Army, Navy, Air Force, and Cyber—Is it Time for a Cyberwarfare Branch of Military?

by Lt Col Gregory Conti and Col John “Buck” Surdu

The Army, Navy, and Air Force all maintain cyberwarfare components, but these organizations exist as ill-fitting appendages that attempt to operate in inhospitable cultures where technical expertise is not recognized, cultivated, or completely understood. The services have developed effective systems to build traditional leadership and management skills.

Disclaimer
The views expressed in this article are those of the authors and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, the Department of Defense, or the United States Government.

At critical points in history, technological advances have driven fundamental changes in the conduct of warfare. The tank, radio, long bow, helicopter, machine gun, military robot, and unmanned aerial vehicle, among many other technologies, changed the face of warfare. Agile military organizations exploited these new technologies—by adopting innovative tactics, doctrine, cultures, and organizations—or faced irrelevance and probable defeat on the battlefield. However, occasionally, a new technology is so significant that it creates a discontinuity in the conduct of war that necessitates creation of an entirely new military service. This situation occurred in the United States, resulting in the formation of the Air Force in 1947. The advent of air power fundamentally altered the conduct of warfighting and drove the transformation of the Army Air Corps into the United States Air Force.

The revolution in cyberwarfare places today’s militaries at a similar cusp in history and necessitates the formation of a cyberwarfare branch of the military, on equal footing with the Army, Navy, and Air Force. We do not make this recommendation lightly—the time is now to reevaluate the structure, organization, and missions of today’s armed forces in order to succeed in the Global War on Terrorism, ensure victory in future conflicts, and avoid technological surprises. This article asks and seeks answers to hard, but necessary questions regarding cyberwarfare and the future of our armed forces.

To understand the compelling need to create a cyberwarfare service, it is useful to examine the missions of the existing United States Armed Forces—

- The Army’s mission is to fight and win our Nation’s wars by providing prompt, sustained land dominance across the full range of military operations and spectrum of conflict in support of combatant commanders.
- The mission of the Navy is to maintain, train, and equip combat-ready Naval forces capable of winning wars, deterring aggression and maintaining freedom of the seas.
- The mission of the United States Air Force is to fly, fight and win…in air, space, and cyberspace.

Of these three, only the Air Force mission mentions cyberspace. This reference was added to the Air Force mission statement in 2006, with the creation of the two-star Air Force Cyber Command, and while acknowledgement of cyberspace as a core military mission by the Air Force is an admirable step forward, it is not the solution. The importance and mission requirements of

cyberwarfare are larger than any existing service organization. More importantly, the cultures of the Army, Navy, and Air Force are fundamentally incompatible with that of cyberwarfare. These existing services operate in the kinetic arena, the directed application of physical force, whereas cyberwarfare exists in the non-kinetic world of information flows, network protocols, and hardware and software vulnerabilities. Both kinetic and non-kinetic operations are critical components of warfighting, and the current ad hoc solution of small pockets of cyberwarfare capability within the existing services is not as effective as it could be.

The Army, Navy, and Air Force all maintain cyberwarfare components, but these organizations exist as ill-fitting appendages that attempt to operate in inhospitable cultures where technical expertise is not recognized, cultivated, or completely understood. The services have developed effective systems to build traditional leadership and management skills. They are quite good at creating the best infantrymen, pilots, ship captains, tank commanders, and artillerymen, but they do little to recognize and develop technical expertise. As a result, the Army, Navy, and Air Force hemorrhage technical talent, leaving the Nation's military forces and our country under-prepared for both the ongoing cyber cold war and the likelihood of major cyberwarfare in the future. One need only review the latest computer security report card, which gave the Federal Government an overall grade of C, and the Departments of Agriculture, Commerce, Defense, Interior, Treasury, Transportation, and Veterans Affairs a grade of D or lower, to our understand our nation's vulnerability.

The Ongoing Cyber Cold War

Make no mistake—the cyber cold war is being waged now. The networks and information processing assets of all branches of the United States Government are under continual attack. In 2007, 1,500 computers in the Department of Defense were taken offline because of a cyber attack. According to Defense Secretary Robert Gates, the Pentagon alone receives hundreds of attacks per day, many from nations that are supposed to be our "friends." Similarly, the Department of Homeland security acknowledged more than 800 attacks in the past two years. Every component of our country, including government, industry, defense, and individual citizens, is becoming increasingly dependent on technology. A successful, major cyber attack could paralyze our country and its armed forces. Such an attack is not idle speculation. The first cyberwar has already occurred. In 2007, the technologically advanced country of Estonia was paralyzed by waves of attacks, suspected to be of Russian origin, that targeted key information assets, including those of Estonia's banks, major media outlets, and government agencies. Both the United Kingdom and United States are facing repeated attacks that some experts attribute to the Chinese Liberation Army. Attacks, such as those faced by Estonia, the United Kingdom, and the United States are harbingers of other more devastating attacks sure to come.

Cyberwarfare is fundamentally different from traditional kinetic warfare. National boundaries in cyberspace are difficult, if not impossible, to define. Lawyers and pundits are still debating the formal definition of an "act of war." Asymmetries abound. Defenders must block all possible avenues of cyber attack. An attacker need only exploit a single vulnerability to be successful. A lone, but specially crafted, phishing e-mail sent to a senior official could compromise an entire network. Attackers can assault objectives from virtually any point on the planet, hopping through a number of intermediate points to mask their trail. Verifying the source of network attacks is a difficult and sometimes impossible task.

The skill sets required to wage cyberwar in this complex and ill-defined environment are distinct from waging kinetic war. Both the kinetic and non-kinetic are essential components of modern warfare, but the status quo of integrating small cyberwarfare units directly into the existing components of the armed forces is insufficient. A separate military service to conduct cyberwarfare must be created. Adding an efficient and effective cyber branch alongside the Army, Navy, and Air Force would provide our nation with the capability to defend our technological infrastructure and conduct offensive operations. Perhaps more important, the existence of this capability would serve as a strong deterrent for our Nation's enemies.

A Clash of Cultures

The cultures of today's military services are fundamentally incompatible with the culture required to conduct cyberwarfare. This assertion in no way denigrates either culture. Today's militaries excel at their respective missions of fighting and winning in ground, sea, and air conflict; however, the core skills each institution values are intrinsically different from those skills required to engage in cyberwarfare. Cyber requires a deep understanding of software, hardware, operating systems, and networks at both the technical and policy levels. The Army, Navy, and Air Force are run by their combat arms officers, ship captains, and pilots, respectively. Understandably, each service selects leaders who excel at conducting land, sea, and air battles and campaigns. A deep understanding and respect for cyberwarfare by these leaders is uncommon.

To understand the culture clash evident in today's existing militaries, it is useful to examine what these services hold dear—skills such as marksmanship, physical strength, and the ability to jump out of airplanes and lead combat units under enemy fire. Accolades are heaped upon those who excel in these areas. Unfortunately, these skills are irrelevant in cyberwarfare. Consider two events, the Best Ranger competition conducted by the Army at Fort Benning, Georgia, and the Capture the Flag contest that occurs each year at the DEFCON hacker conference. Akin to an Iron Man competition, the Best Ranger competition is a career-long achievement recognized across the Army. The winning team proves it has the fortitude to meet intense physical demands. Capture the Flag, on the other hand, brings together some of the world's best hackers in similarly intense competition. Earning a "black badge" as the winning team at DEFCON represents a similar accomplishment, but would pass unrecognized by today's military services. Both require years of preparation—one accomplishment is intensely valued, but the other is not. We are not arguing that there is anything wrong with the Best Ranger competition or similar events. They have proven effective in creating the combat forces necessary to conduct a broad spectrum of operations. We are, however, arguing that similar competitions and accolades are needed to reward those who will be the heroes in a future cyber battle or campaign.

The culture of each service is evident in its uniforms. Consider the awards, decorations, badges, patches, tabs, and other accoutrements authorized for wear by each service. Absent is recognition for technical expertise. Echoes of this ethos are also found in disadvantaged assignments, promotions, school selection, and career progression for those who pursue cyberwarfare expertise, positions, and accomplishments. Some cyberwarfare soldiers, sailors, and airmen who seek to make a career of the military go to great lengths to mask their technical expertise and assignments from promotion boards by making their personnel evaluations appear as mainstream as possible. It is also common for technically oriented career fields to create entire artificial unit hierarchies that mirror combat arms units to help prevent prejudice and retribution. Evidence to back these assertions is easy to find. From a recent service academy graduate who desired more than anything to become part of a cyberwarfare unit but was given no other option than to leave the service after his initial commitment, to the placement of a service's top wireless security expert in an unrelated assignment in the middle of nowhere, to the PhD whose mission was to prepare PowerPoint slides for a flag officer—tales of skill mismanagement abound.

The realities of the existing services' career environment and culture is not lost on their technical experts, many of whom choose to leave military service to pursue their passion. Do technologists believe in serving their country and serving in the military? Many do, but we must create an environment where their expertise is valued, cultivated, and rewarded, else they will take their skills elsewhere. We are not arguing that the cultures extant in the services are not effective in creating the skills needed for a broad spectrum of operations, both conventional and unconventional. Instead, we are arguing that these cultures inhibit (and in some cases punish) the development of the technical expertise needed for this new warfare domain. Given the entrenched values, personnel systems, leadership, and culture, only creation of a new military service from the ground up would allow an environment capable of recruiting, retaining, training, and grooming the cyberwarfare capabilities and personnel our nation desperately needs. For these reasons, we are arguing that the time is right to create a new service focused on cyberwarfare and its interactions with, and support of, the other services in the conduct of more traditional operations.

A key question when forming a cyber branch of military service is whether the National Security Agency (NSA) is already such a force today. NSA seeks to recruit top-tier talent in a wide range of technical disciplines, including computer science, electrical engineering, mathematics, cryptanalysis, and signals analysis. Much of NSA's work is classified, but it falls into two broad missions: information assurance and signals intelligence. However, NSA suffers as a result of the cultures of the Army, Navy, and Air Force. NSA's long-term civilian workforce trains the soldiers, sailors, and airmen, particularly those of mid-career ranks, who rotate into an NSA assignment, only to lose them after a few short years. Technical skill sets atrophy quickly, and many service members rotate to unrelated fields where they lose their expertise. As a result, NSA is constantly training and then losing military personnel, placing a significant burden on its civilian workforce. The problem is compounded because repeated assignments to NSA and similar organizations are not valued by the services, and those service members who excel at cyberwarfare activities face significant risks to their careers.

Fundamentally, we believe that while today's mission and capabilities of NSA overlap to some degree with those of a military cyberwarfare branch, NSA is not the right type of organization. Led by a three-star flag officer, NSA is relegated to a subordinate role when the mission of cyberwarfare should be on par with the other military services. Ultimately, the role of fighting and winning in cyberspace is a military mission, which demands a military organization—one that can recruit, train, and retain highly qualified cyberwarfare combatants.

A Path Forward

The Air Force is heading in the right direction. Its drive toward a cyberwarfare capability is admirable. However, its initiative needs to extend beyond the Air Force to encompass the entire military. Cyber Command's engagement of Slashdot.org, probably the most popular technical news source and discussion forum for the technical community, was the right move. Only by understanding the culture of the technical workforce can a cyberwarfare organization hope to succeed—cultural change must occur in order to maximize our cyberwarfare capabilities. High-and-tight haircuts, morning physical training runs, rigorously enforced recycling programs, unit bake sales, and second-class citizen status are unlikely to attract and retain the best and brightest people.

Cyber warfare requires unique technical skills as well as skills in creative problem solving, poise under pressure, and critical thinking. Attributes that are desirable in soldiers, such as physical endurance, marksmanship, and technical skills associated with the employment of traditional forces and weapons systems, do not translate well to cyber warfare. Instead, skills such as the ability to scan through logs and reports to quickly ascertain the nature and threat of a cyber battle, knowledge of the latest network exploitation techniques and attack tools, and a deep understanding of information flows are the skills needed in a cyber corps operator. While some required traits are similar to today's military forces, such as integrity, teamwork, dedication to mission, the ability to keep secrets, and creative problem solving under pressure, many are fundamentally different. Because the skill sets and mission areas are different, the cyber corps needs to recruit, train, and retain a different breed of warrior. Institutions such as ROTC should be reevaluated to determine their usefulness as a mechanism for staffing our proposed cyberwarfare service. Appropriate training exercises, such as network attack-and-defend exercises, will also need to be created that fit cyberwarfare mission requirements. In short, creating a new cyber service provides the opportunity to rethink kinetic warfare paradigms, adapting some, discarding others, and creating new non-kinetic warfare tactics and strategies.

Personnel with the technical expertise required for cyberwarfare are in high demand. Competitive salaries are always beneficial but not necessarily a requirement. Consider Google. Google has recruited some of the world's best talent in a variety of technical disciplines, not through excessive salaries, but by creating a culture where people want to work. The idea of working on interesting problems, experimenting with cutting-edge technical gear, spending 20 percent of one's time working on a project of one's own choosing, and interacting with similarly talented people has made Google an A-list employer that must turn away qualified applicants. While a cyberwarfare branch's model would likely be different, the key idea is the same—make it the most desired place to work in the computer security community.

Recruiting ethical, trustworthy people is, of course, of paramount importance. In their formative years, many technically talented individuals make critical decisions that influence the direction of their life. In the hacking community, perhaps the most important decision is whether or not to engage in illegal activity. By creating a cyber organization that is elite, complete with role models that junior members would want to emulate, we can recruit individuals before they make irreversible decisions that would eliminate their ability to serve their country.

One key advantage is that the current services would not need to change significantly. They would only need to interface correctly. Services must be able to communicate and coordinate to conduct joint and combined operations. Correctly constructing the interfaces between each service is a key to success. The Army, Navy, Air Force, Marines, Coast Guard, and myriad federal agencies, as well as their international counterparts, successfully coordinate operations today, and cyber will be no exception.

Conclusions

The overwhelming dependence of individuals, militaries, businesses, and governments worldwide on information technologies and the catastrophic consequences of the disruption or destruction of those technologies present a clear and present danger to the United States. We are facing a severe cyberwarfare threat now—but a major cyberwar involving the United States is inevitable. Our existing military organizations' cyberwar capability is inadequate, and this situation is unlikely to change without radical transformation. The best solution is to create a new cyber service and carefully craft its organization and culture to meet current and future needs. A properly designed organization will promote intellectual agility and retain the top-tier talent required to conduct successful offensive and defensive operations in cyberspace. The change will not be easy, but the risks inherent in maintaining the status quo are significantly worse. ■

References

1. “The United States Army: Organization.” *http://www.army.mil/institution/organization.*
2. Navy Organization: *http://navy.mil/navydata/organization/org-top.asp*
3. Air Force Link: *http://www.af.mil/main/welcome.asp*
4. Anne Proctor. “AF launches cyberspace task force.” Air Force Print News, 6 April 2006. *http://www.af.mil/news/story.asp?id=123018708.*
5. Richard Bejtlich. “Air Force Cyberspace Report.” TaoSecurity, 12 October 2007. *http://taosecurity.blogspot.com/2007/10/air-force-cyberspace-report.html.*
6. Eight Report Card on Computer Security at Federal Department and Agencies. House Committee on Oversight and Government Reform, 20 May 2008. *http://republicans.oversight.house.gov/media/PDFs/Reports/FY2007FISMAReportCard.pdf.*
7. Richard Nortonton-Taylor. “Titan Rain—how Chinese hackers targeted Whitewall.” The Guardian, 5 September 2007. *http://www.guardian.co.uk/technology/2007/sep04/news.internet.*
8. “Career Fields.” National Security Agency. *http://www.nsa.gov/careers/careers.cfm.*
9. “Mission Statement.” National Security Agency. *http://www.nsa.gov/about/about00003.cfm.*

About the Authors

Lt Col Gregory Conti | is an Assistant Professor of Computer Science at the United States Military Academy, West Point, New York. He holds a PhD from the Georgia Institute of Technology, an MS from Johns Hopkins University, and a BS from the United States Military Academy, all in computer science. His research includes information warfare, security data visualization, and web-based information disclosure. He may be reached at *gregory.conti@usma.edu.*

Col John “Buck” Surdu | is currently serving as chief of staff of the Army’s Research, Development, and Engineering Command. He has previously served in a variety of infantry assignments, as a researcher at the Army Research Laboratory, as a senior researcher in the Information Technology and Operations Center, as a product manager for the One Semi-Automated Forces (OneSAF), and as a project manager at the Defense Research Projects Agency. In addition to a BS degree in computer science from the United States Military Academy, COL Surdu earned an MBA from Columbus State University. COL Surdu later earned a MS in computer science from Florida State University, focusing on artificial intelligence. He completed his formal education with a doctoral degree in computer science from Texas A&M University focusing on simulation technology and its applications to command and control. He may be reached at *john.surdu@darpa.mil.*

Letter to the Editor

Q ***I understand there is a new way to share research & development (R&D) information across government, industry and academia. Can you provide some information on the project?***

A DoD Techipedia is a Department of Defense (DoD) sponsored wiki service on DoD scientific and technical information (S&T) available to all government and authorized commercial and academic institution personnel. DoDTechipedia was developed to provide an agile means to increase collaboration and communication among the R&D DoD, government, commercial enterprise, and academic community.

From DoDTechipedia’s home page, you can navigate to areas such as acronyms, terminology, technology areas, interest areas, organizations, how to do business, and private and public blogs. Within each technology area, you will find hot topics, key documents, and other information important to that technology area. For example, the information assurance (IA) technology area has included hot topics on IPv6, Software Protection, and Service Oriented Architecture (SOA) Security.

DoDTechipedia is a valuable source of information and technology that will enable users to see and discuss the innovative technologies being developed throughout the DoD and also emerging technologies across the private sector and academic institutions.

Access to DoDTechpedia requires DTIC user registration at *http://www.dtic.mil/dtic/registration* and is located at *https://www.dodtechpedia.mil/dodwiki.* ■