the longstanding tenets of the Posse Comitatus Act, just like any other branch of the armed services. In fact, establishing a distinct cyber service with less institutional ties to the NSA would go a long way toward allaying the concerns of civil libertarians by bringing greater transparency to the cyber domain and subjecting the service to a whole host of oversight mechanisms, as well as more clearly delineated funding streams. As far as domestic cyberspace is concerned, the U.S. Cyber Force would have no jurisdiction whatsoever in the United States; in fact, perhaps it's time to learn from aviation again and consider modeling a domestic cyber-security agency on the Federal Aviation Administration.

Military institutions do not dictate the degree to which a domain constitutes a venue for warfare; rather, militaries merely react logically to changes in state and non-state behavior. In the case of both airspace and cyberspace, technological innovation was the primary driver of behavioral change. With the advent of the Internet and the proliferation of hyper-connected technologies, we are once again on the beach at Kitty Hawk. The Wright Brothers spent three years there experimenting with flight and now, more than three years after then-Secretary of Defense Robert Gates commissioned the U.S. Cyber Command, it is time to think ahead. Thankfully, Brigadier General Billy Mitchell's wisdom extends beyond just airspace; it pertains to all domains of warfare. Let's not wait 20 years to realize it.

Admiral Stavridis completed four years as Supreme Allied Commander at NATO in mid-2013, and is today the Dean of the Fletcher School at Tufts University.

Mr. Weinstein just completed three years as a Strategic Planner at U.S. Cyber Command.