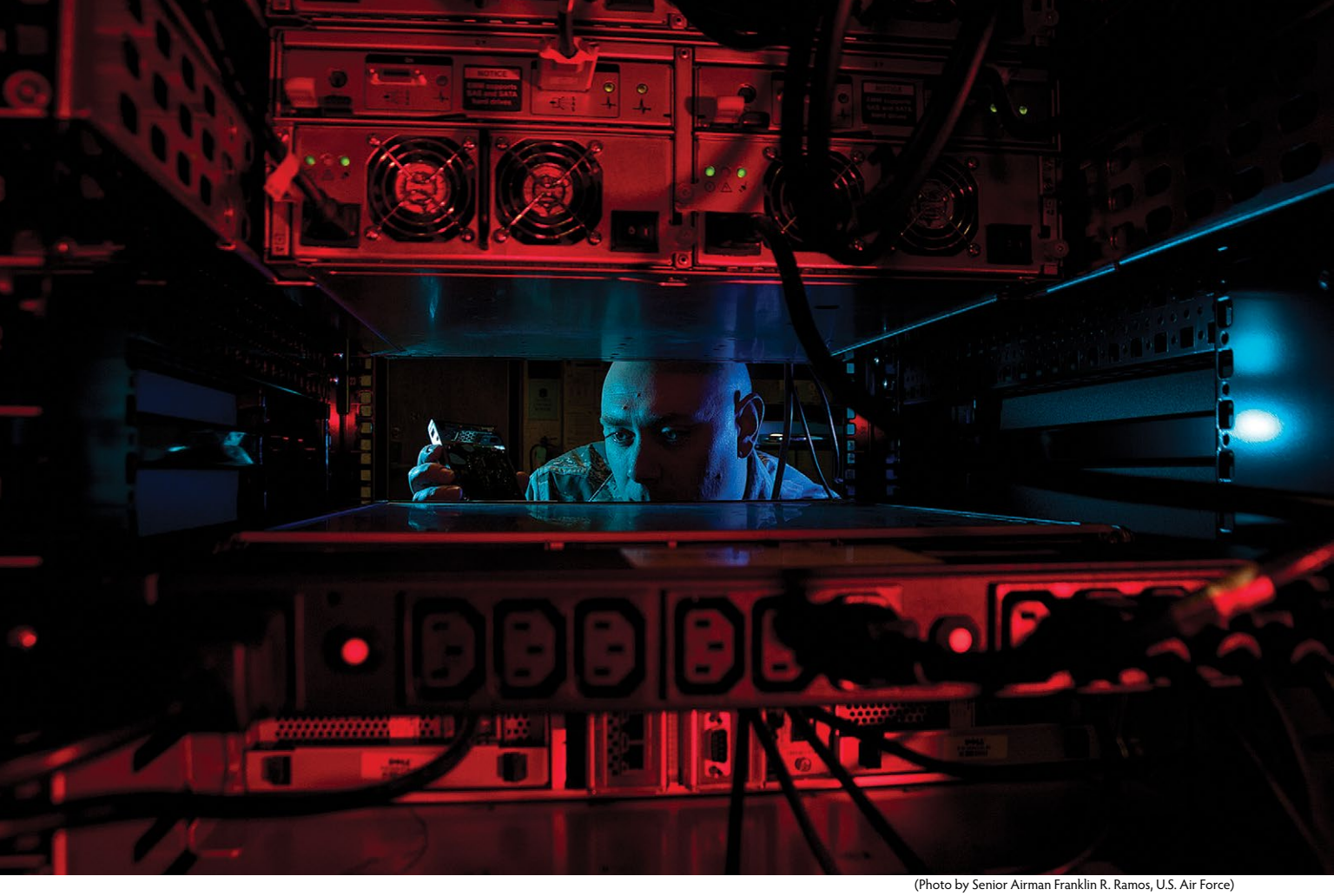


(Photo by Senior Airman Franklin R. Ramos, U.S. Air Force)

U.S. Air Force Staff Sgt. Jerome Duhan, a network administrator with the 97th Communications Squadron, inserts a hard drive into the network control center retina server 24 January 2014 at Altus Air Force Base, Oklahoma, in preparation for a command cyber readiness inspection.

U.S. Cyber Force
One War Away

Maj. Matt Graham, U.S. Army

In *Wealth of Nations*, published in 1776, Adam Smith explains how division of labor allows the greatest efficiency: farmers focus on producing food, blacksmiths focus on crafting goods from metal, and so on.[1] The principle still holds true today; individuals and organizations develop expertise by focusing on a single activity. In the U.S. military, the division of labor between armed services accomplishes this expertise: the Air Force concentrates on air superiority, allowing the Army to focus on land warfare and the Navy to concern itself with maritime combat. The Marine Corps develops its expertise in bridging the gap between land and sea.

Although it possesses some very different characteristics from the physical domains, cyberspace has recently emerged as an independent domain that requires its own particular military expertise. With nations seeking advantages in this new domain, competition within cyberspace has assumed many of the traits of warfare, and

it now requires the same level of expertise as is needed to win wars in the physical world. The military needs an independent U.S. Cyber Force, coequal with the Army, Navy, Air Force, and Marine Corps, to focus on the cyberspace domain.

Current Approach to Cyberspace

The military has not been idle during the advent and development of cyberspace and cyber warfare. The Department of Defense (DOD) established the U.S. Cyber Command (USCYBERCOM) in 2009 as a joint headquarters to orchestrate the cyberspace efforts of the department. Members from each armed service come together within USCYBERCOM to address cyberspace threats. A portion of the DOD budget is directly allocated to USCYBERCOM, and some of its resources come through the armed services. Under USCYBERCOM, each service established a component headquarters (e.g., Army Cyber Command or Fleet Cyber Command) to support the DOD's efforts in cyberspace. The emerging importance of cyberspace certainly warrants each of these actions. However, each armed service devoting a fraction of its attention to cyberspace guarantees two outcomes: the services are distracted from their traditional combat roles in the physical domains, and cyberspace efforts are inefficient (at best), disjointed (likely), or fratricidal (at worst). Currently, this inefficiency is not a major concern and results primarily in bureaucratic frustration. However, when the stakes are higher and U.S. cyberwarriors must prove better than the adversaries' cyberwarriors, these inefficiencies will not be tolerable.

The current approach (with each armed service anteing up to the joint cyberspace effort) is not only inefficient, but it is also unnecessary. A cyberspace operation is largely independent of the platform or physical domain from which a cyberwarrior accesses cyberspace. The logic employed or network vulnerability exploited by a cyberwarrior is the same whether executed from the bridge of an aircraft carrier, the belly of a command-and-control aircraft, or a desk in an air-conditioned office park.

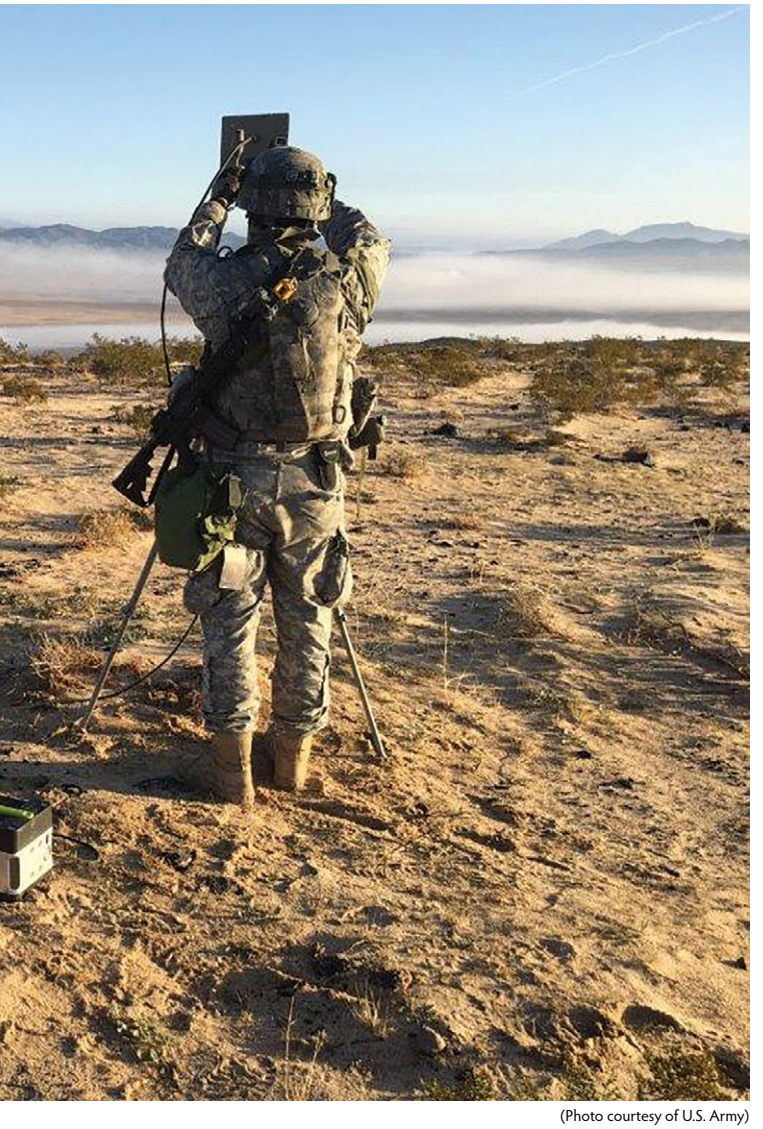
Decisive in a cyberspace operation is the exploitation of vulnerabilities in an adversary's system before the adversary can identify and mitigate them (and vice versa). When considered in this light, cyberwarriors from the Navy and Air Force share more similarities with their fellow cyberwarriors than with other sailors and airmen from their respective armed services.

The U.S. Cyber Force Would Provide Focus

In contrast to the approach the DOD is currently taking, an independent cyber service could provide the necessary level of concentration on cyberspace operations. Greater focus is required to build cyberspace competence throughout the military, and particular gains could be expected in three areas: developing leadership, building cyberwarriors, and operating within cyberspace.

Leadership. The U.S. Cyber Force would ensure the senior-most cyberspace leaders possessed a depth of

experience in cyberspace operations. Currently, senior officers within each of the armed services are promoted for performance in their service's domain (e.g., the Air Force's chief is a fighter pilot, and the chief of naval operations is a submarine officer). It is appropriate that these officers are experienced in their domain's warfare. They must communicate the challenges associated with their domains to political decision makers. These leaders then interpret political guidance and disseminate funding for their services. Who accomplishes this function for the cyberspace domain? The commander of USCYBERCOM currently advocates for cyberspace. However, USCYBERCOM is under U.S. Strategic Command (USSTRATCOM), several levels removed from political decision makers. Furthermore, the USCYBERCOM commander ascends to command from within one of the armed services, largely governed by officers who are focused on their specific physical domains. Since the services determine which officers are to be promoted, even the USCYBERCOM commander must split attention between cyberspace and the domain of his or her service or risk failure to advance. Establishing the Cyber Force, complete with its own member of the Joint Chiefs of Staff, would allow military leaders with experiential depth in cyberspace to effectively communicate the challenges of cyberwarfare to political decision makers. In turn, the Cyber Force leaders could efficiently employ the guidance and resources ascribed to military operations in cyberspace.



(Photo courtesy of U.S. Army)

Soldiers with the 780th Military Intelligence Brigade conduct cyberspace operations 24 January 2016 during a training rotation for the 2nd Stryker Brigade Combat Team, 2nd Infantry Division, at the National Training Center, Fort Irwin, California. The unit, based in Fort Meade, Maryland, was one of several cyber organizations that took part in the rotation as part of a pilot program designed to help the Army build and employ cyber capabilities in its tactical formations.

Cyberwarriors. Beyond developing experienced leaders for cyberwarfare, the Cyber Force would attract and develop better qualified cyberwarriors. Currently, civilians who want to defend the nation in cyberspace must choose one of the existing armed services and undergo its basic training curriculum. While those programs are exquisitely tailored toward producing soldiers, sailors, airmen, and marines, they may be unnecessary and daunting to civilians who merely want to engage in the predominantly mental competition of cyberwarfare. Certainly, DOD employs many civilians who are involved in cyberspace activities; however, this is a suboptimal solution. There are legal complications to civilians conducting warfare, and recruiting cyberwarriors as service members more accurately recognizes their contribution and allows for greater upward mobility and command. By establishing the Cyber Force, the military would appropriately recruit and categorize its cyberwarriors without dissuading interested civilians and influencing them to enter the lucrative computer or communications industries instead.

Training cyberwarriors would also become more efficient in the Cyber Force. Currently, each armed service is forming a training program for its respective cyberwarriors. For example, the Army established the Cyber Center of Excellence at Fort Gordon, Georgia. This distributed method for developing cyberwarriors nearly guarantees inefficiency for the larger DOD

cyberspace effort. Though USCYBERCOM is working to establish common standards for all armed services' cyberspace training, the armed services' interpretations will diverge, if only slightly. Professors at each of these centers will deliver unequal results. For example, the Army may hire the best computer code trainer, while the Marine Corps may hire the best network trainer. Despite common training standards, divergent interpretations and varying skills of instructors will produce cyberwarriors of suboptimal quality. Conversely, the Cyber Force could consolidate the best professors into a single cyberspace training center and better oversee the implementation of standards. Additionally, because students would be consolidated, the brightest would interact with each other, and the faculty would facilitate improved cyberspace research.

(Image courtesy of CERDEC)

The boundaries between traditional cyber threats and traditional electronic warfare threats have blurred. The U.S. Army Materiel Command's Communications-Electronics Research, Development, and Engineering Center (CERDEC) Integrated Cyber and Electronic Warfare program employs both cyber and electronic warfare capabilities as an integrated system to increase the commander's situational awareness.

Development continues beyond training. Assignments and practice pick up where training leaves off. As an independent service, the Cyber Force could skillfully tailor the career development of its cyberwarriors. Appropriate fields might be established (e.g., coding, networking, virus protection, or intrusion management), and career pathways might also be designed, including assignments in cyberspace units, in capability development agencies, and on joint staffs, where they can integrate cyberspace effects with operations in the physical domains. Currently, cyberwarriors are beholden to their services' human resources needs, and they often are seen as interchangeable with communications personnel. While there is certainly overlap between the fields of communications and cyberwarfare, a cyber force would enable better discernment of expertise and better management of human capital.

Operating within cyberspace. The primary advantage of establishing an independent Cyber Force is the ability to develop the most capable force. However, operating within cyberspace will also become less risky and more efficient. In the physical domains, it is relatively easy to divide the battlefield by physical location: the Army operates inland, the Navy operates at sea, the Marines operate in the littorals, and the Air Force in the sky. However, no such obvious boundaries exist in cyberspace, and all four armed services operate throughout it. The opportunity for one service to infringe on, or inadvertently sabotage, another's cyberspace operation is much greater than in the separate physical domains. The command-and-control burden and the risk of cyberspace fratricide increase with the number of cyberwarriors from four different services operating independently in the domain. Another consequence of four discrete cyberspace efforts is the potential for unintended redundancy (i.e., two services may commit resources to solving the same problem or developing the same capability). A joint oversight effort might reduce some redundancy, but more bureaucracy adds time and money to an already time-consuming capability development process. Removing the four armed services from the battle for cyberspace reduces the risk of their stepping on each other and wasting resources.

Advantages for the armed services. In *Good to Great*, Jim Collins modernizes some of Adam Smith's thoughts and notes successful businesses stick to their core concepts, foreswearing distractions. Collins offers

(Photo by Staff Sgt. Chuck Burden, U.S. Army)

U.S. Army Chief of Staff Gen. Mark Milley watches officers from the Army Cyber Institute 12 October 2015 at the U.S. Military Academy, West Point, New York, demonstrate taking down a drone with a cyber capability rifle.

three questions to help determine an enterprise's core concept: What are you deeply passionate about? What can you be the best in the world at? What drives your economic engine?[2] While the last question is difficult to translate for the public sector, the first two help illuminate why cyberspace should not be a core competency for the existing armed services. It is hard to imagine the Navy as the best in the world at cyberwarfare at the same time it is best in the world at maritime warfare. Similarly, few marines would describe themselves as deeply passionate about cyberwarfare. The delicate, distant nature of cyberwarfare conflicts with the Marine Corps' culture of up-close and personal fighting. By shedding the distraction of cyberwarfare and transferring it to the new Cyber Force, the current armed services maintain their focus on specific domains.

As a military service, the Cyber Force could provide forces to each of the combatant commands (CCMDs) in the form of a Cyber Service Component Command (CSCC). Just as the existing armed service components often serve dual-hatted as functional components (e.g., an Air Force service component command may also serve as a joint force air component command), the CSCC would shoulder the functional responsibilities of cyberwarfare. The Cyber Force could equip each of the geographical CCMDs with a CSCC focused on the systems of that CCMD's area of responsibility. USSTRATCOM's CSCC could serve as global synchronizer of threats that cross areas of responsibility, and U.S. Special Operations Command's (USSOCOM) CSCC might provide cyberwarriors capable of physical infiltration to achieve direct access to adversary closed-circuit systems. Though perhaps beyond the DOD's charter, U.S. Transportation Command's CSCC might aim to harden the cyberspace systems of key transportation partners (e.g., key commercial freightliners, air traffic controllers, or railroad partners), helping the joint force overcome anti-access challenges. Operating a cyber force is far simpler and more efficient than the existing services contributing forces to USCYBERCOM, which then must cobble together

cyber units and deliver them to the CCMDs.

Another approach to increase efficiency. A third approach, separate from the current DOD approach or a wholly independent cyber service, would involve promoting the current USCYBERCOM to a functional CCMD, on par with USSTRATCOM or USSOCOM. Elevating USCYBERCOM to a CCMD would be an appropriate, and likely, intermediate step to establishing the independent Cyber Force. This could remove one of the hierarchical layers between USCYBERCOM and political decision makers. Also, USSOCOM enjoys quite a bit of influence over the services' development of special operators. However, this arrangement solves only part of the problem. As a CCMD, USCYBERCOM would still be reliant on the existing services to conduct its operations. Cyberwarriors would still face the decision of which of the services' cyberspace pipelines to navigate on their way to working in USCYBERCOM. This arrangement works for USSOCOM because the training for an Air Force AC-130 pilot is different from that of a Navy SEAL, which is still different from developing an Army Special Forces soldier, but not so in cyberspace. A cyberspace operation is the same regardless of the physical domain from which it is launched. The solution that provides the DOD with the best-staffed, -trained, and -equipped cyberspace units is an independent cyberspace force.

(Photo courtesy of National Security Agency)

U.S. Cyber Command is located in Fort Meade, Maryland, along with the headquarters of the National Security Agency and the Central Security Service.

U.S. Cyber Force Establishment: After the Next War

With so many reasons supporting the establishment of the U.S. Cyber Force, what is stopping it? There are two major hurdles. First, cyberspace is still unproven as a combat zone in the thinking of many senior security leaders. Second, in the absence of an obvious significant security threat, the national security resources required for such a major overhaul will remain unavailable. The United States' next major conflict will likely eliminate both hurdles.

Proving cyberspace is a battle space. The air domain played a role in World War I. Observation balloons and dogfighting (aerial warfare à la the Red Baron) serve as the predominant aerial features of that conflict. However, the combatants of World War II truly grasped the significance of air superiority. The Battle of Britain, the allies' strategic bombing campaign, the advent of parachute units, and, ultimately, the bombings of Hiroshima and Nagasaki all demonstrated the importance of combat in the skies.

Currently, cyberspace resides in the type of limbo status air power occupied during the interwar years. Nonetheless, there have been a few isolated instances of state-on-state cyberwarfare. In April 2007, Russia conducted an effective denial-of-service attack on Estonia's

major networks, paralyzing many of that nation's economic and government functions.[3] Russia also attacked Georgia through cyberspace in conjunction with its 2008 invasion of South Ossetia.[4] Additionally, governments are using cyberspace to penetrate networks routinely, stealing missile plans, chemical formulas, and financial data.[5] However, similar to air power in 1920, cyberspace operations played a relatively small role in the United States' latest wars, and some skeptics still consider cyberspace a hobbyist's arena or *the domain you can turn off*.

Cyberspace activities increasingly impact the day-to-day operations of the U.S. military and the U.S. economy, along with the operations of its allies and adversaries (both state and nonstate). In the next war, cyberspace will likely feature more prominently than it has in previous conflicts. Whether the United States wins or loses the cyberspace battles of the next war, the importance of the battles will justify the creation of the Cyber Force. If the U.S. cyberwarriors emerge victorious, as the airmen did in the skies over 1944 Europe, cyberspace will have been proven as a legitimate warfighting domain, and the case for the independent U.S. Cyber Force will be validated. If the United States fails to achieve cyberspace superiority and suffers the stifling consequences, the inefficiencies in the DOD's current approach to cyberspace will be punctuated, and a cyber force will serve as the remedy.

Carl von Clausewitz noted that war requires the maximum use of force a nation can muster: "If one side uses force without compunction … while the other side refrains, the first will gain the upper hand."[6] Bringing the maximum force to the enemy, including effects through cyberspace, is the surest guarantee of success, and inefficient organization will hamper that effort.

New wars, new budgets. It is an odd dynamic of organizations that when budgets are large, leaders prioritize growth over efficiency. Then, when budgets are smaller and efficiency is truly necessary, the capital required to optimize practices cannot be spared. With a peace dividend as the goal, the expense required to establish a new, more efficient military service is unavailable. As the wars of the last decade end, the defense budgets will likewise shrink. Admittedly, the defense budget shrank following World War II, and the Nation still managed to establish the Air Force. In that situation, national security policy leaders rightly identified the rising communist threat as justification for the expense. Today, following the wars in Iraq and Afghanistan, no single identifiable threat has emerged to convince the Nation to delay the expected peace dividend. Therefore,

(Photo by David Vergun, U.S. Army)

The 2nd Armored Brigade Combat Team, 1st Armored Division's brigade headquarters and tactical operations center at Fort Bliss, Texas, participate in Network Integration Evaluation (NIE) 16.1. The exercise, which ran 25 September through 8 October 2015, evaluated a coalition network that linked together the disparate networks of fourteen other armies that participated live or virtually in a simulated combat environment. New technologies assessed during NIE 16.1 included coalition network capabilities, expeditionary command posts, operational energy capabilities, and manned/unmanned teaming (air and ground robotics).

achieving efficiency by creating an independent cyber service must wait until funds are available. Those defense resources will likely become available when cyberspace proves its viability as a warfighting domain during the next major U.S. conflict.

Conclusion

The United States needs an independent military service focused on cyberspace but will likely wait until the next major conflict to establish it. The current DOD approach to cyberspace, where existing armed services donate personnel of varying experience for USCYBERCOM to knit together, is fraught with inefficiencies. Establishment of the Cyber Force would allow the cyberwarrior community to thrive, and it would unburden the existing armed services from the distraction of cyberspace. The United States' next major conflict will allow cyberwarriors to demonstrate the importance of their domain and will provide the military with the resources to support a major bureaucratic overhaul.

The prediction that it will take another conflict to establish a cyber force is merely an assumption based on the likely course of events. Inspired leadership may hasten the formation of the new military service.

Clausewitz compares war to a wrestling match, noting that a wrestler's "*immediate* aim is to *throw* his opponent in order to make him incapable of further resistance [original emphasis]."[7] He observes that if one wrestler uses all his might to pin his opponent, the pinned belligerent may not ever have the opportunity to muster his total strength. Due to its isolation by two oceans, the United States has historically been afforded the opportunity to muster its military strength before committing to war. However, oceans mean little in cyberspace, and, unprepared, the United States may suffer tremendous damage in the initial cyberspace attacks of the next major war. Wise defense leaders will begin moving the military toward establishment of the U.S. Cyber Force to achieve superior focus and efficiencies before the next conflict rather than after it. ■

Biography

Maj. Matt Graham is an U.S. Army strategist assigned to the Joint Staff Directorate for Joint Force Development. He holds a master's degree in public administration from the George Washington University and a BS from the U.S. Air Force Academy in computer science. His previous assignments include tours in Alaska, Germany, Washington, D.C., Iraq, and Afghanistan.

Notes

1. Adam Smith, *An Inquiry into the Nature and Causes of the Wealth of Nations: A Selected Edition*, ed. Kathryn Sutherland (Oxford, UK: Oxford University Press, 2008), 12–14.

2. Jim Collins, *Good to Great: Why Some Companies Make the Leap … and Others Don't* (New York: Harper Collins Publishers, 2001), 94–96.

3. Scheherazade Rehman, "Estonian's Lessons in Cyberwarfare," U.S. News and World Report website, 14 January 2013, accessed 22 August 2014, http://www.usnews.com/opinion/blogs/world-report/2013/01/14/estonia-shows-how-to-build-a-defense-against-cyberwarfare.

4. E. Lincoln Bonner III, "Cyber Power in 21st-Century Joint Warfare," *Joint Force Quarterly* 74 (2014): 102.

5. Michael Riley, "How Russian Hackers Stole the Nasdaq," Bloomberg Business website, 17 July 2014, accessed 4 March 2016, http://www.bloomberg.com/bw/articles/2014-07-17/how-russian-hackers-stole-the-nasdaq.

6. Carl von Clausewitz, *On War*, ed. and trans. Michael E. Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1989), 75–76.

7. Ibid., 75.