War Fighting in Cyberspace

Evolving Force Presentation and Command and Control

Maj M. Bodine Birdwell, USAF*
Lt Col Robert Mills, PhD, USAF, Retired

The Department of Defense (DOD) is endeavoring to define war fighting in the global cyberspace domain.[1] Creation of US Cyber Command (USCYBERCOM), a subunified functional combatant command (FCC) under US Strategic Command (USSTRATCOM), is a huge step in integrating and coordinating the defense, protection, and operation of DOD networks; however, this step does not mean that USCYBERCOM will perform or manage all cyberspace functions. In fact the vast majority of cyberspace functions conducted by the services and combatant commands (COCOM), although vital for maintaining access to the domain in support of their operations, are not of an *active* war-fighting nature. We apply the concepts of war fighting, offense, and active defense to the domain of cyberspace and propose several recommendations to aid USCYBERCOM as it works with the services and geographic combatant commands (GCC) to fight in cyberspace. That global, regional, and service commanders will have to share command and control (C2) of cyberspace war-fighting capabilities and forces raises several interesting questions about how USCYBERCOM can most effectively work with the GCCs. Specifically, what is the ideal force presentation method, and which C2 model should the DOD use for war-fighting capabilities in cyberspace? Are there lessons learned from similar global-to-regional support challenges that we might apply to cyberspace C2? We offer US Special Operations Command (USSOCOM) as a model for cyberspace force presentation and C2; however, this model is a long-term goal that is not immediately achievable. In the interim, USCYBERCOM can adapt lessons learned from space and air-mobility force presentation and C2 to develop a building-block approach to evolve cyber force presentation and C2 from its current nascent state to a more mature USSOCOM-like state.

Although other models exist, we examine how space, air mobility, and special operations force presentation and C2 models can inform the way USCYBERCOM could interact with the other COCOMs—particularly the GCCs. We also discuss the complex interdependencies, specialized capabilities, and doctrinal approaches FCCs use as they provide capabilities to GCCs. To begin, we briefly address the inadequacy of current doctrine for war fighting in cyberspace. Then we examine how space and air mobility doctrine can serve as useful, although only partly adequate, models for presenting forces and performing C2. Finally, we provide a building-block methodology to take us from current capabilities to a fully developed USSOCOM-like cyberspace model.

---

*Major Birdwell is director of operations, Air Intelligence Squadron, Air Mobility Command, Scott AFB, Illinois. He thanks his wife, Michelle, for her assistance in editing this article; she put in long hours enabling the authors to better articulate their thoughts. Dr. Mills is an associate professor of electrical engineering at the Air Force Institute of Technology, Wright-Patterson AFB, Ohio.

Why the Existing Information Operations Model Is Insufficient

Current Air Force and joint doctrine governing war fighting in cyberspace is scarce. According to Air Force Doctrine Document (AFDD) 3-12, *Cyberspace Operations*, "Although cyberspace operations are integral to all combatant commands, Services, and agency boundaries, as of the date of publication of this AFDD, there is no overarching joint doctrine for planning or operations in cyberspace."[2] A new joint doctrine cyberspace publication is being formally staffed, but published joint doctrine comes no closer to addressing war fighting in cyberspace than a discussion of computer network operations as a subset of information operations (IO).[3] Computer network operations and IO are clearly related, but their purposes differ. Gen Keith B. Alexander, commander of USCYBERCOM, wrote, "Although it is understood that land, maritime, air, and space warfare will be employed to deter (for example, influence) an adversary, no one believes that warfare within these domains is uniquely 'information operations.'"[4]

Both AFDD 3-12 and General Alexander recognize that war fighting in cyberspace is more than a subset of IO; however, at this time Joint Publication (JP) 3-13, *Information Operations*, provides the only joint framework that addresses C2 for cyberspace war fighting. Joint doctrine contains no guidance for cyber force presentation. IO doctrine defines computer network operations, comprised of computer network attack (CNA), computer network defense (CND), and computer network exploitation.[5] For the purpose of this article, we define cyber war-fighting actions as CNA plus a subset of CND called CND-response actions (CND-RA).[6] According to JP 3-13, CNA activities are now integrated at the theater level in the J-39 IO cell.[7] JP 6-0, *Joint Communications System*, notes that CND is integrated within the J-6.[8] This arrangement is problematic because it splits related war-fighting functions between different staff elements and essentially minimizes the importance of a war-fighting domain by burying it within the Joint Staff.

Joint doctrine must separate the shared responsibility for maintaining access to the cyberspace domain, which should be a J-6 (communications) function, from the concept of war fighting in cyberspace, which should be a J-3 (operations) function.[9] General Alexander noted, "Where the principal effect of IO is to influence an adversary *not* to take an action, the principal effect of cyber warfare is to deny the enemy freedom of action in cyberspace" (emphasis in original).[10] To engage in cyber warfare as General Alexander envisions it, responsibility for CNA and CND-RA must expand beyond the Joint Staff and be treated the same as warfare in other domains.

Defining Force Presentation

Force presentation for cyber war fighting is the manner in which USCYBERCOM and the services make CNA and CND-RA capabilities available to the GCCs. JP 1, *Doctrine for the Armed Forces of the United States*, summarizes the roles and responsibilities of the services and COCOMS:

> The Services and United States Special Operations Command (in areas unique to special operations) have responsibilities to organize, train, equip, and sustain forces. . . .
>
> The Commanders, US Central Command, US European Command, US Pacific Command, US Southern Command, and US Northern Command. . . . (1) deter attacks against the United States, its territories, possessions and bases, and employ appropriate force should deterrence fail; (2) carry out assigned missions and tasks and plan for and execute military operations, as directed, in support of strategic guidance.[11]

As the DOD components tasked to fight wars, COCOMs define requirements, and the services then organize, train, equip, and sustain forces to meet them. Currently USSOCOM is unique in that it is a COCOM with service-like responsibilities.

The force presentation and C2 models for space, air mobility, and special operations form steps along a continuum of options that USCYBERCOM can use when providing war-fighting forces and capabilities to the GCCs. The first step, space force presentation, is based on an independent action model that USSTRATCOM uses to control space force presentation and support the GCCs. The second step, air mobility force presentation, is based on an interdependent action model by which US Transportation Command (USTRANSCOM) works with the GCCs to move forces and supplies throughout the world. Finally, special operations forces (SOF) force presentation is based on an organic force presentation model.

Step One: A Space Model—Independent Action

Today, as the DOD develops cyber war-fighting capabilities, we do not have enough cyber war fighters available to distribute them in a decentralized manner among the GCCs. Using an independent action model would enable USCYBERCOM to support the maximum number of GCC requirements because USCYBERCOM could dynamically shift its limited resources to maximize GCC support. USSTRATCOM has done this for decades with space force presentation. Applying space doctrinal concepts can help USCYBERCOM take immediate measures to improve cyber force presentation to the GCCs.

Gen Kevin P. Chilton, former commander of USSTRATCOM, clearly connected space to cyberspace: "Let's move into the line of operation that we call cyberspace. Is that a support line for us? You bet. Just like space. Is it global in nature? You bet. Just like space. Do we operate in it every day? You bet. Just like space. In fact what we're tasked to do is to operate, defend, prepare to attack, and on order attack through this domain."[12]

USSTRATCOM's actions in space occur independently of any actions taken in the theater. That command does not rely upon the GCC to carry out some task before it can complete its own tasks in space. However, the space relationship is inherently a dependent one from the perspective of the GCC. For this reason, GCCs must explicitly state all space support requirements to USSTRATCOM; to do otherwise would potentially disrupt or negatively affect GCC war-fighting operations that depend upon space support.

The space force presentation and C2 template centralize all GCC communications through a specified channel within USSTRATCOM called the joint functional component command space (JFCC Space). That channel communicates with all GCCs and maintains situational awareness of how space operations integrate with all GCC activities. In order to communicate effectively, JFCC Space uses the joint space operations center (modeled after an air and space operations center [AOC] construct) to command and control military space operations effectively.

USSTRATCOM has delegated day-to-day communication activities to JFCC Space. Likewise, JP 3-14, *Space Operations*, notes that "[GCC commanders] may designate a space coordinating authority (SCA) and delegate appropriate authorities for planning, integrating, and coordinating space operations within the operational area."[13] In many regards, the SCA serves as the COCOM's focal point for all space support operations. An SCA can work with JFCC Space for all types of space support issues. The concept of the SCA serves as a cross-domain model for communicating between USSTRATCOM and the GCC. The SCA gathers the requirements from all service and functional components and, on behalf of the GCC, speaks with one voice to USSTRATCOM via JFCC Space.

Achieving USCYBERCOM Independent Action: Cyber Coordinating Authority. To increase the visibility of cyber war-fighting activities, each GCC should adopt the SCA concept for cyber force presentation, in effect creating a cyber coordinating authority (CCA). This action is viable today because it requires limited resources. The greatest challenge to creating a CCA

position within each GCC lies in determining its proper placement. Space doctrine regarding SCA placement defers this decision to each GCC.[14] USCYBERCOM could follow the space doctrinal template of deferring the decision to each GCC, or it could recommend a CCA placement location in order to best integrate USCYBERCOM activities within the GCC scheme of maneuver.

Furthermore, if a CCA were created, USCYBERCOM could continue to complete many of its existing war-fighting functions in a centralized manner. As with space operations, the relationship would remain independent from the FCC perspective and dependent from the GCC perspective. Within the GCC, the services maintain and operate their own networks. USCYBERCOM would direct all CNA and CND-RA activities on behalf of the GCC.

Space doctrine offers insight into cyber force presentation beyond the joint force headquarters level. USSTRATCOM directs its service components (in regard to space) to serve as space proponents within their service, especially the service components of GCCs:

> Common responsibilities of each of the Service components are: advocating for space requirements within their respective Services, providing a single point of contact for access to Service resources and capabilities, making recommendations to USSTRATCOM on appropriate employment of Service forces, providing assigned space forces to CDRUSSTRATCOM [commander, USSTRATCOM] and CCDRs [combatant commanders] as directed, assisting in planning in support of space operations and assigned tasking, and supporting CDRUSSTRATCOM and other CCDRs with space mission area expertise and advocacy of desired capabilities as requested.[15]

USSTRATCOM disperses the space expertise resident in its service components to the GCC service components to provide the GCCs "space mission area expertise and advocacy," as mentioned above. This approach enables USSTRATCOM to centralize C2 space capabilities while ensuring that the GCC components are aware of space capabilities. These space proponents help GCC components integrate space capabilities within their operations.

Achieving USCYBERCOM Independent Action: Service Component Responsibilities. The service components to USCYBERCOM should act as CNA and CND-RA proponents within each GCC. Those components should send liaisons to champion cyber war-fighting capabilities within the respective GCC service and functional components to maximize USCYBERCOM's contribution to GCC war-fighting activities. Space doctrine provides a template for integrating space within the service components, using the Army's space support elements, the Navy's space operations officers, the Marines' space cadre, and the Air Force's director for space forces.[16] Although USSTRATCOM has no special operations component, it does maintain a space support team construct to send space "proponents" to GCC special operations components.[17] USCYBERCOM's embedded cyber war-fighting proponents would advocate methods by which USCYBERCOM CNA/CND-RA actions could help fulfill GCC requirements, which would then filter back to USCYBERCOM via the GCC CCA.

Step Two: An Air Mobility Model—Interdependent Action

Creating a CCA and dispersing proponents throughout the GCC would lay a strong foundation to build a mature methodology for cyber force presentation. These initial measures to leverage lessons learned from space force presentation should continue to evolve into an interdependent communication model. Such an intermediate step is necessary to transition cyber war fighting from a primarily USCYBERCOM mission to a mission shared between USCYBERCOM and GCCs. The next building block, an interdependent model, would enable each GCC to develop a nascent organic cyber war-fighting capability and develop regional cyber war-fighting subject-matter experts.

Interdependent operations differ from independent operations in that both parties rely on each other for mission accomplishment. Interdependent operations are more complex than independent operations because they require coordination to avoid duplication of effort and to maximize utility. Cyber war-fighting actions occurring at near "network speed" will demand detailed planning and coordination because execution speed may render real-time communication impossible. Air mobility operations offer insight into mitigating the communication challenges of interdependent operations.

Because of limited air mobility resources, global air mobility operations must occur interdependently among the FCC, USTRANSCOM, and GCCs. The DOD simply does not have enough air mobility assets to give each GCC all of the airlift it requires. Therefore, all components must share ownership and collaborate. For this reason, air mobility force "ownership" can be segmented into three distinct classifications: those forces under the command of USTRANSCOM, those under the GCC (such as US Pacific Command), and each service's organic air mobility forces.[18]

USTRANSCOM maintains an air component, US Air Forces Transportation, which, in turn, maintains the 618th AOC. The latter, which communicates with GCC AOCs daily to enable global mobility operations, has responsibility for the majority of intertheater airlift, while the GCCs' AOCs have responsibility for the majority of each GCC's intratheater airlift.[19] The 618th AOC and the GCC AOCs thus work interdependently to ensure the success of the global air mobility enterprise.

Joint doctrine offers the concept of a facilitator to aid this process. JP 3-17, *Air Mobility Operations*, defines the director of mobility forces (DIRMOBFOR) as a "coordinating authority for air mobility with all commands and agencies, both internal and external to the JTF [joint task force], including the JAOC [joint air operations center], the 618th TACC [Tactical Air Control Center, now known as the 618th AOC], and the JDDOC [joint deployment and distribution operations center] and/or the JMC [joint movement center]."[20] JP 3-17 describes the DIRMOBFOR as "normally a senior officer who is familiar with the AOR [area of responsibility] or JOA [joint operations area] and possesses an extensive background in air mobility operations. The DIRMOBFOR serves as the designated agent for all air mobility issues in the AOR or JOA, and for other duties as directed."[21] However, because the DIRMOBFOR represents the commander of Air Force forces rather than the joint force air component commander, the director must work with the AOC's commander and its air mobility division for intratheater airlift operations. Within the theater AOC, the air mobility division will "integrate and direct the execution of theater assigned or attached Service organic mobility forces operating in the AOR or JOA in support of JFC [joint force commander] objectives."[22] The 618th AOC works interdependently with the GCC's DIRMOBFOR and AOC to ensure that the war fighter receives support via transportation activities and thus obtains the proverbial beans, bullets, and people.

Achieving USCYBERCOM Interdependent Action: Director of Cyber Forces. The GCC's CCA should become the equivalent of the DIRMOBFOR for cyber war-fighting capabilities (i.e., a DIRCYBERFOR). The DIRCYBERFOR would continue to work with USCYBERCOM, as the CCA did, for external cyber war-fighting capabilities but would also work with the GCC's nascent organic cyber war fighters through theater organic C2 channels. In this second step, the GCCs would develop initial cyber war-fighting capability that will require C2 within the GCC itself—external to USCYBERCOM. Unlike the CCA, the DIRCYBERFOR has a doctrinal template in the placement of the DIRMOBFOR underneath the commander of Air Force forces. Although the processes required to integrate airlift clearly differ from those to integrate USCYBERCOM's nonkinetic fires activities, the concept of a DIRCYBERFOR has value.

Joint doctrine gives the following guidance to JFCs who stand up functional components: "Normally, the Service component CDR with the preponderance of forces to be tasked and the ability to C2 those forces will be designated as the functional component CDR; however, the JFC will always consider the mission, nature and duration of the operation, force capabilities, and the C2 capabilities in selecting a CDR."[23] CNA/CND-RA forces are in such a formative state that GCCs will have difficulty initially determining who to designate as the DIRCYBERFOR. Although not directly grounded in existing joint doctrine, it may be best if both the CCA and DIRCYBERFOR begin at the JFC level and then transition over time to create a cyber functional component at both the GCC and JFC levels in the future.

Achieving USCYBERCOM Interdependent Action: Cyber War-Fighting Element. The AOC's air mobility division process could serve as a model for a theater C2 structure for incipient cyber forces—a cyber war-fighting element (CWE). Whereas an air mobility division endeavors to direct and execute the JFC's organic airlift mission, the CWE would endeavor to direct and execute the JFC's cyber war-fighting mission. As JFCs seek to integrate cyber war-fighting capabilities within the theater scheme of maneuver, a small CWE could report to the DIRCYBERFOR within the JFC staff.

We should inject a word of caution at this point. Step one, the space model, entailed sending proponents forward to help the war fighter present requirements to USCYBERCOM through the SCA. Step two, the air mobility model, cannot subsequently remove these forces and use them as the foundation for standing up CWEs because each GCC component will still need cyber war-fighting proponents to push war-fighter requirements to the CWE and DIRCYBERFOR.

Achieving USCYBERCOM Interdependent Action: Cyber Operations Center. As forces become available to establish CWEs, USCYBERCOM should establish a cyber operations center modeled on the 618th AOC to interact with GCCs. The center would work with GCC CWEs and DIRCYBERFORs to prioritize, allocate, and utilize global cyber war-fighting capabilities.

Step Three: A USSOCOM Model—Organic Action

During congressional testimony, General Alexander observed that

> command and control in cyberspace is still more complicated [than in other domains]. Computer network operations can be regional and global at the same time, and can have effects approaching those of weapons of mass destruction. The devices that give us access to cyberspace exist in the physical world, and in conventional military terms we can say that they are always within the area of responsibility of some geographic combatant command—but they can create effects that take place far away in the area of responsibility of a second command, and they might be enabled to do so by unsuspecting users and their devices located in still a third command's region. Which commander is the mission lead in such a case and is military action appropriate? Which command is supported, and which is supporting? In cyberspace, questions like this must be answered at Internet speed and must take into account our responsibilities and obligations under international law and norms.[24]

The challenges that General Alexander described are daunting, but they are not unique—in fact, they are quite similar to the challenges we face when combating terrorism and conducting special operations in general. The DOD has carefully studied terrorism and determined that the best method to confront this global challenge is to direct USSOCOM to "synchronize planning of global operations against terrorist networks."[25] Because of the similar challenges faced by cyber war fighting and SOF, USCYBERCOM should eventually adopt USSOCOM's force presentation and C2 models.

USSOCOM has chosen to posture forces both globally from the continental United States and regionally (organically) within GCCs. Rather than supporting forces, organic forces are the doctrinal concept for

GCC wartime force presentation defined within JP 1, *Doctrine for the Armed Forces of the United States*.[26] Based upon that document, some type of organic cyber forces should also be the end-state goal for GCC force presentation and C2.

Like special operations, war fighting in cyberspace is both global and regional in nature. The SOF community has addressed the dual global and regional nature of terrorism and developed a C2 architecture and force presentation model that provide USCYBERCOM unique and relevant insights. All SOF forces stationed in the continental United States fall under the command authority of USSOCOM, while those assigned to a GCC fall under authority of the GCC commander. As an FCC, USSOCOM provides additional forces on a temporary basis to GCCs for operational employment, with the GCC normally exercising operational control over them.[27] The GCC exercises C2 of all assigned and attached special forces through a theater special operations command (TSOC), which provides unity of command and serves as "the primary theater SOF organization capable of performing broad continuous missions uniquely suited to SOF capabilities" and "the primary mechanism by which a geographic combatant commander exercises C2 over SOF."[28] The TSOC commander has three principal roles: JFC of SOF in-theater, theater special operations adviser, and joint force special operations component commander.[29] This "triple hatting" makes the position unique within the GCCs. Only this commander is dual hatted as a JFC; GCC service components are dual hatted as component commanders because the service components, unlike SOF, are inherently not joint.

Achieving USCYBERCOM Organic Action: Theater Cyber Operations Command. USCYBERCOM should adopt a USSOCOM force-provider mind-set for each GCC's organic cyber war-fighting component. Each theater would establish a theater cyber operations command (TCYOC) to provide the same type of advocacy and C2 provided by the TSOC for SOF. The TCYOC commander would serve as JFC for all assigned and attached cyber operations personnel, as theater cyber operations adviser, and as joint force cyber operations component commander. Implementing this concept would clearly elevate cyberspace to an appropriate level of importance.

Achieving USCYBERCOM Organic Action: Joint Cyber Attack Component. Organic CNA capabilities from multiple services should be combined under a joint cyber attack component. Joint doctrine provides guidance on how the TCYOC should present forces to the GCC: "Functional component commands are appropriate when forces from two or more Military Departments must operate within the same mission area or geographic domain or there is a need to accomplish a distinct aspect of the assigned mission."[30] If multiple services provide cyber attack and defensive response capabilities within the TCYOC, it would be appropriate to create functional components for each. For example, JP 3-05, *Doctrine for Joint Special Operations*, discusses how a joint special operations air component is often created within a joint special operations task force when multiple services have organic air assets.[31] This component creates a layer of oversight with air expertise above the various SOF aviation elements so that the limited resource can be employed in the most efficient manner.

In the future, a TCYOC probably would have organic service components. The SOF template illustrates a scenario in which multiple services could provide overlapping capabilities. Although many SOF aspects are uniquely connected to a service component, capabilities such as air mobility and airborne fires reside in two service components. Lessons learned from theater operations led to the doctrinal concept of a theater joint special operations air component.

If service CNA/CND-RA capabilities evolved into specialized functions, a study of SOF doctrine would indicate that cyber service components should be adequate. However, overlapping of some aspects of

service-provided CNA/CND-RA capabilities may warrant an additional C2 layer.

Achieving USCYBERCOM Organic Action: Liaison Elements. The GCC cyber war-fighting component must send liaison elements to other functional components. Each GCC maintains a special operations component that must liaise with the other GCC (or subordinate joint task force) components. According to JP 3-05, "To fully integrate SO [special operations] and conventional operations, SOF must maintain effective liaison with all components of the joint force to ensure that unity of effort is maintained and risk of fratricide is minimized."[32] Special operations doctrine addresses specific areas where SOF must send liaison elements:

> SOF commanders have available specific elements that facilitate C2, coordination, and liaison. They include . . . the special operations liaison element . . . to provide liaison to the joint force air component commander . . . or appropriate Service component air C2 facility; and SOF liaison officers (LNOs) placed in a variety of locations as necessary to coordinate, synchronize, and deconflict SO within the operational area. . . . All of these elements significantly improve the flow of information, facilitate concurrent planning, and enhance overall mission accomplishment of the joint force.[33]

The TSOC integrates personnel within the AOC to coordinate, deconflict, and integrate SOF air, surface, and subsurface operations.[34] Special operations doctrine recognizes that communication between organic components within the GCC requires conscious effort and resource allocation.

Achieving USCYBERCOM Organic Action: Cyber War-Fighting Liaison Elements. USCYBERCOM should consider creating cyber war-fighting liaison elements when pursuing TCYOCs. JP 3-05 discusses how the special operations liaison element integrates within the JAOC.[35] Members of the former integrate into processes throughout the AOC. Similarly, the cyber war-fighting liaison elements could integrate cyber war-fighting capabilities within the various JAOC divisions. For example, should the TCYOC plan a significant CNA/CND-RA action, the liaison elements could ensure proper integration and deconfliction of the activity within JAOC processes.

Achieving USCYBERCOM Organic Action: "Service-Like" Responsibilities. USCYBERCOM should be given appropriate "service-like" responsibilities for cyber-specific requirements modeled after those of USSOCOM. The methodology for SOF force presentation addresses force presentation from both the COCOM and service perspectives. USSOCOM has service-like responsibilities in that it organizes, trains, and equips SOF.[36] This includes maintaining its own major force program to procure specialized equipment. For example, the US Air Force will procure a C-130 Hercules and deliver it to Air Force Special Operations Command, which then "upgrades" the C-130 into a special operations AC-130U Spooky gunship. One benefit of this arrangement is that SOF-specific requirements (regardless of the service involved) will receive an appropriate amount of advocacy and not be overshadowed by competing service-level requirements. Analogously, USCYBERCOM should be the DOD's primary FCC to organize, train, and equip CNA and CND-RA forces.

Aside from USSOCOM, it is the role of the services to equip and educate their members. The services tend to develop and acquire capabilities in accordance with their own priorities, which may not necessarily favor decisions optimized for cyberspace operations. Furthermore, cyberspace is inherently a joint (or even interagency) operating area, yet the services may pursue different technical solutions to realize similar capabilities, such as CNA software. Gaps may also arise in research, development, and acquisition. With service-like responsibilities, USCYBERCOM could provide cyberspace-specific advocacy for systems acquisition, research, and development.

Achieving USCYBERCOM Organic Action: Joint Cyberspace Operations University. To train or, in this case, educate its members, USCYBERCOM should develop a

Joint Cyberspace Operations University modeled after Joint Special Operations University. USSOCOM maintains the latter to provide continuing education for worldwide SOF. The university focuses on educating senior and intermediate special operations leaders and selected non-special-operations decision makers (both military and civilian) in joint special operations.[37] Joint Cyberspace Operations University could play an important role in developing future cyberspace leaders. It could partner with service schools in the same way Joint Special Operations University partners with these schools, including the US Air Force's Special Operations School.[38] In addition, USCYBERCOM could leverage a number of existing cyber training and education programs, including the Air Force's Undergraduate Cyber Training School, the Air Force Institute of Technology, and the Naval Postgraduate School.[39] It may even be possible to implement Joint Cyber Operations University in a decentralized manner. New schools that specifically address war fighting in cyberspace, such as a Cyber School of Advanced Air and Space Studies and a Cyber Weapons Instructor Course within the USAF Weapons School could also meet specific USCYBERCOM requirements.[40]

Conclusion

USCYBERCOM can begin implementation today of a building-block approach to normalize force presentation for cyber war fighting and C2. Each step would build upon actions taken in the preceding one. The first step, taking lessons learned from space, would require little additional manpower. Initially, USCYBERCOM would advocate that the GCCs adopt cyber coordinating authority for cyber force presentation. Simultaneously, USCYBERCOM would direct its service components to send cyber war-fighting proponents to respective GCC service and functional components to better integrate USCYBERCOM's contribution to GCC war-fighting activities.

The second step in the building-block approach would involve transitioning from a space to an air mobility model. The CCA from the previous step would evolve into a DIRCYBERFOR for cyber war-fighting activities. As forces become available, GCCs would establish cyber war-fighting elements, and USCYBERCOM would stand up a cyber operations center to interact with GCCs.

Within the air mobility model, USCYBERCOM cyber war-fighting proponents would remain embedded within the GCC, as they were under the space model. However, within the USSOCOM model, these USCYBERCOM proponents would evolve into liaisons from the GCC cyber war-fighting component to the other GCC components. With this building block, the individuals would remain, but their C2 chain would change from USCYBERCOM to the GCC.

In the third step (the USSOCOM model), the relationship between the theater JFC staff and USCYBERCOM C2 center would evolve to one of an FCC responsible for global cyber war-fighting operations and a GCC cyber war-fighting component responsible for regional cyber war-fighting activities. The USCYBERCOM C2 center would also maintain responsibility for synchronizing regional actions between GCCs. This synchronization responsibility would require close coordination between the GCC cyber components and the USCYBERCOM C2 center.

USSOCOM has utilized its "service-like" responsibilities to advance special operations war-fighting capabilities. Adapting USSOCOM's service-like attributes could aid USCYBERCOM in much the same manner. The importance of education in developing a cyber war-fighting force cannot be overstated, and Joint Special Operations University offers a model that USCYBERCOM can adapt.

Although the DOD still grapples with the very concept of war fighting in cyberspace and remains unclear about what actions would constitute acts of war, it must still address the question of how to present cyber forces and exercise C2 of them. Cyber-

space is definitely a contested domain, but is it a unique one? Although some aspects of cyberspace are undoubtedly unique, we argue that in the area of force presentation and C2, cyberspace is analogous to other war-fighting domains; hence, we can apply lessons from space and air operations to cyberspace. We therefore recommend that USCYBERCOM adopt our doctrinally based blueprint for presenting and exercising C2 of cyber war-fighting forces. ✪

Scott AFB, Illinois
Wright-Patterson AFB, Ohio

Notes

1. Joint doctrine defines *cyberspace* as a global domain. See Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 12 April 2001 (as amended through 30 September 2010), http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

2. Air Force Doctrine Document 3-12, *Cyberspace Operations*, 15 July 2010, 14, http://www.e-publishing.af.mil/shared/media/epubs/AFDD3-12.pdf.

3. JP 3-13, *Information Operations*, 13 February 2006, IV-5, http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.

4. Lt Gen Keith B. Alexander, "Warfighting in Cyberspace," *Joint Force Quarterly* 46 (Third Quarter 2007): 60, https://digitalndulibrary.ndu.edu/cgi-bin/showfile.exe?CISOROOT=/ndupress&CISOPTR=20001&CISOMODE=print.

5. JP 1-02, *Department of Defense Dictionary*, defines *computer network attack* as "actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves" (93); *computer network defense* as "actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks" (93); and *computer network exploitation* as "enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks" (93).

6. CND-RAs are "deliberate, authorized defensive measures or activities that protect and defend DOD computer systems and networks under attack or targeted for attack by adversary computer systems/networks. RAs extend DOD's layered defense-in-depth capabilities and increase DOD's ability to withstand adversary attacks." Chairman of the Joint Chiefs of Staff Instruction 6510.01E, *Information Assurance (IA) and Computer Network Defense (CND)*, 12 August 2008, GL-7, http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf.

7. JP 3-13, *Information Operations*, IV-5.

8. JP 6-0, *Joint Communications System*, 10 June 2010, III-1, http://www.dtic.mil/doctrine/new_pubs/jp6_0.pdf.

9. For a more in-depth discussion on the importance of separating war fighting in the domain from actions taken to maintain access to the domain, see Dr. Robert F. Mills, Maj M. Bodine Birdwell, and Maj Kevin R. Beeker, "Apples & Oranges: Operating and Defending the Global Information Grid," *IAnewsletter* 13, no. 2 (Spring 2010): 39–40, http://iac.dtic.mil/iatac/download/Vol13_No2.pdf.

10. Alexander, "Warfighting in Cyberspace," 60.

11. JP 1, *Doctrine for the Armed Forces of the United States*, 2 May 2007 (incorporating change 1, 23 March 2009), ii, III-12–13, http://www.dtic.mil/doctrine/new_pubs/jp1.pdf.

12. Gen Kevin Chilton, "Remarks to the November 2008 Air Force Association Global Warfare Symposium," http://www.stratcom.mil/speeches/17/.

13. JP 3-14, *Space Operations*, 6 January 2009, III-2, http://www.dtic.mil/doctrine/new_pubs/jp3_14.pdf.

14. Ibid.

15. Ibid., IV-7–8.

16. Ibid., IV-8–11.

17. JP 3-05, *Doctrine for Joint Special Operations*, 17 December 2003, IV-7, http://www.dtic.mil/doctrine/new_pubs/jp3_05.pdf.

18. JP 3-17, *Air Mobility Operations*, 2 October 2009, I-7, 9, http://www.dtic.mil/doctrine/new_pubs/jp3_17.pdf.

19. Ibid., II-2.

20. Ibid., II-4.

21. Ibid., II-4–5.

22. Ibid., II-8.

23. JP 1, *Doctrine for the Armed Forces of the United States*, V-19.

24. House, *Statement of General Keith B. Alexander, Commander, United States Cyber Command, before the House Committee on Armed Services, 23 September 2010*, 111th Cong., 2nd sess., 6–7, http://www.defense.gov/home/features/2010/0410_cybersec/docs/USCC

%20Command%20Posture%20Statement_HASC_22 SEP10_FINAL%20_OMB%20Approved_.pdf.

25. "Mission of U.S. Special Operations Command," accessed 24 September 2010, http://www.socom.mil/SOCOMHome/Pages/About.aspx.

26. JP 1, *Doctrine for the Armed Forces of the United States*, III-12, 13.

27. JP 3-05, *Doctrine for Joint Special Operations*, III-2, 3.

28. Ibid., III-4.

29. Ibid.

30. JP 1, *Doctrine for the Armed Forces of the United States*, V-4.

31. JP 3-05, *Doctrine for Joint Special Operations*, III-9.

32. Ibid., viii.

33. Ibid., III-10.

34. Ibid., III-12.

35. Ibid.

36. Ibid., III-2.

37. Ibid., A-1.

38. For basic information about the school, see "U.S. Air Force Special Operations School," Air Force Special Operations Command, accessed 10 November 2010, http://www.afsoc.af.mil/usafsos/.

39. See "New Undergraduate Cyber Training School Opens," 17 June 2010, accessed 6 December 2010, http://www.keesler.af.mil/news/story.asp?id=123209936; "Graduate School of Engineering and Management, Center for Cyberspace Research (CCR)," accessed 10 November 2010, http://www.afit.edu/en/ccr/; and "Center for Cyber Warfare Established at NPS," accessed 10 November 2010, http://www.nps.edu/Academics/Institutes/Cebrowski/News-and-Events/cybersummit/docs/CyberCenter.pdf.

40. Maj Paul D. Williams, "Cyber ACTS/SAASS: A Second Year of Command and Staff College for the Future Leaders of Our Cyber Forces," *Air and Space Power Journal* 23, no. 4 (Winter 2009): 21–29, http://www.airpower.au.af.mil/airchronicles/apj/apj09/win09/win09.pdf.

The conclusions and opinions expressed in this document are those of the author cultivated in the freedom of expression, academic environment of Air University. They do not reflect the official position of the U.S. Government, Department of Defense, the United States Air Force or the Air University.