APRIL 2014

DISRUPTIVE DEFENSE PAPERS

Digital Theaters

Decentralizing Cyber Command and Control

By Ben FitzGerald and Lt Col Parker Wright, USAF

Center for a New American Security

Acknowledgements

The authors would like to thank Bob Butler and Richard Danzig for their support of this paper. We would also like to thank our CNAS colleagues Shawn Brimley and Liz Fontaine for their excellent editing and production help, and Evan Waranowski for his research assistance.

Cover Image
Illustration by Fred Matamoros for the Center for a New American Security.

APRIL 2014

Digital Theaters

Decentralizing Cyber Command and Control

By Ben FitzGerald and Lt Col Parker Wright, USAF

About the Authors

Ben FitzGerald is a senior fellow and the director of the Technology and National Security Program at the Center for a New American Security.

Lt Col Parker Wright, USAF is a senior military fellow at the Center for a New American Security.

I. INTRODUCTION

By Ben FitzGerald and
Lt Col Parker Wright, USAF

Cybersecurity is now a key priority for the Department of Defense (DOD) and one of the few areas experiencing budget, personnel and capability increases. However, expansion of cyber capability is unlike that of more traditional, mature and well-understood domains. Rapid growth among new cyber organizations raises the real risk that DOD will inadvertently duplicate capabilities, create unnecessary stovepipes or deploy capabilities that it cannot manage effectively. An early focus on command and control (C2) of theater cyber – the cyber capabilities and operations that support combatant commanders – will provide a strong basis for wise decision making and a means to help build cyber capabilities in a strategically coherent manner.

The DOD focus on cyber operations is evident in all areas of defense planning and assessment. Cyber featured prominently throughout the 2014 Quadrennial Defense Review: The total budget for DOD cybersecurity projects is increasing to $5.1 billion, and U.S. Cyber Command (USCYBERCOM) will add 4,000 new personnel to its ranks by 2016. As the DOD cyber footprint expands, one of the biggest challenges for USCYBERCOM will be maturing its approach to C2. If it controls cyber capabilities too tightly, USCYBERCOM risks limiting development. If it controls cyber capabilities too loosely, then it risks their misapplication, with potentially strategic consequences.

Theater cyber is often overlooked in discussions of cyber, which usually emphasize rare, high-end covert "strike" capabilities and the broader challenges of critical infrastructure protection. Within the geographic combatant commands, however, DOD can most rapidly and meaningfully mature its cyber capability and integrate cyber into other military operations. USCYBERCOM must establish a C2 construct for theater cyber that sustains service interests

Second Lt. Stephanie Stanford, 90th Information Operations Squadron cyber development lead, Staff Sgt. Aaron Wendel, 90th IOS cyber network technician, and Senior Airman Brett Tucker, 90th IOS cyber systems operator, perform cyber operations at Lackland Air Force Base, Texas.

(BOYD BELCHER/U.S. Air Force)

and investment, ensures that USCYBERCOM has sufficient ability to oversee and manage cyber operations within a global context and guarantees combatant commanders access to responsive cyber capabilities at the required capacity.

This paper describes potential models, key considerations and recommendations for establishing a mature and effective theater cyber C2 structure.

II. OPERATIONALIZING CYBER

Over the past five years, DOD has made great strides in turning a nascent cyber capability into an operational military tool. As DOD cyber matures, the combatant commanders are eager to leverage this new warfighting capability as part of their theater military campaigns.

Cyber Mission Force

The secretary of defense established USCYBERCOM in 2009 as a sub-unified command of U.S. Strategic Command (USSTRATCOM). USCYBERCOM is tasked to conduct cyberspace operations: "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace."[1] According to joint cyber doctrine, there are three subsets of cyberspace operations:

- Defensive cyberspace operations include "passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems."[2]
- Offensive cyberspace operations are those "intended to project power by the application of force in or through cyberspace."[3,4]
- DOD information network operations are intended to "design, build, configure, secure, operate, maintain, and sustain DOD networks to create and preserve information assurance on the DOD information networks."[5]

By 2016, USCYBERCOM will field 133 cyber mission teams organized into three distinct forces to conduct specified missions to defend national critical infrastructure, protect DOD networks and support combatant commander operations (Figure 1).[6]

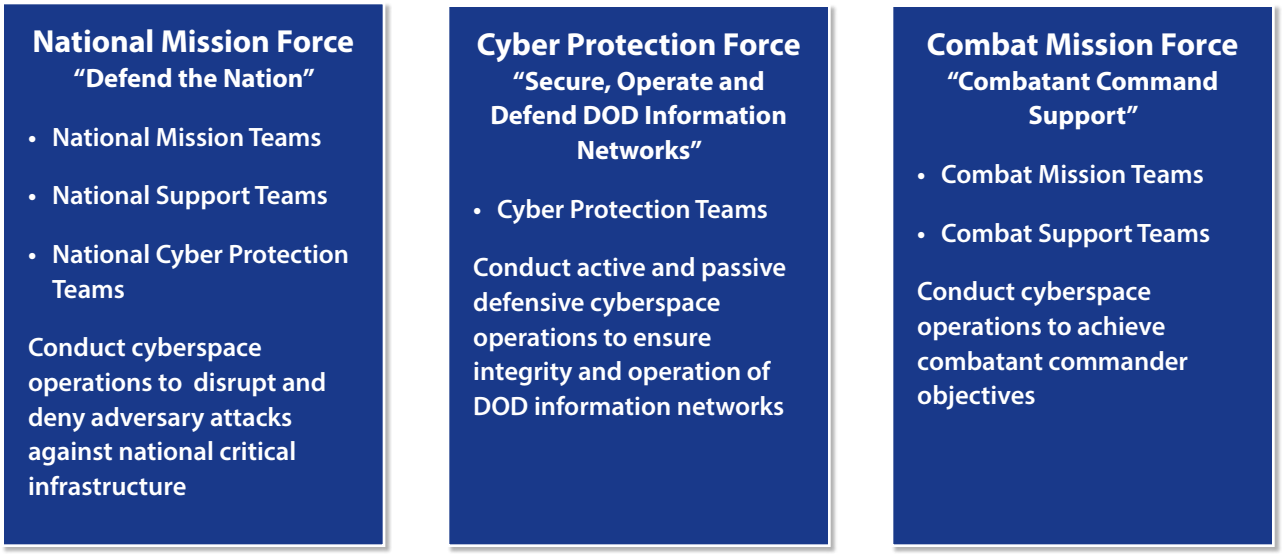
For USCYBERCOM, the cyber mission team is the basic fighting element. They are self-contained service-specific units "analogous to battalions in the Army and Marine Corps – or squadrons in the Navy and Air Force."[7] The cyber mission teams will vary in size from 50 to 100 personnel and will have specified, standardized crew positions to leverage the various skillsets. The teams will be manned predominantly by enlisted forces and commanded by mid-grade officers. Each of the services has established a service component to USCYBERCOM and is developing service-specific cyber cadres to conduct cyberspace operations, some of which will be part of the cyber mission force. Figure 2 shows the major USCYBERCOM, service cyber component and associated units. The total cyber mission force will comprise 6,100 intelligence, communications, electronic warfare, information operations and cyberspace operations personnel.[8]

By 2016, USCYBERCOM will field 133 cyber mission teams organized into three distinct cyber mission forces to conduct specified missions to: defend national critical infrastructure, protect DOD networks and support combatant commander operations.

Theater Cyber

Combatant commanders recognize that cyber is an integral component of their theater military operations. Cyberspace operations allow a commander to project power without detection and with a lower risk to forces and can be used to free up regular forces to accomplish other tasks. Combatant commanders may execute cyberspace operations independently or in concert with other theater forces: "Cyberspace attack capabilities are employed to support maneuver

FIGURE 1: CYBER MISSION FORCE

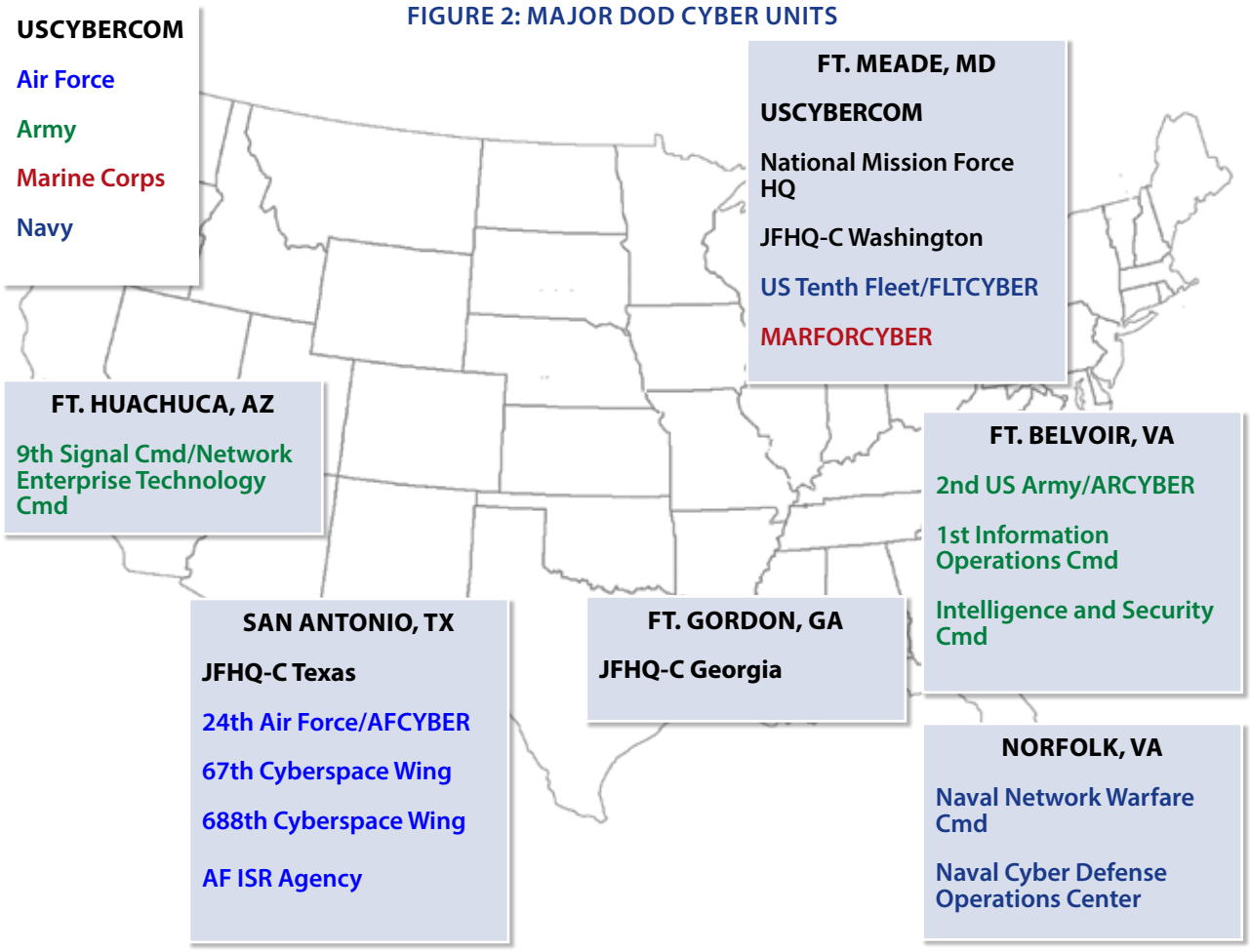


Source: Committee on Armed Services, U.S. Senate, *Advance Questions for Vice Admiral Michael S. Rogers, USN, Nominee for Commander, United States Cyber Command* (March 11, 2014), 37, www.armed-services.senate.gov/imo/media/doc/Rogers_03-11-14.pdf.

operations by creating simultaneous and complementary effects."[9] Theater commanders can employ cyberspace capabilities to impede an adversary's ability to direct its military forces, disrupt or corrupt an adversary's situational awareness, secure surprise by masking the maneuver of friendly forces, seize control of adversary platforms (unmanned air vehicles, satellites, etc.) or processes (logistics, targeting, etc.), degrade an adversary's supporting infrastructure (electricity, fuel, etc.) to create secondary effects, and diminish an adversary's confidence in the integrity and reliability of his command, control and communications systems. USCYBERCOM has dedicated the combat mission force to conduct these operations on behalf of the combatant commanders.

Integrating these theater cyber forces into theater operations challenges the prevailing concept of cyber as a national, strategic capability that is tightly controlled and closely guarded. As the combat mission and combat support teams stand up, it is unclear whether and how they will be integrated into the theater chain of command. To date, USCYBERCOM has relied on a cyber support element (CSE) as its storefront at the combatant commands to synchronize cyber activities with theater operations. The CSEs have proven useful in beginning to integrate cyber into operational planning, but they are not designed to command and control forces. USCYBERCOM has aligned the combat mission and combat support teams under Joint Force Headquarters-Cyber (JFHQ-C) to provide dedicated support to combatant commander operations. JFHQ-C Washington supports U.S. Special Operations Command, U.S. Pacific Command and U.S. Southern Command. JFHQ-C Georgia supports U.S. Central Command, U.S. Africa Command and U.S. Northern Command. JFHQ-C Texas supports U.S. European Command, U.S. Strategic Command and U.S. Transportation Command.[10] Incorporating the combat mission force, the JFHQ-Cs and the CSEs into an effective C2 construct remains one of USCYBERCOM's biggest challenges.

FIGURE 2: MAJOR DOD CYBER UNITS



Sources: U.S. Air Force, "24th Air Force Fact Units and Fact Sheets," www.24af.af.mil/library/factsheets/index.asp; U.S. Army Cyber Command, "Army Cyber," www.arcyber.army.mil; U.S. Navy, "U.S. Fleet Cyber Command: U.S. Tenth Fleet," www.fcc.navy.mil; Committee on Armed Services, *Advance Questions for Vice Admiral Michael S. Rogers;* and U.S. Strategic Command, "U.S. Cyber Command," www.stratcom.mil/factsheets/2/Cyber_Command. Accessed April 2, 2014.

DOD has at various points said that theater cyber will be "under the *command and control* of whichever combatant command to which they are assigned," will be "aligned under one of four Joint Force Headquarters-Cyber in *direct support* of geographic and functional combatant commands," will be "assigned to the *operational control* of individual Combatant Commanders," will "*work together* with regional and functional commanders" and will be "*under the direction* of the regional and functional commanders."[11] Perhaps DOD has a precise definition of theater cyber C2 and is communicating it imprecisely (either intentionally or not). However, there is a risk of confusion as long as DOD continues to use specific terms generically to describe the command relationships between USCYBERCOM and the combatant commanders. Real distinctions exist between directing and commanding and between working together and providing direct support. DOD must begin using accepted joint definitions to describe cyber C2 and must establish a clear and specific C2 structure for theater cyber.

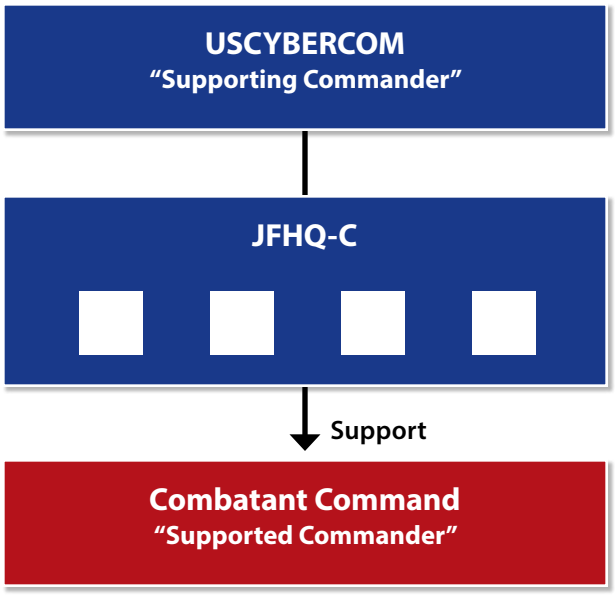
III. COMMAND AND CONTROL MODELS

Despite the unique C2 challenges and opportunities in the cyber domain, existing C2 models serve as important analytic points of reference. Building a C2 structure from existing experience, while accounting for necessary adaptations, offers a means to ground cyber in practical reality. Central to the discussion of theater cyber C2 are the relationships between USCYBERCOM and the combatant commands and the authorities that each will exercise. Command relationships establish "the interrelated responsibilities between commanders" and are defined by operational authorities delegated to the commanders.[12] These include combatant command (COCOM), operational control (OPCON), tactical control (TACON) and support.[13] The following examples describe four existing real-world C2 arrangements that highlight these different command relationships. As presented, they progressively decentralize C2 and shift authority to the combatant commanders.

Space

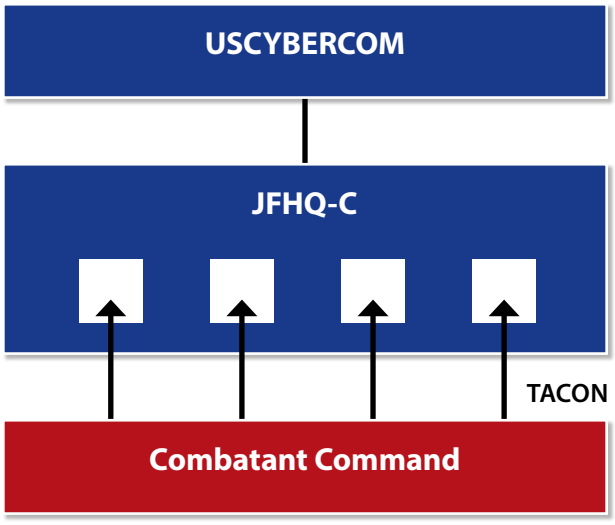
USSTRATCOM, through its joint functional component commander for space (JFCC-Space), is responsible for planning and conducting space operations. DOD designates USSTRATCOM as a supporting commander for other combatant commander operations. As such, USSTRATCOM is "responsible for providing the assistance required by the supported commander," but the combatant commanders have no authority beyond general direction of the supporting effort.[14] A space coordinating authority at each combatant command works with the theater commanders to coordinate and synchronize space operations to support campaign plans and operations. The combatant commanders provide their requirements and request space capabilities in support of their theater operations. JFCC-Space exercises full command authority and C2s all aspects of space operations.

FIGURE 3: SUPPORT MODEL



Applying this "support" model to theater cyber C2 would designate USCYBERCOM a supporting commander for the various combatant commanders' theater operations (Figure 3). A JFHQ-C would command and control the combat mission forces. The combatant commanders would exercise no command authority over any cyber forces, but a "cyber coordinating authority" at each combatant command would synchronize cyber operations to ensure the combatant command's requirements were met. This is the most centralized C2 approach of the four we examine here. A cyber C2 structure modeled on space operations would promote the most efficient application of scarce cyber capabilities and would give USCYBERCOM maximum oversight of, and leverage over, cyber operations. A direct-support C2 model would best enable USCYBERCOM to prioritize cyber operations across the three cyber lines of operation (national, combatant command and protection) and across the various combatant commands to ensure that the highest-priority operations are executed first.

FIGURE 4: TACON MODEL



Global Strike

USSTRATCOM is responsible for integrated global strike operations. USSTRATCOM employs a joint functional component commander for global strike (JFCC-GS) who executes C2 for global strike forces and integrates global strike capabilities into theater operations. JFCC-GS temporarily transfers TACON of designated global strike forces to the geographic combatant commander when those forces are employed as part of a theater campaign. TACON is the authority over forces "that is limited to the detailed direction and control of movements or maneuvers within the operating area necessary to accomplish missions or tasks assigned."[15] This narrowly scoped authority provides the degree of control necessary to direct tactical employment of specified assets.

A similar "TACON" model for theater cyber operations would temporarily transfer TACON of designated combat mission teams to the supported combatant commander when those forces are employed as part of a theater campaign (Figure 4). TACON of those cyber forces would revert back to USCYBERCOM when the supported operations were completed. The combatant commander could thereby give detailed direction to designated cyber forces made available by USCYBERCOM for a specific mission or task. The combatant commander would have a degree of control over the dedicated cyber combat mission force, while USCYBERCOM would retain the authority to manage those forces as part of the global whole through a JFHQ-C. The combatant commander would exercise command and control only in execution, which would allow CYBERCOM to oversee planning and make any necessary operational adjustments based on the overall global cyber effort. USCYBERCOM would have the ability to pull back TACON as required.

Special Operations

U.S. Special Operations Command (USSOCOM) has Theater Special Operations Commands (TSOCs) at each of the geographic combatant commands. USSOCOM transfers OPCON of these theater special operations forces to the combatant commander, who exercises the authority by designating the TSOC commander as a joint forces special operations component commander. OPCON is the "authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission."[16] It excludes authorities for logistics and administration. It may be delegated to and exercised by subordinate commanders at any echelon. TACON is inherent in OPCON (unless transferred). The USSOCOM commander does not exercise C2 of theater special operations but does determine assignment and apportionment of special operations forces to the various combatant commands (in consultation with the combatant commanders). The commander of USSOCOM has routine interaction with the various TSOCs to ensure that they can both leverage and inform the global network of special operations forces.[17]

FIGURE 5: OPCON MODEL

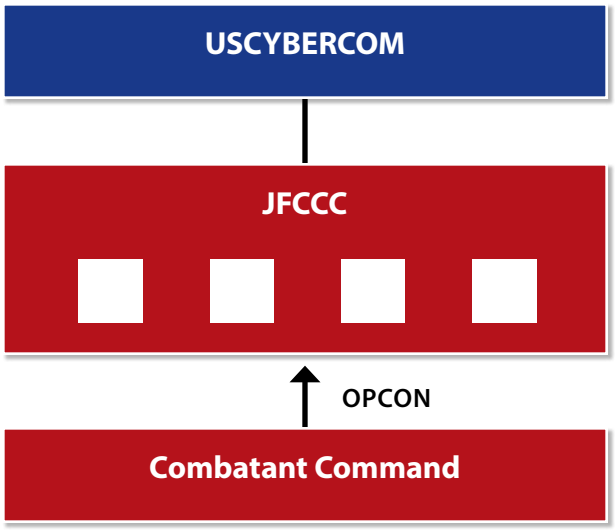
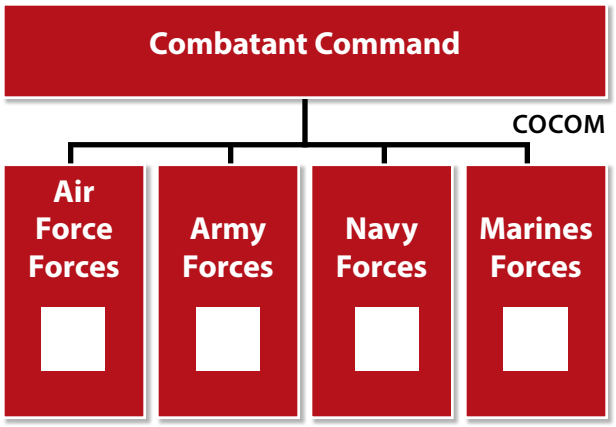


FIGURE 6: COCOM MODEL



Using this "OPCON" model for cyber forces, USCYBERCOM would attach designated cyber combat mission forces to the various combatant commands. It would delegate OPCON of the cyber forces to the combatant commander, who would then designate a joint-force cyber component commander (JFCCC) to exercise cyber C2 (Figure 5).[18] This model dedicates cyber forces for the theater with a level of permanence and establishes a local cyber commander to interface with the combatant commander and components. The transfer of OPCON to the combatant commander would give that commander much greater authority over the cyber force and would leave USCYBERCOM with a more limited ability to oversee cyber operations in that theater. The combatant commander would have further authority to organize this dedicated cyber force and would be able to transfer TACON to subordinate commands and/or establish subordinate cyber commanders. Exercising OPCON would allow the combatant commander to establish operational objectives and organize attached cyber forces, realigning them to another mission area or changing their focus, priorities and preparatory actions. USCYBERCOM would continue to determine the allocation and apportionment of cyber forces to the combatant commanders and would appoint cyber commanders (in consultation with the affected combatant commanders). As in the model for special operations forces, the combatant commander would be responsible for keeping USCYBERCOM informed of theater cyber plans and operations so that USCYBERCOM could direct any necessary changes in line with other cyber efforts. This would entail a robust coordinating element and processes to synchronize operations with USCYBERCOM.

Electronic Warfare. Unlike in the previous three examples, the combatant commanders in this model do not share C2 of electronic warfare forces with another combatant commander. The combatant commanders exercise COCOM of their assigned electronic warfare forces. COCOM is the full command authority that can only be exercised by a combatant commander and cannot be delegated or transferred. Only the combatant commander, exercising COCOM, can give "authoritative direction over all aspects of military

operations, joint training, and logistics necessary to accomplish the mission assigned to the command."[19] TACON and OPCON are inherent in COCOM (unless transferred). As such, the combatant commander, through various service or functional components, operates organic electronic warfare assets. They are not centrally managed but rely on a robust coordination cell to align and synchronize all of the components' electronic warfare activities.

Adopting this "COCOM" approach would require DOD to attach cyber combat mission forces to the combatant commands (Figure 6). The service/functional components would then exercise OPCON of those assigned cyber forces. The combatant commander would establish a cyber coordination cell at the joint-force command headquarters. This model would fully integrate cyber forces into the current component construct and would vest the various component commanders with authorities to execute cyberspace operations. The combatant commanders would exercise COCOM of their assigned cyber combat mission forces. In other words, the combatant commander would "own" the cyber forces as organic capabilities. This is the most decentralized C2 structure of the four considered here. This model fully transfers command authority to the combatant commanders and severs all operational linkages to USCYBERCOM. It would give the combatant commanders authoritative direction for training, logistics and organization of their cyber forces. They could direct theater-specific requirements for their cyber forces and could organize them as needed to accomplish assigned theater responsibilities. USCYBERCOM would continue to manage national missions and cyber operations that cross combatant commander areas of responsibility but would have to rely on robust liaison elements at the combatant commands to keep abreast of theater cyber operations. Most problematic for this arrangement would be the continued delegation of Title 50 authorities to the combat mission force. This would require a legal finding that would allow combatant commanders to exercise statutory authorities given to the director of the National Security Administration (NSA).

Each of these four models applies a different command relationship to meter the degree of authority exercised by the combatant commander in keeping with the specific operational requirements of the particular force. Likewise, DOD must take into account the specific requirements for cyberspace operations as it fashions a unique C2 model for theater cyber.

IV. CONSIDERATIONS FOR THEATER CYBER C2

Command and control of theater cyber forces has a number of unique aspects that make it different from commanding and controlling other theater forces:

- Combat mission forces conduct distributed operations from their home station. They will not deploy to theater – their physical location will not change regardless of the C2 construct employed. Thus, they will operate from a distance, separated from other theater forces and theater commanders.
- Combat mission forces have a global reach not limited by physical geography. Any distinctions among cyber forces will be artificial and not dictated by natural boundaries.
- Maneuver in cyberspace is virtual. There is no distance to travel, so cyber actions occur almost instantaneously.

Commanding and controlling cyber combat mission forces in this unique operating environment requires DOD to build a unique C2 superstructure. To do so, DOD must find a balance between centralizing C2 at USCYBERCOM and pushing C2 to the combatant commanders. Demands for unity of effort, force responsiveness, force availability and organizational versatility are among the elements that DOD must consider.

Unity of Effort

DOD must manage the competing demands for *functional* unity of effort for global cyber operations and for *geographic* unity of effort for a combatant commander's theater operations.

Because actions taken in cyberspace transit across – and may reverberate beyond – specified geographic areas of responsibility, cyberspace operations must be synchronized to ensure that they do not conflict with other efforts both in cyberspace and beyond. Generating a cyber effect inside a theater requires the cyber force to leverage a global architecture with nodes and potential impacts in many other theaters. A combatant commander may not be aware of or concerned with the impact that desired cyber operations will have on operations in other theaters or on national missions. For example, a cyberspace operation in Central Command could have far-reaching diplomatic consequences in Europe. Avoiding conflicts between operations in cyberspace is not as simple as drawing lines on a map or establishing altitude ceilings. It requires active, dynamic management. This is particularly important given the rate of change in cyberspace and the need to closely manage cyber weapons. Cyber weapons, once used, tend to lose their effectiveness elsewhere. USCYBERCOM must ensure that a cyber action by Pacific Command does not disarm Central Command or vice versa. Functional unity of effort would best enable USCYBERCOM to synchronize and deconflict all cyber operations around the globe to ensure that they are aligned with and reinforce broader U.S. government efforts. Furthermore, the level of interagency coordination required for cyber operations suggests the need for a centralized planning and management structure.

DOD must find a balance between centralizing C2 at USCYBERCOM and pushing C2 to the combatant commanders.

Although military objectives in cyberspace differ among commands, cyberspace capabilities should be developed and employed uniformly given their sensitivity and novelty. GEN Keith Alexander,

The Red Flag 14-1 cyber protection team works on defense procedures inside the Combined Air and Space Operations Center-Nellis during the exercise, at Nellis Air Force Base, Nev.

(SENIOR AIRMAN BRETT CLASHMAN /U.S. Air Force)

previous Commander of USCYBERCOM, has expressed his desire to build a "high-quality, certified, and standardized force" that is "trained to common and strict operating standards."[20] As cyber capabilities migrate to the combatant commands for the first time, encouraging a functional unity of effort can ensure that the cyber force as a whole matures in a concerted and coordinated fashion. Functional unity of effort promotes quality control, promulgates best practices across the cyber force and avoids the misapplication of cyber within a theater. USCYBERCOM can ensure that cyber forces will be employed as intended and designed. A well-meaning but uninformed combatant commander may not utilize his cyber force to the full extent possible. Furthermore, USCYBERCOM must enforce operational security and operational discipline given the sensitive techniques and methods employed and the desire to avoid attribution.

Meanwhile, a combatant commander must fully integrate cyber capabilities into operational planning to ensure that cyber is directed toward the command's operational objectives and synchronized with the command's other capabilities. Although USCYBERCOM is concerned with global cyber operations, the geographic combatant commanders have unique perspectives, responsibilities and requirements for their respective theaters. To realize the full potential of cyber capabilities, the combatant commands must institutionalize cyber operations alongside their other theater warfighting functions. This begins with operational planning. A combatant commander creates unity of effort through detailed operational planning that aligns various forces to accomplish specified objectives. In contrast to functional unity of effort, geographic unity of effort synchronizes designated cyber forces with other theater forces to ensure that all of the

combatant commander's capabilities are working in unison to meet his priorities.

Responsiveness

DOD must build in levers to make theater cyber forces sufficiently responsive to USCYBERCOM, the combatant commanders and the military services.

USCYBERCOM must exercise sufficient oversight and control of the special authorities and sensitive capabilities with which it has been entrusted. In the absence of established norms of behavior, USCYBERCOM cannot be sure how an adversary (or an ally) will react to its cyberspace operations. As such, cyber operations pose a high risk of unintended strategic consequences. USCYBERCOM must exercise sufficient C2 of theater cyber forces to effectively manage thresholds and avoid unintended escalation. USCYBERCOM must maintain a vantage point to anticipate and mitigate second- and third-order effects and ensure that cyber effects do not reverberate beyond intended targets. Furthermore, USCYBERCOM must ensure compliance with all applicable laws, statutes and regulations. USCYBERCOM has been delegated authorities by the NSA director that are critical to conducting cyberspace operations.[21] Cyber forces must responsibly exercise those delegated authorities, with USCYBERCOM providing the appropriate oversight to guarantee strict accountability and adherence to all applicable statutes.

Combatant commanders must be able to dynamically direct cyber forces in concert with their other joint forces as the battlespace evolves. Cyberspace operations happen at the speed of light. Combatant commanders need the ability to command and control their designated cyber forces with similar speed. Any C2 structure that employs multiple chains of command or requires multiple approvals before acting will be too slow for cyberspace operations. The designated combat mission teams must be responsive to the combatant commander in execution. As a campaign proceeds, a combatant commander must be able to adjust cyber operations to synchronize with other forces' maneuvers and fires. The line between offense and defense in cyberspace can change quickly. Combatant commanders must be able to thrust and parry in cyberspace, and the C2 structure must support the smooth transition between the two.

Meeting military service cyber requirements is key to sustaining critical service investment in the development of cyber capability. The military services provide the trained cyber forces that USCYBERCOM employs. Although part of the joint cyber team, the services nonetheless expect that their service requirements and those of their service components at the combatant commands will be met in kind with their joint force contribution. If service cyber requirements are underserviced, the services will question their investment. For the services, cyber is a zero-sum game. Every additional unit of cyber costs them another unit of capacity elsewhere in the force. A theater cyber C2 structure that obscures service contributions or weakens the link between the service, its operational cyber units and its various service component requirements risks losing service interest and investment in developing cyber.

Availability

Cyber cannot be limited to strategic applications; it must be available at the operational and tactical levels. DOD must ensure that the combatant commanders have assured access to theater cyber forces at sufficient capacity. Cyber is a specialized capability that needs a dedicated cadre that is neither isolated from, nor independent of, the other combat arms.

Combatant commanders will plan for and employ cyber capability only when they are confident that it will be available in sufficient quantities when called upon. USCYBERCOM recognizes the need to present forces that the combatant

commanders can count on: "forces they can train with, plan for, plan on, and employ like forces and units in any other military domain."[22] If combatant commanders cannot rely on the cyber force, they will be less inclined to integrate it into campaign plans. Furthermore, combatant commanders want guaranteed cyber capability with a level of permanence, not one that is doled out by USCYBERCOM. Standing relationships generate familiarity and build trust between the cyber force and the combatant commander. Although combatant commanders need not exercise full command authority of their designated cyber forces in order to have guaranteed cyber support, a combatant commander's comfort level with the command arrangement will influence the use of dedicated cyber forces.

Cyber is a specialized capability that needs a dedicated cadre that is neither isolated from, nor independent of, the other combat arms.

Combatant commanders prefer a local, empowered cyber commander and a dedicated cyber force. Coordinating with a distant USCYBERCOM commander can be cumbersome. Combatant commanders prefer someone within reach. Most commanders are as interested in "choke-con" – the ability to physically reach a subordinate commander – as they are with any of the official command relationships.[23] A collocated cyber commander will have a higher affinity for the combatant commander and be predisposed to respond to that commander's needs first. One indicator of this is whether the cyber commander takes daily direction from the combatant commander or from the USCYBERCOM chain of command. If the principle cyber leader with whom the combatant commander interacts is neither an empowered commander nor easily accessible, then the combatant commander will rely less on viable cyber capabilities and revert to traditional methods of waging war.

Cyber cannot be stovepiped at the operational level; it must be pushed to the tactical level if cyberspace operations are to become a viable and reliable military option. If cyber is viewed as a separate and distinct capability that is managed independently, then the air, land and maritime components will be less inclined to leverage it. Pushing capability and authority to the tactical level will encourage cyber employment, innovation and unanticipated applications. Fielded units are more likely to develop and nurture tactical applications and to envision new ways of employing cyber at the tactical level. They know where cyber could be applied to replace or reinforce current service capabilities, and they have a better understanding of the systems and processes unique to their service. Moreover, a cyber stovepipe will produce joint requirements that no capability provider wants to fund because it is not receiving a demand signal from the field.

Versatility

DOD must determine the degree of flexibility that it wants to incorporate into the C2 structure for theater cyber. This will require tradeoffs between a specialized workforce that aligns service cyber elements to service component requirements and a general workforce that is able to fulfill the range of combatant commander requirements.

Specialized combat mission and combat support teams enable a division of labor among the services to provide a tailored cyber capability based on specific subject matter expertise. Rather than fielding a team of generalists, service-aligned cyber would

provide depth of expertise, including unique institutional perspectives and an appreciation of service values, priorities and requirements. Service-unique cyber teams would have a better understanding of how their particular service operates and employs its forces and the same for their adversary counterparts. Service-unique cyber teams would enjoy a shared trust and understanding with their service compatriots. The former chief of staff of the Marine Forces Cyber Command suggests, "While there will be some associated skills for cyber, they will remain Marines first, cyber warriors second."[24]

In contrast, a uniform cyber force with interchangeable teams is inherently flexible and efficient, giving the cyber commander the ability to dynamically direct cyber capacity against the commander's highest-priority tasks. A standardized cyber workforce would give maximum flexibility to the cyber commander to address the highest-priority requirements with any combat mission team, regardless of service. It would increase the combat mission force's agility to dynamically shift to more pressing requirements. Pooling commander requirements to be serviced by any available combat mission team takes advantage of distributed operations to mass cyber forces against the commander's priorities. The ability to dynamically "lift and shift" scarce cyber resources to where they are most needed would produce efficiencies within the force, whereas much of the dedicated cyber force may be left on the sidelines if it is segregated among the various components. This option would also give USCYBERCOM greater flexibility in allocating service contributions to the various combatant commanders. Services would not be required to field unique teams at every combatant command.

V. RECOMMENDATIONS

In reality, the theater cyber C2 structure that DOD implements will be determined less by technical or theoretical merits than by the bureaucratic interplay between USCYBERCOM, the military services and the various combatant commanders. The compromise solution must successfully balance each of their equities. Nonetheless, evaluating the existing C2 models and taking into account the considerations above suggests a "best fit" for theater cyber.

DOD and Congress should take the following steps to establish a mature and effective C2 structure that responsibly decentralizes C2 of theater cyber forces.

USCYBERCOM SHOULD EXERCISE COCOM BUT DELEGATE OPCON OF COMBAT MISSION FORCES TO THE COMBATANT COMMANDERS

USCYBERCOM must decide to what extent it will decentralize command and control of cyber operations. A "support" arrangement modeled on space operations would centralize cyber C2 at USCYBERCOM. At the other end of the spectrum, a structure like that for electronic warfare, which gives the combatant commander full command authority, would fully decentralize cyber C2. Considering the need for both USCYBERCOM and the combatant commands to exercise a degree of C2 over the theater cyber force, neither approach is viable. USCYBERCOM and combatant commander requirements do not allow for true unity of effort. Sharing authority at the expense of either functional or geographic unity of effort balances global cyber and theater demands for responsiveness.

USCYBERCOM should therefore follow the Special Operations model and transfer OPCON of theater cyber forces to the combatant commanders. Giving combatant commanders TACON of their designated cyber forces would make the forces more responsive to direction during execution of theater operations. Although keeping OPCON at USCYBERCOM eases oversight of global cyber operation, it forces combatant commanders to reach back to USCYBERCOM to direct cyber activities. Instead, giving OPCON to the combatant commanders would give them the greatest assurance that cyber capabilities will be available when needed. It makes cyber a theater capability rather than a strategic capability that the combatant commander can request. It also ensures that cyber capabilities are fully integrated into local planning and aligned with theater operations. Doing so, however, increases risk for USCYBERCOM because it weakens their oversight of delegated Title 50 authorities and complicates their synchronization of global cyber efforts.[25] USCYBERCOM would have to manage this risk with routine coordination with the geographic combatant commands' cyber forces, much as SOCOM does with the TSOCs. Also, DOD and USCYBERCOM would need to provide detailed rules of engagement to manage the exercise of these cyber authorities within proscribed limits. USCYBERCOM should retain the ability to manage the first-use of sensitive cyber weapons to preserve operational surprise and viability for higher priority operations in the future. Congress should affirm the combatant commanders' ability to command, not merely direct, theater cyber forces and remove any statutory obstacles to the effective exercise of theater cyber C2.

COMBATANT COMMANDERS SHOULD ESTABLISH JOINT FUNCTIONAL CYBER COMPONENT COMMANDS

A combatant commander needs a single, local cyber commander to ensure unity of effort within the combatant command. DOD cannot rely on a planning cell to link USCYBERCOM and the combatant commands; it must have empowered theater cyber commanders who answer to the combatant commanders. Under the JFHQ-C construct, the service cyber component commanders act both as the commanders of their service's cyber component and as joint-force headquarters commanders. Similar to the JFCC-Space and JFCC-Global Strike arrangements, this gives each combatant

commander a single cyber commander with whom to coordinate supporting cyber operations.

This construct, however, makes transferring OPCON of theater cyber forces to the combatant commanders problematic. Because USCYBERCOM will only be able to field at most four JFHQ-Cs (one per service component), each will have to support multiple combatant commanders simultaneously. As a result, they will not be collocated with their supported combatant command. If the JFHQ-Cs neither deploy forward nor support a single combatant commander, it would make sense to establish a cyber component commander at the combatant command.[26]

The presence of distinct functional cyber components at the combatant commands would ground cyber as an equal fighting force within a combatant command and give the cyber commander an equal seat at the table with the other component commanders.[27] A cyber functional component would be a full member of the combatant command team, which is distinctly different from having a separate joint functional component at USCYBERCOM. Furthermore, this option helps to mature cyber warfighting as an integral part of combatant command operations. Establishing a cyber component would centralize cyber planning and execution within the combatant command and give the other components a focal point to synchronize cyber activities.[28] It would also further institutionalize cyber as a warfighting domain and nurture the development of a specialized but integrated cyber cadre. Thus, USCYBERCOM would not need to employ JFHQ-Cs for the combat mission force. All administrative actions for the respective teams could be performed by the service cyber components.

USCYBERCOM SHOULD FIELD SPECIALIZED, SERVICE-ALIGNED COMBAT MISSION AND COMBAT SUPPORT TEAMS

Because DOD is unlikely to assign COCOM of cyber forces to the combatant commanders as it does for electronic warfare, USCYBERCOM will need to find a way to bridge the gap between operational cyber and tactical cyber. Otherwise, cyber will not be integrated into theater operations or resourced and supported by the military services. DOD must avoid stovepiping cyber in the joint force cyber component and segregating it from the rest of the command's forces. One way to do that is to align the combat mission teams to support their service elements at the combatant commands.[29] A service-aligned force would employ combat mission teams from a particular service in support of elements from the same service by targeting adversary counterparts. For instance, Air Force combat mission teams would support air component requirements in support of an air attack by targeting enemy air force networks. Cyber forces should have common standards but specialize in a way that leverages service-unique capabilities and allows an appropriate division of labor while retaining some ability to shift to the highest-priority tasks.[30] Although it is the most efficient option, a versatile force does not

Petty Officer 2nd Class Ryan Allshouse uses the intrusion detection system to monitor unclassified network activity from the automated data processing workspace aboard the aircraft carrier *USS Ronald Reagan*. IDS is part of the integrated shipboard network system and serves as an important computer network defense enabler protecting the unclassified shipboard network from cyber attack.

(U.S. Navy Photo)

engender the kind of trust necessary for combatant commanders to fully adopt and integrate cyber at the theater level. A service-aligned force sacrifices versatility to nurture continued service investment, creates permanence to build trust with combatant commanders and builds the tactical linkage required to mature cyber application in military campaigns. USCYBERCOM should establish common training, certification and qualification standards and then allow the services to field those teams to reflect the unique character and capabilities of their service.

What cyber would lose in efficiency by dedicating service forces to service requirements, it would gain in terms of integration. Retaining dedicated capacity for cyber is critical given the amount of preparatory work that must be done to enable cyber operations. If cyber forces are pulled from firefight to firefight, vital operational preparation of the cyber battlespace may be neglected. Furthermore, linking operational cyber and service components will give the services a vested interest in cyber requirement generation, innovation, funding and capability development. If the service cyber elements are not tethered to their parent service elements, they risk becoming disconnected from the larger force and may, in time, migrate away from providing the tailored support that is needed.

DOD SHOULD ESTABLISH USCYBERCOM AS A FULL UNIFIED COMMAND BUT RETAIN THE DUAL-HATTING ARRANGEMENT FOR THE NSA DIRECTOR AND THE COMMANDER OF USCYBERCOM ONLY UNTIL CYBER IS EFFECTIVELY ESTABLISHED AS A FIGHTING FORCE

None of the four models we explore here suggests an answer to the question of whether or not the NSA director and USCYBERCOM commander should be dual-hatted, nor do they suggest a requirement to maintain an expanding USCYBERCOM as a subunified command under USSTRATCOM. Eliminating the cumbersome C2 relationship with USSTRATCOM would streamline C2 of the cyber mission force and ease decentralization of C2 for the combat mission force. There are also good reasons to appoint a separate NSA director and USCYBERCOM commander. The threat of consolidating too much power in a single individual should not be the driving force behind such a decision. Nor does the fact that NSA and USCYBERCOM leverage a common infrastructure require that the same individual command both organizations. The principle challenge is a matter of span of control. It remains to be seen whether one person can effectively manage a fully-staffed functional combatant command and the NSA at the same time. Furthermore, a single individual cannot adequately represent each organization's competing equities to the full extent. Last, and perhaps most important, the missions of NSA and USCYBERCOM are distinctly different. Although they both leverage cyberspace, their intent in doing so is vastly different. NSA is hoping to extract intelligence from cyberspace, whereas USCYBERCOM aims to deliver force in and through cyberspace. Each requires a different mindset.

For the time being, however, it appears that retaining the dual-hatting arrangement is prudent. The most compelling argument for dual-hatting is the NSA legal authorities that USCYBERCOM can more easily leverage because the two organizations' chains of command intersect at the top. Furthermore, having the same boss certainly encourages the two organizations to cooperate in a way that they may not otherwise do with separate commanders. Until cyber is fully established as a military capability with mature processes and cadres, keeping both organizations under the command and control of a single individual would minimize bureaucratic conflict in cyberspace and avoid unnecessary legislative battles over extending statutory authorities to USCYBERCOM. Nonetheless, both DOD and Congress should begin laying the groundwork to facilitate ending the dual-hatting of the NSA director and USCYBERCOM commander in the not-too-distant future.

VI. CONCLUSION

No C2 structure is perfect, and C2 alone does not guarantee effective capability or operations. C2 structures must also constantly evolve to remain effective and relevant. This is especially true in the cyber domain, which is by nature highly dynamic, especially while in its infancy relative to other military disciplines. It is therefore highly unlikely that DOD will settle on a perfect, stable C2 structure on its first attempt.

Despite almost inevitable initial imperfection, and regardless of the particular approach taken, USCYBERCOM, the geographic combatant commanders and the services must formally develop C2 at the theater level and beyond as soon as possible. Failure to commence this process in an intentional, collaborative manner risks creating, and locking in, ineffective or inappropriate C2 and technical architectures that will be difficult to change. Now is the time to seize the initiative and create a platform for success.

ENDNOTES

1. Department of Defense, *Joint Operations,* JP 3-0 (August 11, 2011), GL-8, http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf.

2. Department of Defense, *Department of Defense Dictionary of Military and Associated Terms*, JP 1-02 (November 8, 2010, most recently amended March 15, 2014), 69, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

3. Ibid., 192.

4. According U.S. Army Field Manual 3-38, *Cyber Electromagnetic Activities,* a cyberspace attack may shut off hardware and/or corrupt software: "A cyberspace attack may be directed at information resident in, or in transit between, computers (including mobile phones and personal digital assistants) and computer networks used by an enemy or adversary. Enemy or adversary actors may be denied the ability to use resources or have their information resources used for friendly purposes as a result of a cyberspace attack." Furthermore, a cyberspace attack "may employ capabilities such as tailored computer code in and through various network nodes such as servers, bridges, firewalls, sensors, protocols, operating systems, and hardware associated with computers or processors." Department of the Army, *Cyber Electromagnetic Activities,* U.S. Army Field Manual 3-38 (February 2014), 3-3.

5. DOD, *Department of Defense Dictionary of Military and Associated Terms*, 71.

6. Committee on Armed Services, U.S. Senate, *Advance Questions for Vice Admiral Michael S. Rogers, USN, Nominee for Commander, United States Cyber Command* (March 11, 2014), 37, www.armed-services.senate.gov/imo/media/doc/Rogers_03-11-14.pdf.

7. GEN Keith B. Alexander, Commander, U.S. Cyber Command, testimony to the Committee on Armed Services, U.S. Senate, March 12, 2013, 6, http://www.defense.gov/home/features/2013/0713_cyberdomain/docs/Alexander%20testimony%20March%202013.pdf.

8. Committee on Armed Services, *Advance Questions for Vice Admiral Michael S. Rogers*, 22. Also, the service cyber forces are a mix of uniformed service members, civilians and contractors. Contractors allow the services to field initial or new capabilities quickly while the uniformed cadre matures. Civilians provide longer tours of duty to increase dwell time and expertise, and the military operators afford an operational perspective that the other two do not.

9. Department of the Army, *Cyber Electromagnetic Activities*, 3-3.

10. Committee on Armed Services, *Advance Questions for Vice Admiral Michael S. Rogers*, 22.

11. GEN Keith B. Alexander, Commander, U.S. Cyber Command, testimony to the Committee on Armed Services, U.S. Senate, February 27, 2014, 5, www.armed-services.senate.gov/imo/media/doc/Alexander_02-27-14.pdf; Alexander, testimony to the Committee on Armed Services, March 12, 2013, 6; and Committee on Armed Services, *Advance Questions for Vice Admiral Michael S. Rogers,* 14. Emphasis added.

12. DOD, *Department of Defense Dictionary of Military and Associated Terms*, 46.

13. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States,* JP-1 (March 25, 2013), http://www.dtic.mil/doctrine/new_pubs/jp1.pdf.

14. Ibid., V-8; and DOD, *Department of Defense Dictionary of Military and Associated Terms*, 253.

15. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States,* V-7.

16. Ibid., V-6.

17. The command and control arrangement for theater SOF forces was updated in 2013 to give COCOM of the TSOCs to the commander of USSOCOM. Previously, the TSOCs operated under the COCOM of the combatant commanders. See Andrew Feickert, "U.S. Special Operations Forces (SOF): Background and Issues for Congress" (Congressional Research Service, September 18, 2013), 1, https://www.fas.org/sgp/crs/natsec/RS21048.pdf.

18. See Harry Friberg, "U.S. Cyber Command Support to Geographic Combatant Commands" (Army War College Strategy Research Project, February 3, 2011), http://handle.dtic.mil/100.2/ADA543404. Friberg recommends establishing a joint functional cyber component command modeled on the Theater Special Operations Command.

19. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States,* V-2.

20. Alexander, testimony to the Committee on Armed Services, March 12, 2013, 7.

21. "The ability of USCYBERCOM personnel to operate under delegated SIGINT authorities and leverage the national cryptologic platform is a critical capability, enabling the Command to fully execute its cyberspace mission in an informed, timely, and coordinated manner." Committee on Armed Services, *Advance Questions for Vice Admiral Michael S. Rogers*, 33.

22. Alexander, testimony to the Committee on Armed Services, March 12, 2013, 9.

23. The Air Force's early experience in Afghanistan demonstrates a drawback of virtual presence. See Maj Gen Kenneth S. Wilsbach and Lt Col David J. Lyle, "NATO Air Command-Afghanistan: The Continuing Evolution of Airpower Command and Control," *Air & Space Power Journal* (January/February 2014), 11, http://www.airpower.maxwell.af.mil/digital/pdf/articles/2014-Jan-Feb/SLP-Wilsbach-Lyle.pdf.

24. J.R. Wilson, "MARFORCYBER: Marines Fight in a New Domain," Defense Media Network, January 5, 2012, http://www.defensemedianetwork.com/stories/marforcyber-marines-fight-in-a-new-domain/.

25. Based on his personal interviews with the USCYBERCOM deputy commander and staff judge advocate, David Hathaway finds it unlikely that the authority to execute offensive cyberspace operations would be delegated beyond USCYBERCOM because of the sensitivities involved. See David Hathaway, "The Digital Kasserine Pass: The Battle over Command and Control of DOD's Cyber Forces" (Brookings Institute, July 15, 2011), http://

www.brookings.edu/~/media/research/files/papers/2011/7/15%20cyber%20forces%20hathaway/0715_cyber_forces_hathaway.pdf.

26. U.S. Army Cyber Command anticipates this: "A joint cyber component command aligned to geographic combatant commanders (GCC) will provide the full range of cyber organization requirements of this vision. The Army will align its operational framework to nest with this structure." U.S. Army Cyber Command, *Landcyber White Paper: 2018-2030* (September 9, 2013), 14, http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA592724.

27. LCDR Michael Elliot evaluated the merits of a joint functional cyber component command and found that such a construct scored higher in terms of simplicity, unity of effort and homogeneity than an approach that centralized C2 at USCYBERCOM or one in which C2 of cyber is exercised directly by the joint force commander. LCDR Michael Elliot, "Operational Command and Control of Joint Task Force Cyberspace Operations" (Naval War College, May 27, 2008), http://www.dtic.mil/dtic/tr/fulltext/u2/a484515.pdf.

28. Under a joint functional cyber component construct, the other functional components could establish liaisons at the JFCCC to request and synchronize cyber fires with their schemes of maneuver. This could be similar to liaison elements at the Air Operations Center requesting air support from the JFACC.

29. It does not appear, however, that this is the approach USCYBERCOM has adopted. In his response to advance questions for his confirmation hearing, Admiral Rogers wrote that "targets developed for fires and effects delivered in and through cyberspace do not necessarily correspond with traditional Service domains" and "may require an Army unit to operate against naval or air targets and vice versa." Committee on Armed Services, *Advance Questions for Vice Admiral Michael S. Rogers*, 23. If this is the case, then the service elements will not necessarily align with their service components at the combatant commands and the various component requirements may be pooled at the combatant command for the assigned CMTs to service.

30. Rather than separating the service cyber elements from the service components at the combatant commands, the combatant commander should treat them akin to fleet air defense (FAD) or Marine close air support (CAS). Navy air and Marine air satisfy organic requirements for FAD and CAS first and then contribute any excess capacity to the joint force air component commander to employ as part of the joint force commander's theater air campaign. In a similar fashion, Army combat mission teams would service priority land component commander requirements first, and then satisfy any other joint force commander priorities.

About the Center for a New American Security

The mission of the Center for a New American Security (CNAS) is to develop strong, pragmatic and principled national security and defense policies. Building on the expertise and experience of its staff and advisors, CNAS engages policymakers, experts and the public with innovative, fact-based research, ideas and analysis to shape and elevate the national security debate. A key part of our mission is to inform and prepare the national security leaders of today and tomorrow.

CNAS is located in Washington, and was established in February 2007 by co-founders Kurt M. Campbell and Michèle A. Flournoy. CNAS is a 501(c)3 tax-exempt nonprofit organization. Its research is independent and non-partisan. CNAS does not take institutional positions on policy issues. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the authors.

Center for a New American Security
1152 15th Street, NW
Suite 950
Washington, DC 20005

TEL 202.457.9400
FAX 202.457.9401
EMAIL info@cnas.org
www.cnas.org

Production Notes

Paper recycling is reprocessing waste paper fibers back into a usable paper product.

Soy ink is a helpful component in paper recycling. It helps in this process because the soy ink can be removed more easily than regular ink and can be taken out of paper during the de-inking process of recycling. This allows the recycled paper to have less damage to its paper fibers and have a brighter appearance. The waste that is left from the soy ink during the de-inking process is not hazardous and it can be treated easily through the development of modern processes.

Center for a
New American
Security

STRONG, PRAGMATIC AND PRINCIPLED
NATIONAL SECURITY AND DEFENSE POLICIES

1152 15th Street, NW
Suite 950
Washington, DC 20005

TEL 202.457.9400
FAX 202.457.9401
EMAIL info@cnas.org

www.cnas.org

ISBN 978-1-935087-84-7

Printed on Post-Consumer Recycled paper with Soy Inks