Foreign Policy
at BROOKINGS

The Digital Kasserine Pass:

The Battle Over Command and Control of DoD's Cyber Forces

Colonel David C. Hathaway, US AIR FORCE
FEDERAL EXECUTIVE FELLOW

21st CENTURY
DEFENSE INITIATIVE
POLICY PAPER
15 July 2011

The views expressed in this monograph are those of the author and do not reflect the official policy or position of the Department of the Air Force, Department of Defense, or the U.S. Government.

CONTENTS

Page

ILLUSTRATIONS III

EXECUTIVE SUMMARY IV

CHAPTER 1: INTRODUCTION .... **ERROR! BOOKMARK NOT DEFINED.**

CHAPTER 2: CONTROL OF THE CYBER DOMAIN—CONFLICTING PERSPECTIVES 5

Cyberspace Characteristics 5

DOD Cyberspace Constraints 6

Command Perspectives 7

USCYBERCOM 7

Geographic Combatant Command 8

CHAPTER 3: OPTIMIZING C2 FOR CYBERSPACE MISSIONS 10

USSOCOM Model 10

Advantages of the USSOCOM Model 12

Disadvantages of the USSOCOM Model 13

USTRANSCOM Model 14

Advantages of the USTRANSCOM Model 16

Disadvantages of the USTRANSCOM Model 16

CHAPTER 4: RECOMMENDATIONS 18

CHAPTER 5: CONCLUSIONS 21

GLOSSARY 23

BIBLIOGRAPHY 26

ABOUT THE AUTHOR 28

ILLUSTRATIONS

Page

FIGURE 1. USSOCOM Model – Steady State 11

FIGURE 2. USSOCOM Model – Contingency 12

FIGURE 3. USTRANSCOM Model— Steady State 14

FIGURE 4. USTRANSCOM Model—Contingency 15

FIGURE 5. Hybrid Cyber C2 Model — Steady State 18

FIGURE 6. Hybrid Cyber C2 Model — Contingency 19

EXECUTIVE SUMMARY

The dramatic increase in reliance on cyberspace over the last decade for US military operations resulted in the creation of the sub-unified command, US Cyber Command (USCYBERCOM). Its mission is to operate and defend the global information grid and conduct full-spectrum cyberspace operations, if required. However, the regional combatant commands (COCOMs) see cyberspace as another operational domain that they want and need to integrate with the physical domains of air, land, sea, and space. These two perspectives are at odds with each other with respect to the optimal command and control (C2) structure for cyberspace. The challenge is to develop a command and control structure that allows USCYBERCOM to execute its global responsibilities while also allowing the geographic commanders the ability to effectively integrate cyber operations into their plans and operations.

Two predominant models have emerged: the USSOCOM model and the USTRANSCOM model, the former a very regionally focused structure and the latter very centrally focused. In order to determine the best command and control structure for cyberspace within DoD, the author conducted interviews throughout USCYBERCOM, its service components, and several of the unified commands. Additionally, the author observed a tabletop cyber exercise in preparation for US Pacific Command's (USPACOM) annual Exercise Terminal Fury. The author concludes that a hybrid model with features of the regional USSOCOM model and the centralized USTRANSCOM model best takes into account the global nature of cyberspace, while enabling integration of regional cyber effects.

CHAPTER ONE
Introduction

> *We are in the midst of a dramatic change in the relationship between technology and the nature of warfare.*
>
> —David J. Lonsdale

In September 1914, during the Battle of the Marne, the French used airpower to increase the effectiveness of their army, a first in warfare. They used their aircraft to help detect the German army's turn to the northeast of Paris. This significant imbalance in awareness between the opposing sides allowed the French and British forces to strike at the German flank.[1] Ninety-three years later, a similar first in warfare occurred in the skies over Syria. However, this time it was a cyberspace operation that tipped the balance.

On September 6, 2007, a truly integrated cyber and kinetic attack occurred in a remote part of eastern Syria. On that night, Israeli Air Force (IAF) fighter aircraft stormed in from the northeast and attacked a suspected Syrian nuclear weapons facility. The IAF fighters destroyed the facility and escaped back to Israel unscathed.[2] How was this lopsided operation possible? Syrian air defenses, while not the most modern in the world, were certainly sufficient to put up at least some defense. However, the Syrian air defenses did not even react – because on this night the Syrian air defense operators sat looking at essentially blank screens.[3] Nothing appeared out of the ordinary; Israeli cyber operators had completely disabled the Syrian air defense network.[4] The attack in cyberspace against the Syrian air defenses was a critical enabler for the kinetic strike conducted by the IAF. Without the integrated cyberattack, what was a fairly small raid into Syria would have required a much larger force to fend off the Syrian air defenses. It would have required an operation similar in scale to the missile and aircraft strikes on Libyan air defenses executed in March 2011 in preparation for implementation of the US-, UK-, and French-implemented no-fly zone. This larger Israeli strike force would have been seen as much more provocative and fomented more forceful condemnation of the Israeli action. Consequently, it could have escalated into a much larger regional conflict. The integration of the cyber-attack with the kinetic strike generated the desired effect – the destruction of the suspected nuclear weapons facility – while minimizing other potential fallout.[5]

The Israeli-Syrian example shows how an integrated and coordinated cyber operation can be a dramatic force multiplier for kinetic operations. Other examples demonstrate how cyber operations may in themselves create the desired effects and negate the need for kinetic action altogether. In 2007 a Distributed Denial of Service

(DDOS) attack launched from Russia against Estonian government and financial service websites put severe pressure on Estonia's government to stop a planned movement of a Soviet-era statue.[6] More recently, the Stuxnet worm attacked Iranian nuclear facilities, causing physical damage to their centrifuges.[7] These examples illustrate some of the ways cyber operations can affect a potential adversary. However, they also demonstrate the vulnerabilities of these new cyber capabilities and the importance of robust defenses to protect network cyber threats.

While the Israeli-Syrian example demonstrates how a coordinated use of cyber and kinetic attacks can have synergistic effects, it does not illustrate the complexity involved in that coordination. In essence, the Israelis pulled off a raid on one Syrian facility. The coordination for this operation was very simple compared to the coordination required to integrate cyber into a major theater war. But the Israelis and others are now debating the best way to organize and employ cyberspace, recognizing the intelligence functions as well as operational capabilities that reside in this new domain.[8] This includes trying to coordinate, integrate, and deconflict cyber operations in support of hundreds of operations near-simultaneously across all of the physical domains.

The ability to command and control the armed forces has been a recognized critical capability since the introduction of the telegraph, telephone, and radio. With these technologies military leaders were able to wield an unprecedented level of command and control over operations. However, these advances also created vulnerabilities to exploitation, deception, and disruption.[9] Immediately, militaries had to find ways to protect their command and control capability through encryption and redundancy.

Today, in order to increase the span and speed of command and control, nearly all of US military command and control travels on computer networks. Accordingly, what DoD leaders fear most is an attack on the military's networks that would compromise U.S. forces' command-and-control systems, thereby undermining an entire campaign.[10] While the ability to exploit and attack an adversary's networks is important to military offensive effectiveness, operating and defending one's own networks will ensure the viability of what has become a cornerstone of US military capability.[11] However, it is not as simple as developing an operational cyber capability.

In order to effectively capitalize on cyber domain capabilities, the US military must establish the command and control structure to enable cyber superiority just as it does in the physical domains.[12] DoD has tasked US Strategic Command (USSTRATCOM) through its sub-unified command, US Cyber Command (USCYBERCOM), with operating and defending the military's Global Information Grid (GIG) and being prepared to conduct full-spectrum cyberspace operations.[13] However, the geographic combatant commands (GCCs) not only see the cyber domain as something in which they heavily rely on, but also as another warfighting domain that can dramatically influence their regional plans and operations.[14] These two different perspectives lend themselves to very different command and control structures. The challenge is finding the optimal command and control relationship for cyberspace. It must allow USCYBERCOM to conduct its global missions while ensuring that the GCCs have confidence in their networks and can effectively integrate cyber operations into their regional operations.[15]

Developing the optimal command and control structure for cyberspace to support the size and scope of US DoD operations is no simple task; and it is not the first time the military has had to deal with the command and control of emerging capabilities. A similar challenge occurred during WWII in North Africa. Prior to 1943, doctrine had not yet matured to deal with the inherent flexibility of airpower. In the months leading up to the battle at Kasserine Pass in Tunisia, US air forces were allocated in support of specific ground units and essentially employed as airborne artillery. This prevented the most efficient use of limited airpower resources and resulted in significant Allied air and ground force losses.[16] The Allies failed to capitalize on opportunities to achieve longer-term advantages through the establishment of air superiority.[17] The command and control issue boiled down to centralized versus decentralized control of airpower.[18]

Due to the unique characteristics of cyberspace, the argument over centralized control of cyberspace operations is occurring at the COCOM level rather than through airpower doctrine at the GCC component level. This paper explores the current doctrine for cyberspace and the various command and control issues emerging within the cyber domain. It then lays out the advantages and disadvantages of two command and control models for cyberspace, and recommends an optimized way to operate, defend, exploit and attack in cyberspace at both the global and regional level.

Notes

[1] John H. Morrow, Jr., "The First World War, 1914-1919," in *A History of Air Warfare,* ed. John A. Olsen (Washington, DC: Potomac Books, 2010), 6.

[2] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It.*(New York: HarperCollins, 2010), 1-8.

[3] David Eshel, "Cyber-Attack Deploys in Israeli Forces," *Aviation Week*, 15 September 2010. http://www.aviationweek.com/aw/generic/story.jsp?id=news/dti/2010/09/01/DT_09_01_2010_p42-248207.xml&channel=defense.

[4] David A. Fulghum, "No Fingerprints: Culprits in the Cyberattack on Iran Are Still Unknown," *Aviation Week* 172, no. 36 (4 October 2010): 29-30.

[5] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It.* (New York: HarperCollins, 2010), 2.

[6] Ibid.,

[7] Ed Barnes, "Mystery Surrounds Cyber Missile That Crippled Iran's Nuclear Weapons Ambitions," *FoxNews.com*, 26 November 2010, http://www.foxnews.com/scitech/2010/11/26/ secret-agent-crippled-irans-nuclear-ambitions/

[8] David A. Fulghum, "Israel Assesses Changing Threats." *Aviation Week*, 13 August 2010. http://www.aviationweek.com/aw/generic/story.jsp?id=news/awst/2010/08/09/AW_08_09_2010_p42-243720.xml&channel=defense.

[9] Rex Hughes, "A Treaty for Cyberspace," *International Affairs* 86, no. 2 (March 2010): 525-526.

[10] Gen Keith B. Alexander, commander, USCYBERCOM (address, Center for Strategic and International Studies, Washington, DC, 3 June 2010).

[11] Department of Defense, *Quadrennial Defense Review Report*, (Washington, DC: Department of Defense, February 2010), ix.

[12] Brig Gen Brett T. Williams (J-6, USPACOM, Camp Smith, HI), interviewed by author, 21 December 2011.

[13] Department of Defense, *U.S. Cyber Command Fact Sheet*, (Washington, DC: Department of Defense Office of Public Affairs, May 2010).

[14] Brig Gen Brett T. Williams (J-6, USPACOM, Camp Smith, HI), interviewed by author, 21 December 2010.

[15] LtGen Robert E. Schmidle (Deputy Commander, USCYBERCOM, Fort Meade, MD), interviewed by author, 17 December 2010.

[16] Maj Shawn P. Rife, "Kasserine Pass and the Proper Application of Airpower," *Joint Forces Quarterly* 20 (Autumn/Winter 1998-1999): 74.

[17] Ibid., 72.

[18] Ibid.

CHAPTER TWO

Control of the Cyber Domain—Conflicting Perspectives

> *Although attacks in the cybersphere do not involve use of physical weapons, their destructive impacts, physical and otherwise, may be no less lethal to societies.*
>
> —Jeffrey R. Cooper

The application of existing command and control models is complicated by the unique characteristics of operations in the cyberspace domain, making selection of a command and control structure for cyberspace more difficult than for other warfighting domains.

Cyberspace Characteristics

The first unique characteristic of cyberspace operations is the speed at which they can occur. When we think of time for US ground and sea power operations, we think in days or even weeks depending on the location of forces. US airpower boasts global reach and can generate effects in hours and at best minutes. However, none of the physical domains can match the speed of cyber. When talking about cyber effects, one talks in fractions of a second. Traveling at the speed of light, cyber effects can traverse the globe in about 0.17 seconds[1] – about the time it takes to blink.

The second unique characteristic of cyber is the lack of geographic relevance. Cyber operators are not tied to a specific geographic location. For example, cyber operators generating effects for USPACOM can in most cases be just as effective operating from Texas as from Hawaii.[2] Additionally, operators attacking US networks are just as unconstrained by geography. Using the USPACOM example, there is no reason to expect an attack initiated by a country in the USPACOM area of responsibility (AOR) to actually emanate from within the USPACOM AOR. Instead, an attacker could employ bots within virtually any country as the mechanism of the attack. As an illustration, the Russian invasion of Georgia following Georgia's 2008 attempt to reign in the separatist territories of South Ossetia and Abkhazia was accompanied by a persistent Distributed Denial of Service (DDOS) attack that shut down access to most Georgian government websites and put pressure on the government by disrupting Georgia's banking system.[3] The attack incorporated six botnets made up of thousands of computers from around the world owned by mostly unwitting citizens.[4] As a result, the DDOS attack, while initiated from within Russian territory and thus the US European Command

(USEUCOM) area of responsibility, ended up emanating from various countries outside of EUCOM, including the United States.[5]

The third unique characteristic of operations in cyberspace is their potentially viral nature. While there is always potential for collateral damage with the employment of kinetic operations in the physical domains, this does not match the potential for globalized collateral damage that malicious software can cause within cyberspace.[6] It can be difficult to limit the scope of an attack in cyberspace. While a cyber operation may target a specific network or control system, the tool used may easily spread and damage other unintentional and possibly friendly systems. The Stuxnet worm that attacked Iran's nuclear facilities illustrates this potential.

In June 2010, Iran was attacked by the most precise cyber weapon seen to date, the Stuxnet worm. Experts describe Stuxnet as an incredibly advanced, undetectable computer worm. They estimate it took years to develop and was designed to propagate from computer to computer until it found Iran's nuclear enrichment program.[7] What made Stuxnet different from the DDOS attacks employed against Estonia in 2007 and Georgia in 2008 were the physical effects created outside the cyberspace domain. Stuxnet worked its way into the computer networks of the Iranian nuclear facilities until it reached the control systems it was uniquely designed to manipulate and forced the centrifuges to operate at incorrect speeds. It did all this while hiding its activities from the control panels and those monitoring them.[8]

Even with the Stuxnet worm's precision and given the fact that the Iranian nuclear control systems were air-gapped, Stuxnet still did not remain isolated to Iran's nuclear facilities: as of February 2011, Stuxnet had infected over 60,000 computers. While over half of these were Iranian computers, known infections occurred in Australia, Azerbaijan, China, Finland, Germany, India, Indonesia, Malaysia, South Korea, the United Kingdom, and the United States.[9] While the infections in most of these countries have been mitigated by the use of effective antidotes, the fact remains that even a worm designed to target a precise control system can still inflict significant collateral damage; and this damage is not bound by country borders or regional limits.

While these characteristics impact the type of command and control best suited for cyberspace, other factors within DoD also influence the decision.

DoD Cyberspace Constraints

One factor that weighs heavily on the type of command and control structure that DoD selects for cyberspace is personnel. The first personnel issue is the availability of trained cyber operators. A relatively small pool of cyber experts within DoD comprises the agency's ability to tackle advanced computer network defense, attack, and exploitation techniques.[10] As the services actively build their cyber capabilities, this factor still influences DoD's command and control options, at least in the near-term. The second personnel issue is that creating a cyber force is a zero-sum game. USCYBERCOM and the services cannot expect an increase in service personnel end strength to accommodate the increased cyber force requirement. In other words, for every trained cyber warrior created, a service must give up an individual accomplishing another mission.[11] While DoD may be able to find creative ways to employ a civilian, National Guard, or reserve work force to augment the growing needs in cyberspace requirements, there will still likely be pressures to limit the growth of DoD in support of these emerging requirements.

Another factor influencing the cyberspace command and control issue is the architecture of the networks within DoD. Cyberspace within DoD is made up of 15,000 different networks used globally for the over 4,000 installations. At any given time, the services are supporting connectivity for as many as seven million computers and telecommunications tools operating in 88 different countries.[12] To complicated matters, the services organize and manage these networks differently – each service has attempted to organize their networks to best meet the needs of the warfighters they support. For example, this has led to a very centralized control structure within the Air Force, whereas the Navy has chosen a more dispersed structure better suited for fleet operations.[13]

These differing architectures, while optimized for service functions, don't necessarily align themselves well with GCC boundaries. That said, cyberspace is a man-made domain; therefore, the services could restructure the network architecture as needed.[14] But attempting to build artificial boundaries in cyberspace would require an unsupportable number of resources. Essentially, the services would have to recreate network operations centers in each GCC with the associated network administrative personnel and equipment, creating insurmountable inefficiencies.[15] Regardless of whether the services choose to undertake the arduous task of restructuring their networks, the network architecture does impact the selection of a command and control structure for cyberspace.

Command Perspectives

The emergence of cyberspace capabilities and vulnerabilities has led to conflicting perspectives within DoD on requirements driven by USCYBERCOM's global mission and the geographic combatant commands' regional mission.[16]

USCYBERCOM

Recognizing that the US military's heavy reliance on cyberspace has created significant opportunities and vulnerabilities, the DoD created USCYBERCOM, which became fully operational in November 2010 and is a sub-unified command under

USSTRATCOM. It is charged with operating and defending the US military's global information grid (GIG) and executing full spectrum cyber operations, if required, to ensure US freedom of movement in all domains.[17] USCYBERCOM is tasked to lead DoD efforts to:[18]

1. Develop a more comprehensive and coherent cyberspace approach;
2. Improve cyber expertise and awareness throughout the force;
3. Centralize command of cyberspace; and
4. Expand partnerships with other governments and US agencies.

With the standup of USCYBERCOM came the assignment of the service cyber forces to USCYBERCOM: AFCYBER (24th Air Force), ARFORCYBER, MARFORCYBER, and NAVFORCYBER (10th Fleet) make up USCYBERCOM's pool of trained cyber forces. These forces provide and operate the 15,000 different military networks used globally.[19]

In line with the tasking USCYBERCOM has been given, it naturally views cyberspace from a global perspective. It sees threats that easily traverse sovereign state boundaries and have the potential to wreak havoc for very little investment by the aggressor. To USCYBERCOM, the global nature and speed of cyber operations necessitates a more centrally controlled and executed structure.[20] This varies significantly from the GCC perspective.

Geographic Combatant Command

The geographic combatant commands are tasked with carrying out DoD missions within a specific region of the world. The Presidentially approved Unified Command Plan (UCP), along with defining the regional boundaries, defines each GCC commander's authority and establishes command relationships. The GCC has combatant command (COCOM), operational control (OPCON), and/or tactical control (TACON) of physical-domain military forces operating within their assigned AOR. This allows the GCC commander to direct forces in accordance with the authorities granted in the UCP to generate effects in defense of US interests in their AOR.[21] The GCCs, in conjunction with their service components, are responsible for integrating the physical domains into a coherent joint plan to create those desired effects. However, the cyberspace domain is not as easily integrated.

The GCCs face a challenge with respect to integrating the cyberspace domain into their plans and operations; they don't own the computer networks on which they rely. This is because the services have historically provided and operated the GCC networks as a support function. While the GCCs define their network requirements, it has been up to the services to provide that capability. However, there is more to cyberspace operations than just providing and operating networks in what the DoD has classified and an operational domain. The five facets of cyberspace operations are: provide, operate, defend, exploit, and attack. In order for the GCC to have a credible capability in each of these facets, different command relationships and authorities will be required than have historically been provided through the service support functions.

Notes

[1] Col David T. Fahrenkrug, (Director, Strategic Studies Group, Headquarters Air Force), interviewed by author, 16 September 2010.

[2] Brig Gen Charles K. Shugg (24th Air Force Vice Commander, Lackland AFB, TX), interviewed by author, 16 December 2010.

[3] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It.* (New York: HarperCollins, 2010), 17-21.

[4].Ibid.

[5] Ibid.

[6] Ibid., 202-203.

[7] Ed Barnes, "Mystery Surrounds Cyber Missile That Crippled Iran's Nuclear Weapons Ambitions," *FoxNews.com*, 26 November 2010, http://www.foxnews.com/scitech/2010/11/26/ secret-agent-crippled-irans-nuclear-ambitions/

[8] Richard A. Clarke, Former Special Advisor on Cyber Security to President George W. Bush. (address, American Association for the Advancement of Science, Washington, DC, 22 November 2010).

[9] James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival: Global Politics and Strategy* 53, no. 1 (February-March 2011): 23.

[10] Michael Clark (Deputy J-5, USCYBERCOM, Fort Meade, MD), interviewed by author, 21 December 2011.

[11] Vice Admiral Bernard J. McCullough, commander, US Fleet Cyber Command (address, Government Executive Cybersecurity Insider Series, Washington, DC, 14 Dec 2010).

[12] James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival: Global Politics and Strategy* 53, no. 1 (February-March 2011): 37.

[13] Brig Gen Charles K. Shugg (24th Air Force Vice Commander, Lackland AFB, TX), interviewed by author, 16 December 2010.

[14] Brig Gen Brett T. Williams (J-6, USPACOM, Camp Smith, HI), interviewed by author, 21 December 2010.

[15] Col Victor J. Diaz Jr. (commander, 624th Operations Center, Lackland AFB, TX), interviewed by author, 10 March 2011.

[16] Michael Clark (Deputy J-5, USCYBERCOM, Fort Meade, MD), interviewed by author, 21 December 2011.

[17] Department of Defense. *U.S. Cyber Command Fact Sheet*, (Washington, DC: U.S. Department of Defense Office of Public Affairs, 2010).

[18] Department of Defense. *Quadrennial Defense Review Report*, (Washington DC: Office of the Secretary of Defense, February 2010), ix-x.

[19]Ibid., 37.

[20] Michael Clark (Deputy J-5, USCYBERCOM, Fort Meade, MD), interviewed by author, 21 December 2011.

[21] Department of Defense, "DefenseLINK: Unified Command Plan," http://www.defense.gov/specials/unifiedcommand/ (accessed 1 Mar 2011).

Chapter Three

Optimizing C2 for Cyberspace Missions

Considered together, the unique characteristics of cyber and differing defense command perspectives lead to divergent points of view on the best way to command and control cyber forces. As the debate within DoD regarding the optimal command and control relationship continues, senior leaders are discussing many different proposals. However, most proposals are a variation of two models: the US Special Operations Command (USSOCOM) model and the US Transportation Command (USTRANSCOM) model.

USSOCOM Model

Many DoD leaders see parallels between the uniqueness of Special Operations, which led to the creation of the Special Operations Command (USSOCOM), and cyber operations. Both are made up of capabilities from all services; both have global and regional missions; and both have sufficiently unique missions that the DoD determined a special command structure was warranted.

In applying a USSOCOM model to cyberspace (see Figure 1), the primary command relationship is between the GCC and a regional cyber commander (RCC). This is analogous to the relationship between the GCC and the Theater Special Operations Command (TSOC). The RCC would be COCOM to the GCC, responsible for operation and basic defense of the networks in the GCC's AOR. The RCC would also be responsible for integrating cyber effects into regional plans and operations and serving as the primary liaison with USCYBERCOM for inter-agency deconfliction of cyber effects. Furthermore, the RCC would have, at a minimum, OPCON of the service networks, so that the GCC could make risk decisions regarding, for example, the continued use of potentially compromised networks.[1] The integration of cyber effects with GCC plans and Phase 0 operations would be carried out by GCC staff and the GCC's physical-domain components. However, USCYBERCOM would be responsible for manning, training, and equipping all cyber forces, and would also retain responsibility for cyber operations that crossed the GCC's regional boundaries. If required, USCYBERCOM would be able to coordinate with the RCC in support of global operations. USCYBERCOM would also support the RCC if it required additional capability in support of the GCC's Phase 0 operations. This would be accomplished through established supported/supporting relationships.

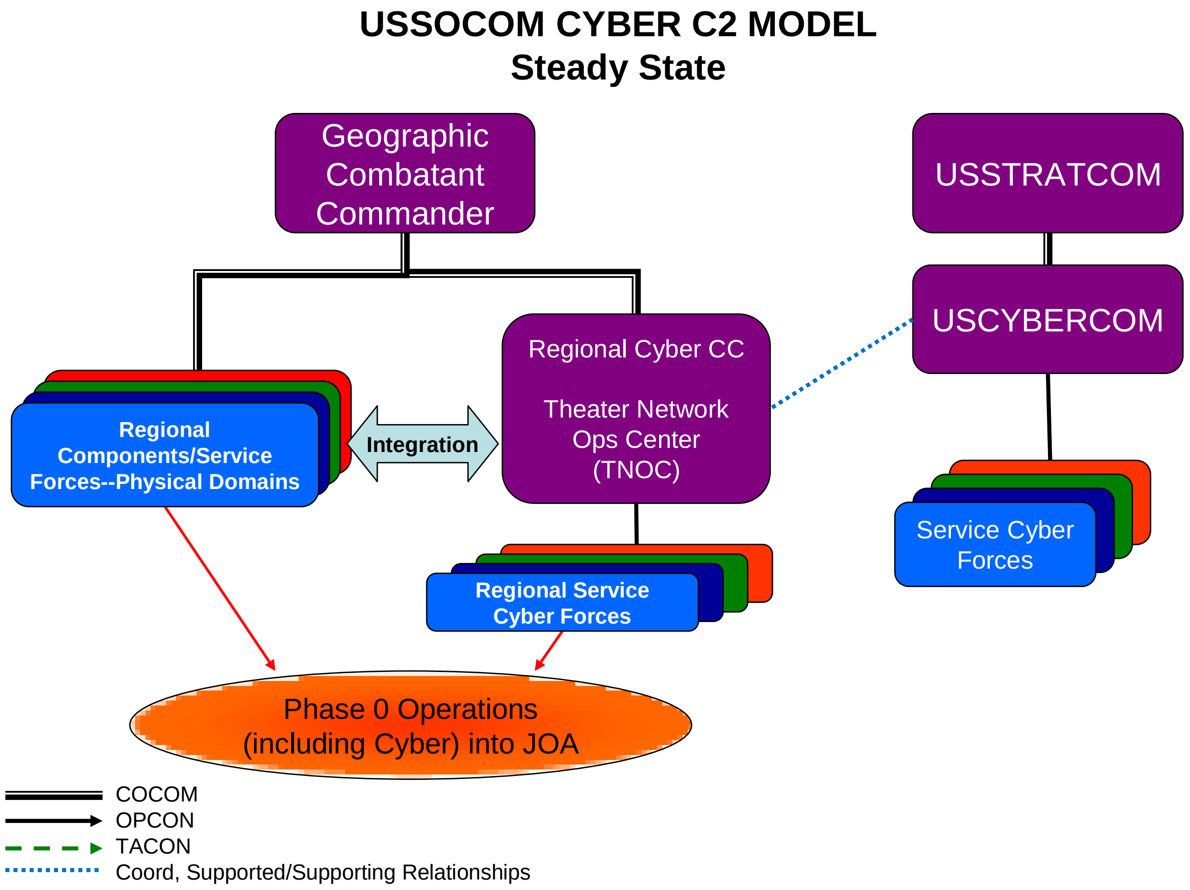
USSOCOM CYBER C2 MODEL
Steady State
Geographic Combatant Commander
USSTRATCOM
USCYBERCOM
Regional Cyber CC
Theater Network Ops Center (TNOC)
Regional Components/Service Forces--Physical Domains
Integration
Regional Service Cyber Forces
Service Cyber Forces
Phase 0 Operations (including Cyber) into JOA
COCOM
OPCON
TACON
Coord, Supported/Supporting Relationships

Figure 1.

During contingency operations where the GCC would most likely stand up a Joint Task Force (JTF), the structure would become a little more complicated (see Figure 2). USCYBERCOM, through its parent unified command, USSTRATCOM, would reinforce the GCC's cyber forces as required. The GCC would stand up a JTF Cyber Force Command subordinate to the RCC, but assign TACON to the JTF. This JTF Cyber Force Command would pick up the responsibility to plan and execute cyber exploitation and attack missions specific to the JTF's joint operations area (JOA), while the regionally focused forces would continue with operate and defend missions for the entire AOR. The JTF and its components would integrate the physical and cyber domain operations through cyber support elements associated with each component (not depicted). Using this model however, USCYBERCOM would maintain responsibility for coordinating and executing cyber operations that crossed GCC boundaries.

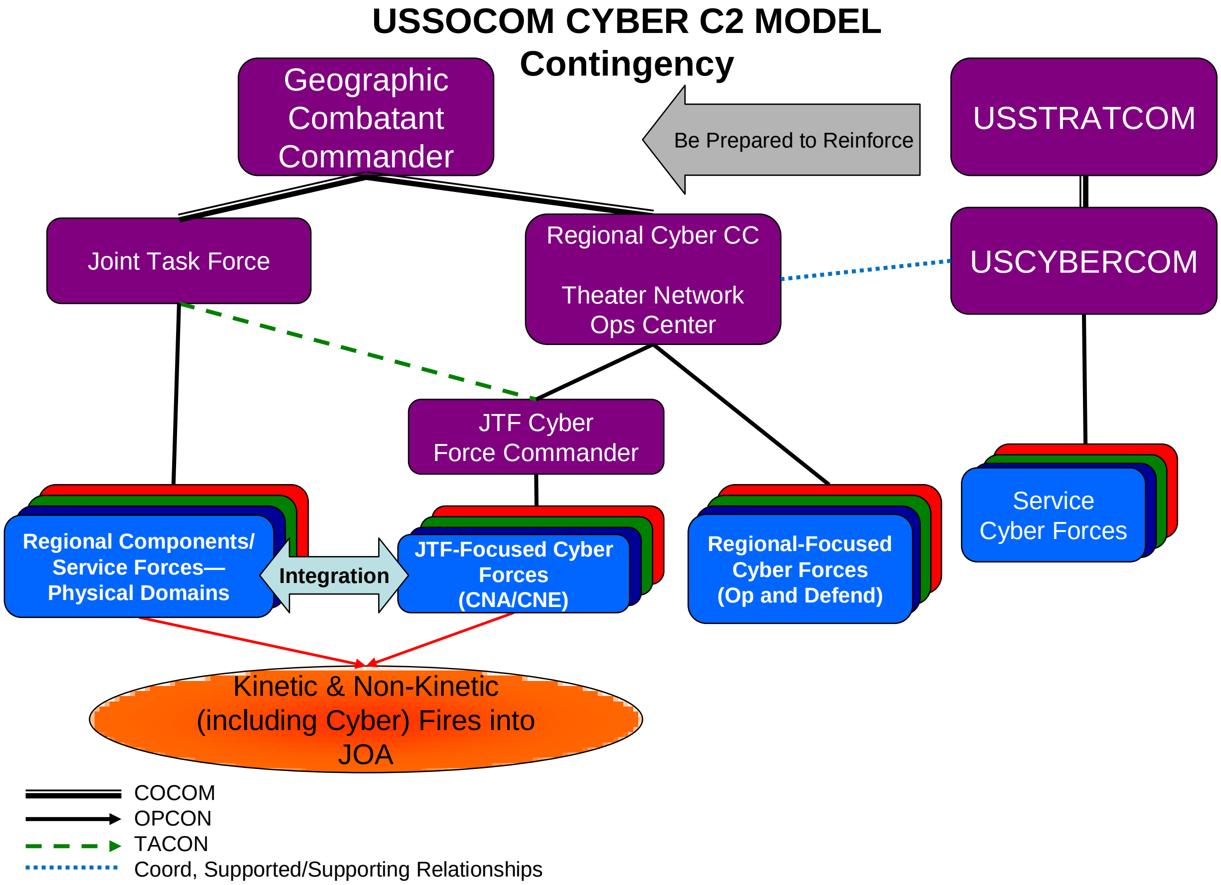
USSOCOM CYBER C2 MODEL
Contingency
Geographic Combatant Commander
Be Prepared to Reinforce
USSTRATCOM
Joint Task Force
Regional Cyber CC
Theater Network Ops Center
USCYBERCOM
JTF Cyber Force Commander
Service Cyber Forces
Regional Components/ Service Forces— Physical Domains
Integration
JTF-Focused Cyber Forces (CNA/CNE)
Regional-Focused Cyber Forces (Op and Defend)
Kinetic & Non-Kinetic (including Cyber) Fires into JOA
COCOM
OPCON
TACON
Coord, Supported/Supporting Relationships

Figure 2.

Advantages of the USSOCOM Model

One advantage to implementing the USSOCOM command and control model for cyberspace is that it is tried and tested. An example of the success of this command and control structure is the joint operations executed during Operation Iraqi Freedom. USCENTCOM's Special Operations component effectively conducted integrated combat operations with conventional forces across the entire Iraq theater of operations. They supported the air component's efforts in Iraq's western desert to negate the threat of Iraqi SCUD missiles to Israel and Jordan. They also protected dam infrastructure and supported other operations beyond the land component's limits. Furthermore, they were a critical force in northern Iraq, where they helped stabilize the line between the Iraqi army divisions and the Kurdish forces.[2] The USSOCOM command and control structure made this joint integration and operational effectiveness possible.

There are other advantages to organizing and controlling cyberspace operations through a USSOCOM model. First, this model maintains unity of command within the GCC.[3] This helps facilitate effective integration of cyber operations with operations in the physical domains. Second, it treats cyber operations just like operations in the physical domains. While this is certainly not required, treating all operational fires the same helps make coordination and integration easier.

Disadvantages of the USSOCOM Model

However, some of the unique features of cyberspace operations make applying a USSOCOM model less than optimal. First, the USSOCOM model was designed around the fact that nearly all Special Operations are conducted at the GCC level. As discussed, all Special Operations Forces activities were executed under USCENTCOM command and authority during Operation Iraqi Freedom. Therefore, a command and control structure that emphasizes the regional relationship was fitting. However, a vast majority of cyber operations (whether they are exploitation, attack, or active defense actions) will not be confined within one GCC.[4] Because of this, a much stronger relationship between the RCC and USCYBERCOM than is provided by the USSOCOM model is needed.[5]

Second, due to the potential for global collateral damage and the sensitivity of some cyber techniques, the execution authorities for many cyber operations will likely reside at USCYBERCOM at a minimum.[6] Take, for example, the Stuxnet worm. Even though experts classified it as a precision weapon,[7] it still ended up infecting tens of thousands of computers in several countries.[8] An attack of this nature can have devastating effects well beyond the scope of the intended target. Therefore, it is unlikely that the cyber execution authorities required to make the RCC effective will be delegated to the GCC.[9] Similarly, the sensitive nature of some cyber operations will require close coordination and deconfliction with the NSA, CIA, and FBI, to name a few.[10] All of these agencies have equities in operations occurring in cyberspace. This coordination would be a monumental task if required of the RCCs in each GCC.

Third, assuming that the RCC had the required authorities delegated to it, establishing an RCC at each unified command that is sufficiently robust to plan and execute those authorities would require significant resources. Each unified command would require a duplicative cyber force structure.[11] Additionally, an RCC operating in regional isolation would require essentially a complete redesign of the current network structure.[12] As the services did not build the networks with the regional boundaries as the driving factor, this would be no small task. Each GCC would require additional servers and other equipment which the services currently have centralized. This would be counterproductive to the progress the services have made toward more efficient and effective network operations.[13] Redesigning the networks could create a regional JOA for cyber and enable the GCC to manage their own passive network defense. However, USCYBERCOM would still most likely be involved with most offensive actions due to the global nature of cyber operations. USCYBERCOM would also likely conduct active defensive actions since many, if not most scenarios would require actions outside the GCC JOA. Active defensive actions are those in which a defender uses "offensive" cyber operations to reach out to adversary networks to stop an attack on DoD networks.[14] The tremendous effort and cost to develop the TSOC-like RCC provides relatively little gain to the GCC.

Fifth, while the USSOCOM model provides a regional unity of command and effort, it does not provide functional unity of effort.[15] As previously mentioned, since the majority of cyber operations will cross regional command boundaries, not having unity of effort within cyberspace will make operations inefficient and possibly ineffective.

USTRANSCOM Model

The USTRANSCOM model is a much more centralized command and control model than the USSOCOM model. Within the mobility world, USTRANSCOM retains OPCON of global mobility assets, and only designates OPCON of assets to a GCC when they are physically retained within the GCC boundaries and used strictly for intra-theater missions. This allows USTRANSCOM much greater flexibility to manage global mobility priorities.[16] In applying this model to cyberspace, we arrive at the steady state model depicted in Figure 3.

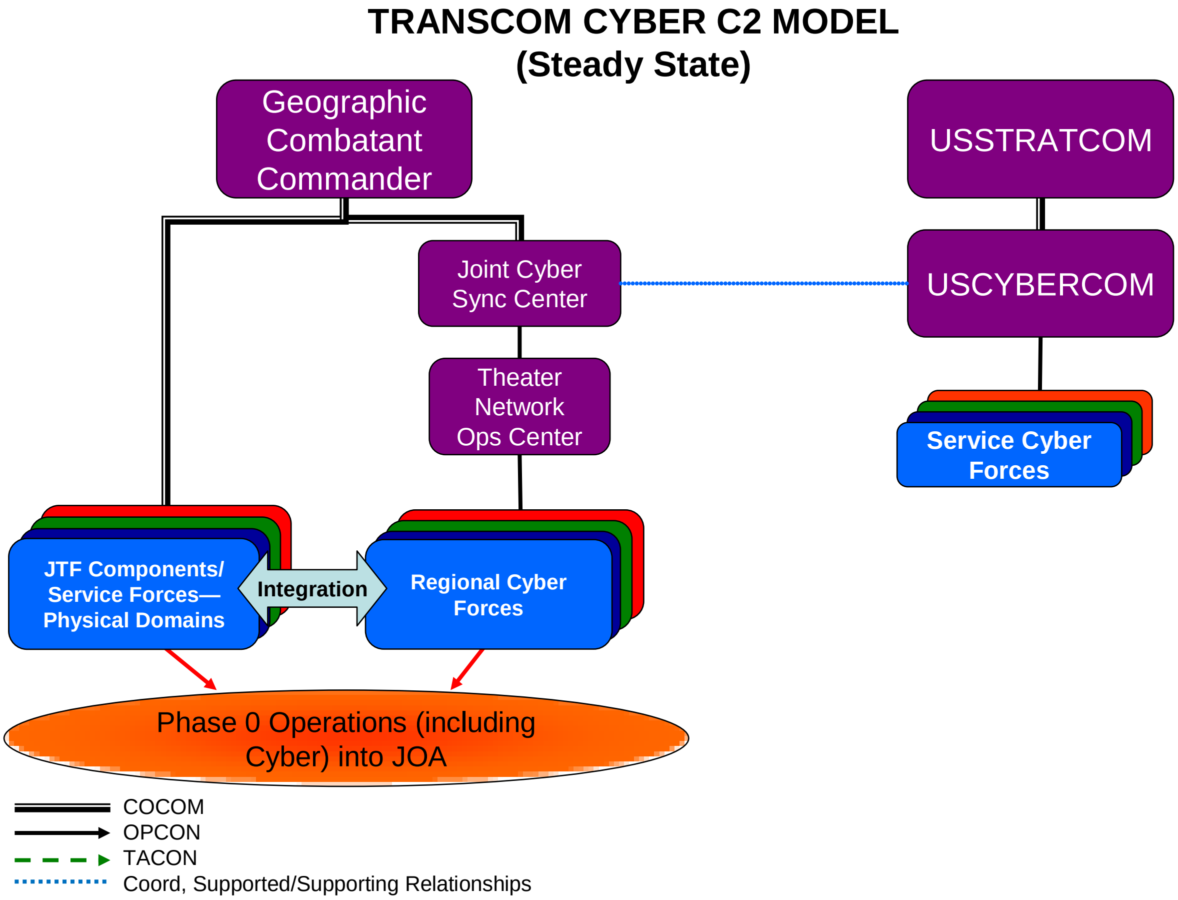
TRANSCOM CYBER C2 MODEL
(Steady State)
Geographic Combatant Commander
USSTRATCOM
Joint Cyber Sync Center
USCYBERCOM
Theater Network Ops Center
Service Cyber Forces
JTF Components/ Service Forces— Physical Domains
Integration
Regional Cyber Forces
Phase 0 Operations (including Cyber) into JOA
COCOM
OPCON
TACON
Coord, Supported/Supporting Relationships

Figure 3.

The USTRANSCOM model incorporates a Joint Cyber Synchronization Center (JCSC) that is COCOM to the GCC and is responsible for coordinating cyber operations with USCYBERCOM.[17] The JCSC, in turn, directs cyber operations through the Theater Network Operations Center, whose primary role during regional Phase 0 shaping operations is basic network operation and defense. In a supporting role, USCYBERCOM would conduct cyber operations in support of the GCC's Phase 0 operations. Furthermore, USCYBERCOM would be responsible for all network exploitation and attack operations both globally and regionally. All regional support would be coordinated through the JCSC.[18]

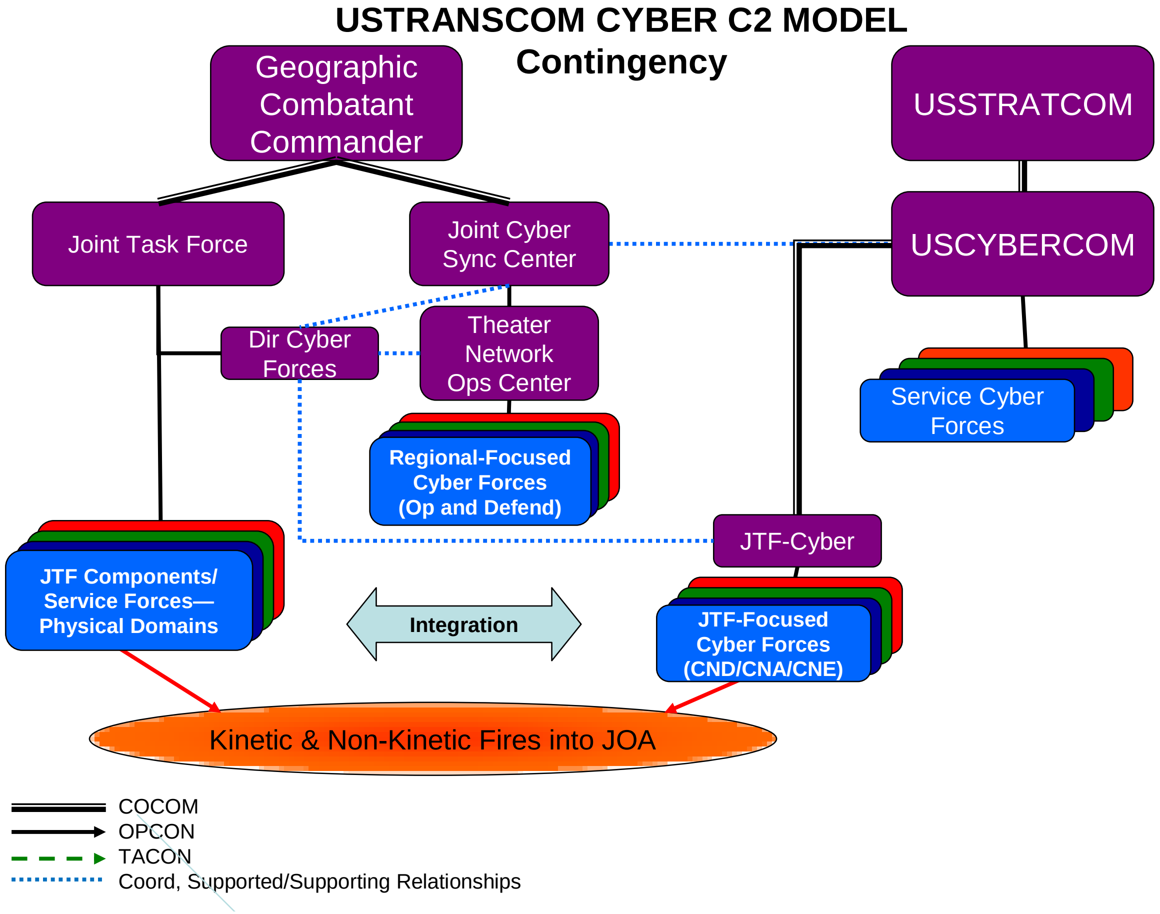
USTRANSCOM CYBER C2 MODEL
Contingency
Geographic Combatant Commander
USSTRATCOM
Joint Task Force
Joint Cyber Sync Center
USCYBERCOM
Dir Cyber Forces
Theater Network Ops Center
Service Cyber Forces
Regional-Focused Cyber Forces (Op and Defend)
JTF-Cyber
JTF Components/ Service Forces— Physical Domains
Integration
JTF-Focused Cyber Forces (CND/CNA/CNE)
Kinetic & Non-Kinetic Fires into JOA
COCOM
OPCON
TACON
Coord, Supported/Supporting Relationships

Figure 4.

Once the GCC moves into contingency operations and stands up a JTF, the command structure changes dramatically (see Figure 4). Major changes include a GCC-designated Director of Cyber Forces and the creation of a JTF-Cyber.[19] This Director of Cyber Forces (JTF-Cyber) works for the JTF and coordinates all cyber operations for that JTF. The JTF-Cyber is COCOM to USCYBERCOM and brings cyber exploitation and attack capabilities to the GCC. While OPCON of the JTF-Cyber is retained by USCYBERCOM, they act in a supporting role to the GCC for regional cyber operations and provide the robust cyber capability that the GCC will need during contingency operations.

Advantages of the USTRANSCOM Model

The advantages of the USTRANSCOM model are inherent in the more centralized nature of its command and control structure. In both the steady state and contingency models, USCYBERCOM would retain OPCON of the majority of cyber forces, allowing it the flexibility to apply limited assets against the highest priority mission – whether global or regional – in support of a GCC's operations.[20] The GCCs would have TACON of the service forces operating and defending the networks in their AOR, thereby maintaining some indigenous capability, but most advanced capabilities would reside with USCYBERCOM. Another advantage of the centralized model is that personnel and capabilities are concentrated where the authorities are expected to reside.[21] This provides the most efficient and effective use of limited resources. Lastly, this model provides unity of command at the global level, where a vast majority of cyber operations will occur.

Disadvantages of the USTRANSCOM Model

There are two significant disadvantages to applying a USTRANSCOM model to cyberspace. First, there is no unity of command at the GCC level.[22] Having virtually all cyber capability centrally controlled and executed creates challenges for integrating cyber capability into the GCC's plans and operations. Second, the lack of unity of command is further exacerbated by significant impediments to regional unity of effort during contingency operations. The USTRANSCOM model relies heavily on coordination and supporting/supported relationships. This works sufficiently in USTRANSCOM's mobility world. While mobility operations are a critical enabler for the GCC's operations, inter-theater mobility operations generally don't have to be woven into the GCC's kinetic operations. This is not the case with cyber operations. Cyberspace is the backbone of DoD command and control at all levels. Cyber operations also have the ability to create effects both in the cyberspace domain and the physical domains. A structure that depends on extensive coordination would make integrating these capabilities extremely difficult.[23]

Notes

[1] Brig Gen Brett T. Williams (J-6, USPACOM, Camp Smith, HI), interviewed by author, 21 December 2010.

[2] Authors experience as Chief of Strategy for the USCENTCOM air component from July 2001 to September 2003.

[3] Joint Publication (JP) 3-0, *Joint Operations*, 17 September 2006, Change 2, 22 March 2010, A-2.

[4] Brig Gen Charles K. Shugg (Vice Commander, 24th Air Force, Lackland AFB, TX), interviewed by author, 16 December 2010.

[5] LtGen Robert E. Schmidle (Deputy Commander, USCYBERCOM, Fort Meade, MD), interviewed by author, 17 December 2010.

[6] Ibid.

[7] Ed Barnes, "Mystery Surrounds Cyber Missile That Crippled Iran's Nuclear Weapons Ambitions," *Fox News*, 26 November 2010, http://www.foxnews.com/scitech/2010/11/26/ secret-agent-crippled-irans-nuclear-ambitions).

[8] James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival: Global Politics and Strategy* 53, no. 1 (February-March 2011): 23.

[9] Col Gary D. Brown (Staff Judge Advocate, USCYBERCOM, Fort Meade, MD), interviewed by author, 24 January 2011.

[10] Ibid.

[11] Michael Clark (Deputy J-5, USCYBERCOM, Fort Meade, MD), interviewed by author, 21 December 2011.

[12] Brig Gen Brett T. Williams (J-6, USPACOM, Camp Smith, HI), interviewed by author, 21 December 2010.

[13] Col Victor J. Diaz Jr. (commander, 624th Operations Center, Lackland AFB, TX), interviewed by author, 10 March 2011.

[14] Michael Clark (Deputy J-5, USCYBERCOM, Fort Meade, MD), interviewed by author, 21 December 2011.

[15] Joint Publication (JP) 3-0, *Joint Operations*, 17 September 2006, Change 2, 22 March 2010, A-2.

[16] Maj John Caranata, "Application of USTRANSCOM C2 Model for USCYBERCOM" (position paper presented to the Center for Cyber Research, Air Force Institute of Technology, December 2010), 4.

[17] Ibid.

[18] Ibid., 5.

[19] Ibid., 5-6.

[20] Brig Gen Gregory Brundidge, (J-6, USEUCOM, Stuttgart, GE), interviewed by author, 14 January 2011.

[21] Ibid.

[22] Joint Publication (JP) 3-0, *Joint Operations*, 17 September 2006, Change 2, 22 March 2010, A-2.

[23] Brig Gen Gregory Brundidge, (J-6, USEUCOM, Stuttgart, GE), interviewed by author, 14 January 2011.

CHAPTER FOUR
Recommendations

USCYBERCOM cannot effectively execute its mission by dispersing its limited capability to all the GCCs. Likewise, it cannot effectively support the GCC's regional missions by attempting to centrally plan and execute all cyber operations from Fort Meade.[1] The need for a structure that facilitates both missions leads to a hybrid command and control structure model that has features of both the USSOCOM and USTRANSCOM models.

In order to integrate cyber effects into regional plans, USCYBERCOM will need to have a regional presence. This presence should be in the form of a regional cyber command (RCC) that answers to USCYBERCOM but is responsive to the GCC (see Figure 5). Having the RCC COCOM to USCYBERCOM ensures unity of command for

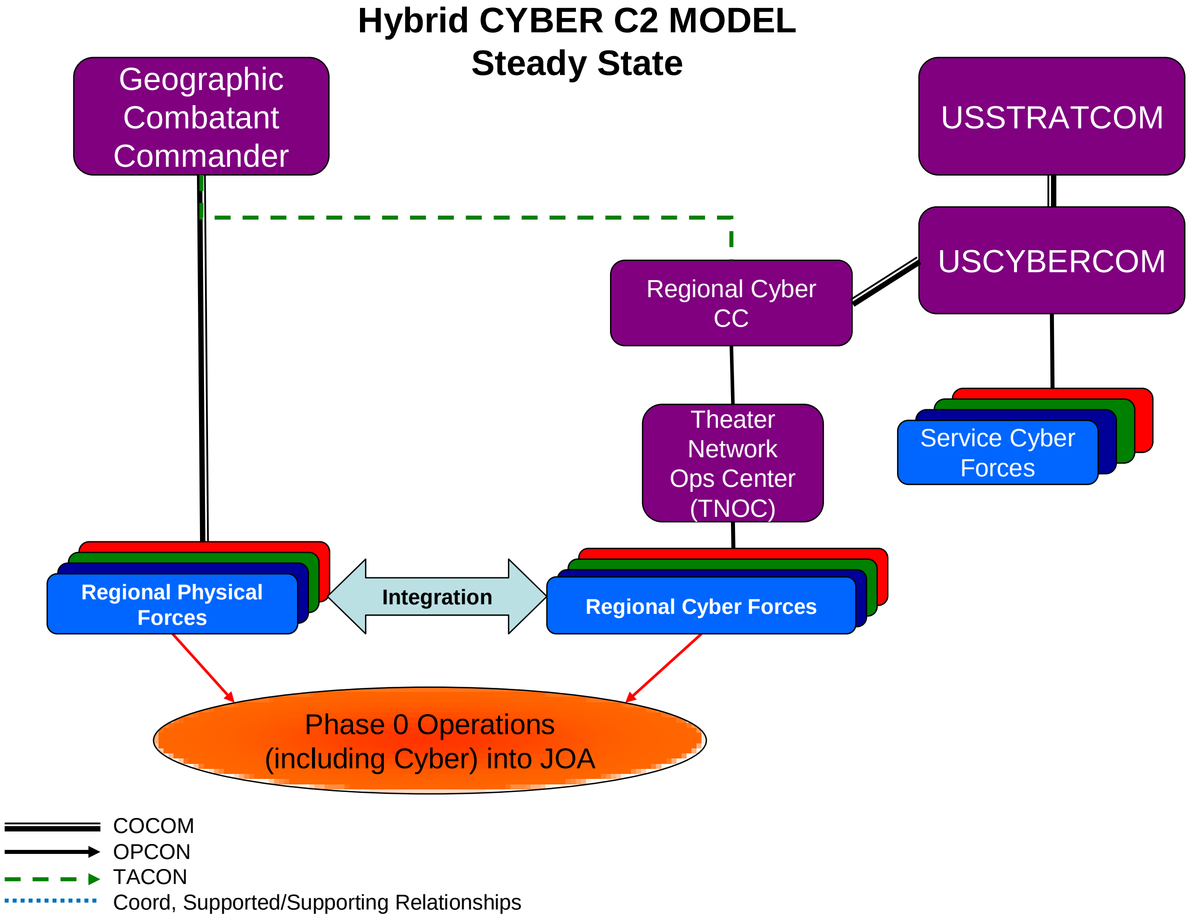

Figure 5.

global cyber operations, as well as operations conducted outside of the GCC's AOR by USCYBERCOM, for effects in support of that GCC. With a TACON relationship to the GCC for regional issues, the RCC will be focused primarily on integrating cyber operations in support of its GCC and provide the GCC with unity of effort. USCYBERCOM, through the COCOM relationship with the RCC, would have the authority to pull back TACON of the RCC as required to support inter-regional operations. This would avoid the potential ambiguities associated with the massive coordination required in the USTRANSCOM model.

During a contingency operation within a GCC's region, USCYBERCOM would augment the regional cyber forces, as required, and stand up a JTF-Cyber component (see Figure 6). Since the augmentation forces would still have OPCON to USCYBERCOM, they could manage the forward presence to meet GCC needs while ensuring mission balance with global priorities. As noted previously, personnel located around the globe can for the most part conduct cyber operations in support of a GCC

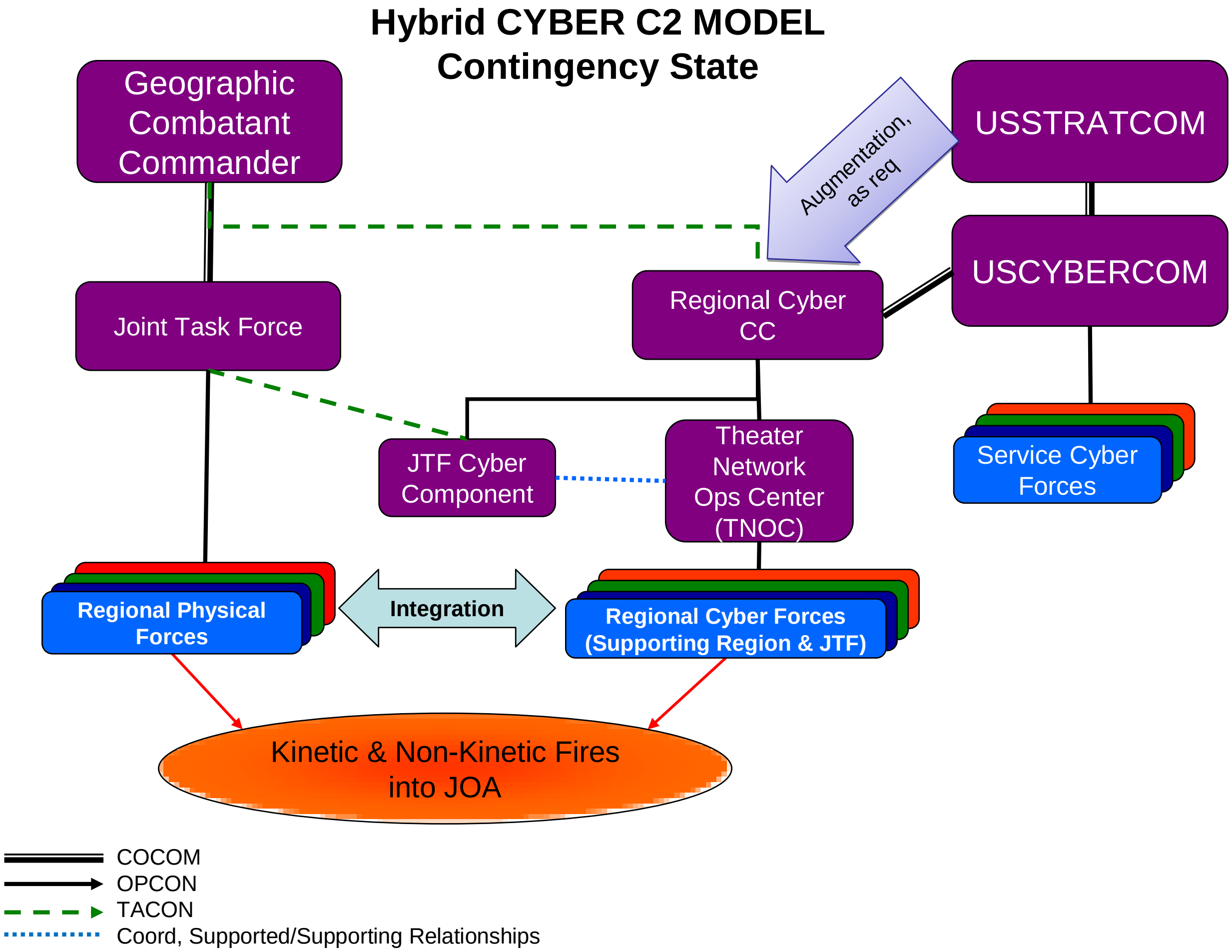

Figure 6.

without being physically located in the GCC's AOR. Tie that to the speed of cyber effects, and now USCYBERCOM has the required flexibility to shift low-density, high-demand capability rapidly from one mission to another. The JTF-Cyber component would ensure integration of cyber effects at the JTF level, while coordinating and deconflicting operations through its primary tether back to USCYBERCOM. Again, since the authority to execute most cyber operations in the exploit and attack mission areas would be retained and/or coordinated at USCYBERCOM, the functional cyber unity of command of the hybrid model becomes that much more important.[2]

While the hybrid model has features of both the USSOCOM and USTRANSCOM models, it is not a perfect model from either the USCYBERCOM or GCC perspective. First, maintaining a regional cyber component for each GCC will require more personnel than if all cyber efforts were centrally consolidated. At the same time, the COCOM relationship with USCYBERCOM should enable the use of reach back support, which should enable some personnel efficiencies. Second, USCYBERCOM's management of cyber priorities will likely reduce the GCC's confidence in their ability to obtain the cyber effects when they want them. This will require a robust relationship between the RCCs and the GCCs they serve. Third, the RCC will have to be mindful of the weaker command link to the GCC and ensure that the GCC is aware of cyber attacks and vulnerabilities that may affect GCC operations. This way, the GCC commander can make educated decisions based on the associated cyber risks.

The hybrid cyber command and control structure capitalizes on the advantages of both the USSOCOM model and the USTRANSCOM model. It has the centralized command and control nature of the USTRANSCOM model which facilitates USCYBERCOM's global missions and the extensive inter-agency coordination required for virtually all cyber actions. However, it employs a much more precise, USSOCOM-like command structure at the GCC level, avoiding the significant coordination requirements of the USTRANSCOM model. This command structure enables the effective integration of cyber operations into the GCC's plans and operations. While not perfect for either USCYBERCOM or the GCCs, the hybrid model ensures unity of command for cyberspace operations while still providing the needed regional unity of effort.

Notes

[1] USPACOM/USCYBERCOM Tabletop Exercise in preparation for Exercise TERMINAL FURY (Camp Smith, HI), author's observations, 24 January 2011.

[2] Col Gary D. Brown (Staff Judge Advocate, USCYBERCOM, Fort Meade, MD), interviewed by author, 24 January 2011.

CHAPTER FIVE
Conclusions

> *Although attacks in the cybersphere do not involve use of physical weapons, their destructive impacts, physical and otherwise, may be no less lethal to societies.*
>
> —Jeffrey R. Cooper

Many of the same arguments for command and control of airpower at the GCC level apply to cyberspace, but at a global level. Since WWII, air power advocates have successfully argued that due to its unique nature air power should be treated differently from the other domains.

> Because of air and space power's unique potential to directly affect the strategic and operational levels of war, it must be controlled by a single airman who maintains the broad, strategic perspective necessary to balance and prioritize the use of a powerful, highly desired yet limited force. A single air commander, focused on the broader aspects of an operation, can best mediate the competing demands for tactical support against the strategic and operational requirements of the conflict…Centralized control of air and space power should be accomplished by an airman at the air component commander level who maintains a broad theater perspective in prioritizing the use of limited air and space assets to attain established objectives in any contingency across the range of operations.[1]

As an illustration, during the opening phases of Operation IRAQI FREEDOM, the Combined Forces Air Component Commander (CFACC) had the responsibility for coordinating and deconflicting air operations throughout the entire USCENTCOM theater. The CFACC additionally had, at a minimum, TACON of a majority of the air assets in theater. The reason air power experts tout this as the best method for command and control of air power is its flexibility and speed to apply effects across the entire geographic area. Any dividing up of air assets and apportioning them to subordinate commands within the region negates the efficiency gained by being able to direct air assets where most needed based on joint priorities and the changing situation. Similar arguments apply to the cyberspace domain, but on a global scale.

Just as air power has unique characteristics that warrant a centralized control model, the cyberspace domain also has distinctive characteristics. Like the air domain, forces operating in the cyberspace domain have tremendous flexibility to apply effects over a vast area. Cyberspace forces also have the advantage of speed, but at several orders of magnitude greater; operations can be conducted from nearly anywhere in the world, and those effects travel at the speed of light. This global flexibility and near-instantaneous reach means that, just as air power should be controlled by an airman in a regional Air Operations Center to prevent the inefficient and uncoordinated employment of air power, cyberspace should be controlled by a cyber operator (for lack of a better term) at a cyber command with a global perspective. The operator could then manage global cyber effects while supporting each of the regional combatant commands. Any dividing up of cyber forces into regional areas of operation significantly multiplies the force structure required; attempts to create regional cyberspace seams where none exist; and ignores the global nature of cyberspace operations. This does not imply that the GCCs should not have any access to and influence over cyber capabilities for their AOR. However, the primary command relationship for regional cyber forces should be back to USCYBERCOM.

The basic tenet of air and space power can be re-written for cyberspace as follows: Because of cyberspace power's unique potential to directly affect the strategic and operational levels of war, it must be controlled by a single cyber operator who maintains the broad, strategic perspective necessary to balance and prioritize the use of a powerful, highly desired yet limited force. A single cyber commander, focused on the broader aspects of global cyber operations, can best mediate the competing demands for tactical support against the strategic and operational requirements of the conflict. Centralized control of cyberspace should be accomplished by a cyber operator at the functional COCOM level who maintains a broad global perspective in prioritizing the use of limited cyberspace assets to attain established objectives in any contingency across the range of operations.

The second half of this tenet of air and space power, decentralized execution, is less applicable in cyberspace. Due to the potential for far-reaching collateral effects and the related high-level authorities required to take action in cyberspace, the full tenet of cyberspace should be centralized control, centralized execution. With that said, there is no way USCYBERCOM can effectively centrally plan and execute all cyber operations and ensure integration of cyber capabilities to GCC plans and operations. The hybrid cyber model enables USCYBERCOM to manage global priorities and ensures the effective integration of cyberspace capabilities at the regional level in support of the GCCs.

Notes

[1] Air Force Doctrine Document (AFDD) 1, Air Force Basic Doctrine, 17 November 2003, 28.

GLOSSARY

AFCYBER	Air Forces Cyber
ARFORCYBER	Army Forces Cyber
CNA	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Exploitation
COCOM	Combatant Command
DDOS	Distributed Denial of Service
DOD	Department of Defense
DOS	Denial of Service
GIG	Global Information Grid
GCC	Geographic Combatant Command
JOA	Joint Operations Area
MARFORCCYBER	Marine Forces Cyber
NAVFORCYBER	Navy Forces Cyber
OPCON	Operational Control
RCC	Regional Cyber Command
TACON	Tactical Control
USCENTCOM	United States Central Command
USCYBERCOM	United States Cyber Command

USPACOM	United States Pacific Command
USSTRATCOM	United States Strategic Command
USTRANSCOM	United States Transportation Command

botnet. A botnet is a collection of software agents, or robots, that run autonomously and automatically. The term most recently refers to malicious software, but it can also refer to a network of computers using distributed computing software.

doctrine. (DOD) Fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application.

combatant command. Nontransferable command authority established by title 10, United States Code, section 164, exercised only by commanders of unified or specified combatant commands unless otherwise directed by the President or the Secretary of Defense. Combatant command (command authority) cannot be delegated and is the authority of a combatant commander to perform those functions of command over assigned forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command. Combatant command (command authority) should be exercised through the commanders of subordinate organizations. Normally this authority is exercised through subordinate joint force commanders and Service and/or functional component commanders. Combatant command (command authority) provides full authority to organize and employ commands and forces as the combatant commander considers necessary to accomplish assigned missions. Operational control is inherent in combatant command (command authority).

cyberspace. A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 1-02. SOURCE: CJCS CM-0363-08)

cyberspace operations. The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid.

global information grid. The globally interconnected, end-to-end set of information capabilities associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. It includes all owned and leased communications and computing systems and services, software (including applications), data, security services and other associated services necessary to achieve information superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. It supports all Department of Defense, National Security Systems, and related Intelligence Community missions and functions (strategic, operational, tactical and business), in war and in peace. It provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms and deployed sites). It also provides interfaces to coalition, allied, and non-DOD users and systems.

offensive cyber operations. Military operations and activities in cyberspace for cyber attack against and (or) cyber exploitation of adversary information systems and networks. Encompasses the capabilities formerly known as computer network exploitation and computer network attack.

operational control. Operational control 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.

phase 0 operations (also called Shaping operations) Joint and multinational operations inclusive of normal and routine military activities and various interagency activities performed to dissuade or deter potential adversaries and to assure or solidify relationships with friends and allies. They are executed continuously with the intent to enhance international legitimacy and gain multinational cooperation in support of defined military and national strategic objectives. They are designed to assure success by shaping perceptions and influencing the behavior of both adversaries and allies, developing allied and friendly military capabilities for self-defense and coalition operations, improving information exchange and intelligence sharing, and providing US forces with peacetime and contingency access. Shape phase activities must adapt to a particular theater environment and may be executed in one theater in order to create effects and/or achieve objectives in another.

supporting. In the context of a support command relationship, the commander who aids, protects, complements, or sustains another commander's force, and who is responsible for providing the assistance required by the supported commander.

tactical control. Tactical control provides sufficient authority for controlling and directing the application of force or tactical use of combat support assets within the assigned mission or task.

unity of command. Unity of command means that all forces operate under a single commander with the requisite authority to direct all forces employed in pursuit of a common purpose. During multinational operations and interagency coordination, unity of command may not be possible, but the requirement for unity of effort becomes paramount.

unity of effort. Coordination and cooperation toward common objectives, even if the participants are not necessarily part of the same command or organization.

BIBLIOGRAPHY

Air Force Doctrine Document (AFDD) 1, Air Force Basic Doctrine, 17 November 2003.

Alexander, Gen Keith B., commander, USCYBERCOM. Address. Center for Strategic and International Studies, Washington, DC, 3 June 2010.

Barnes, Ed. "Mystery Surrounds Cyber Missile That Crippled Iran's Nuclear Weapons Ambitions." Fox News, 26 November 2010. http://www.foxnews.com/scitech/2010/11/26/ secret-agent-crippled-irans-nuclear-ambitions (accessed 29 November 2010).

Caranata, Maj John. "Application of USTRANSCOM C2 model for USCYBERCOM." Paper presented to the Center for Cyber Research, Air Force Research Institute. December 2004.

Clarke, Richard A. Former Special Advisor on Cybersecurity to President George W. Bush. Address. American Association for the Advancement of Science, Washington, DC, 22 November 2010.

Clarke, Richard A. and Knake, Robert K. *Cyber War: The Next Threat to National Security and What to Do About It.* New York: HarperCollins, 2010.

Department of Defense. "DefenseLINK: Unified Command Plan." http://www.defense.gov/specials/unifiedcommand/ (accessed 1 Mar 2011).

Department of Defense. *Quadrennial Defense Review Report*, February 2010.

Department of Defense. *U.S. Cyber Command Fact Sheet*. Washington, DC: U.S. Department of Defense Office of Public Affairs, May 2010.

Eshel, David. "Cyber-Attack Deploys In Israeli Forces." *Aviation Week*, 15 September 2010. http://www.aviationweek.com/aw/generic/story.jsp?id=news/dti/2010/09/01/DT_09_01_2010_p42-248207.xml&channel=defense (Accessed 29 November 2010).

Farwell, James P. and Rohozinski, Rafal. "Stuxnet and the Future Cyber War." *Survival: Global Politics and Strategy* 53, no. 1 (February-March 2011): 23-40.

Fulghum, David A. "Israel Assesses Changing Threats." *Aviation Week*, 13 August 2010. http://www.aviationweek.com/aw/generic/story.jsp?id=news/awst/2010/08/09/AW_08_09_2010_p42-243720.xml&channel=defense (accessed 29 November 2010).

Fulghum, David A. "No Fingerprints: Culprits in the Cyberattack on Iran Are Still Unknown." *Aviation Week* 172, no. 36 (4 October 2010), 29-30.

Hughes, Rex. "A Treaty for Cyberspace." *International Affairs*, Vol 86, No. 2.

Joint Publication (JP) 3-0, *Joint Operations*, 17 September 2006, Change 2, 22 March 2010.

Rife, Maj Shawn P. "Kasserine Pass and the Proper Application of Airpower." *Joint Forces Quarterly* 20 (Autumn/Winter 1998-1999): 71-77.

McCullough, VADM Bernard J. Commander, US Fleet Cyber Command. Address. Government Executive Cybersecurity Insider Series, Washington, DC, 14 Dec 2010.

Morrow, John H., Jr. "The First World War, 1914-1919." In *A History of Air Warfare.* Edited by John A. Olsen. Washington, DC: Potomac Books, 2010.

About the Author

Colonel David Hathaway was commissioned as a distinguished graduate through the Air force Reserve Officer Training Corps. He has commanded F-16 fighter units at the flight, squadron and most recently at the vice wing command levels, which has included multiple deployments to the USCENTCOM area of responsibility. He is a graduate and former instructor of the USAF Weapons School and a graduate from the School of Advanced Air and Space-power Studies. He was the architect of the air and space power strategy for Operations Enduring Freedom and Iraqi Freedom as the Chief of Strategy for USCENTAF. He has served on the Joint Staff in Global Force Management and as the Joint Operations Division Chief for USSOUTHCOM.

Colonel Hathaway's degrees include: a bachelor of science in engineering mechanics from the University of Wisconsin-Madison; master of aviation science from Embry Riddle Aeronautical University; master of military operational art and science and master of airpower art and science from Air University. His graduate research focused on the future role of unmanned combat aerial vehicles and assessment of operational effects during major combat operations.