Cyberspace as a Theater of Conflict:

Federal Law, National Strategy and The Departments of Defense and Homeland Security

GRADUATE RESEARCH PROJECT

Sam Arwood, Major, USAF

AFIT/IC4/ENG/07-01

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

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

AFIT/IC4/ENG/07-01

Cyberspace as a Theater of Conflict:

Federal Law, National Strategy and The Departments of Defense and Homeland Security

GRADUATE RESEARCH PROJECT

Presented to the Faculty

Department of Electrical & Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of C4I Systems

Sam Arwood, BS

Major, USAF

June 2007

AFIT/IC4/ENG/07-01

Cyberspace as a Theater of Conflict:

Federal Law, National Strategy and The Departments of Defense and Homeland Security

Sam Arwood, BS

Major, USAF

Approved:

_____//signed//_____ _____
Robert F. Mills, PhD, USAF (Chairman) date

_____//signed//_____ _____
Richard A. Raines, PhD, USAF (Member) date

AFIT/IC4/ENG/07-01

Abstract

Research questions: My research is divided into three distinct parts, each linked and dependent upon one another. First is a review and an evaluation of the legal relationships between the Combatant Commanders, the Services, and DoD Agencies with respect to cyberspace. What roles are tasked to each and what limitations are in place based upon those assigned roles. And are any of these current relationships at odds with federal law? Second, I linked National Strategy to a Service's targeting strategy via the Effects Based Planning process. This demonstrates the ability to link target selection to the elements of national power as well as identify possible desired effects based upon adversary target selection. Last, is an evaluation of military cyberspace activities and responsibilities based upon the conclusions and observations of the first two sections. Included in this evaluation is a brief look at cyberspace activities not yet addressed by the DoD but soon to be a responsibility of the Department.

Table of Contents

List of Figures

I. Introduction

> "The current military-technical revolution, as in the case of some earlier periods of major change in military affairs, is part of a broader revolution with political, economic and social dimensions. It is being shaped by profound changes in technology, perhaps most notably in the area of information technology…"
>
> *-- William J. Perry, October 1994*

Figure 1. William J. Perry[1]

Cyberspace: The electronic medium of computer networks, in which online communication takes place.[2]

Cyberspace as an entity is being shaped, twisted, and forced into different molds in an attempt to define its utility and lethality within constructs shaped by our current warfare domains. The Air Force today speaks of this new environment in terms of "learning to fly and fight in cyberspace" – it's reminiscent of the Army Air Corps speaking of aircraft as only support elements to ground forces. Kenneth Allard mentions a similar problem with respect to the beginning of Air Power when he states – "…these developing perspectives of Land, Sea and Air combat tended to represent syntheses of old doctrines geared to new circumstances".[3] Until General Billy Mitchell, the military leaders of the day could not see past their biases to recognize Air Power as anything more

[1] Taylor, Phillip M., Professor, Institute of Communications Studies, University of Leeds, United Kingdom. "Concepts of Information Warfare." Presentation Slide Lecture to the Norwegian Staff Defense College students and faculty. Norwegian Staff Defense College, Oslo Norway. November 2006 http://ics.leeds.ac.uk/papers/pmt/exhibits/2669/Oslo06.ppt (No page number)
[2] The American Heritage® Dictionary of the English Language, Fourth Edition. Copyright 2002, 2000 by Houghton Mifflin Company. (No page number)
[3] Allard, Kenneth. *Command, Control, and the Common Defense* (Revised Edition). Washington DC: National Defense University. 1996. (Page 93)

than a minor support activity. We have to escape retrogressive thinking. To fully exercise cyberspace's capabilities we need individuals who understand this new environment as well as General Billy Mitchell understood the true potential of Air Power. But today, we have something that General Mitchell didn't have – and that is a Department of Defense that recognizes cyberspace as a domain that we must master; because, it's now an issue of national security and an element of national power. Just as General Mitchell realized that air power was not just a ground support activity, we need individuals today that understand that cyberspace power is not just a ground, air or naval support activity.

As the cyberspace technical discussions take place across DoD, there is an issue that keeps coming up, namely "What is cyberspace?" Throughout this paper, the cyberspace concept is limited to the DoD Network, which includes all Internet Protocol (IP) Address space. The reason for this limitation is that it is the introduction of computer networks to the civilian and military communities that has lead to the current cyberspace power discussions. This is similar, but not parallel in nature, to the introduction of aircraft that fueled air power discussions – that eventually lead to an independent Service. Aircraft had been around for a while, but it was not until air power proved its capabilities that the Air Force was born. Cyberspace is now crossing that same threshold, not into a separate Service, but as a warfare domain in its own right.

As our understanding and definition of cyberspace evolves, our military capabilities, our justice system and our legal responsiveness (Congress) will evolve. Given the cyberspace domain as a new theater of conflict, the purpose of this paper is to examine the relationships, roles and responsibilities, authorities and doctrine, with respect to Federal Law, of the Services, the Combatant Commanders (COCOMs) and the

Departments of Defense (DoD) and Homeland Security (DHS). There are implications to the "rest of Information Operations" throughout this paper, and the majority of the conclusions drawn, apply equally.

II. COCOMs vs. Services: Roles And Responsibilities

Federal Law

Federal Law shapes the discussion of the roles of the Services and the COCOMs. Congress has continually reinforced the concept of jointness in each subsequent Act that affects DoD organization and structure. The key to this, and all legislation, is the Congressional intent based upon their response to what initiated the need for a change in the first place. Congress and the Office of the President have drawn a line between combat and non-combat operations, as well as Service activities and COCOM activities. To start this discussion – we have to go back to the beginning of today's concept of jointness.

In general warfare within the United States, the vision that did more to shape the current DoD structure than any other, is that of President Eisenhower. His experiences during World War II gave him great insight into the issues of bringing together the capabilities of ground, air and naval forces. President Ronald Reagan noted this in his message to the 99th Congress when they were debating the context of the Goldwater-Nichols Department of Defense Reorganization Act of 1986. President Reagan stated "President Eisenhower's experience of high military command has few parallels among Presidents since George Washington."[4] President Reagan was making this comment to remind Congress that the DoD establishment, at that time, was a well engineered effort

[4] Reagan, Ronald. President of the United States, Washington DC. "Defense Reorganization – Message From The President Of The United States; Transmitting His Views On The Future Structure And Organization Of Our Defense Establishment And The Legislative Steps That Should Be Taken To Improve Defense Reforms". The 99th Congress, 2nd Session, House Document: 99-209. 28 April 1986. (Page 2)

undertaken by leaders with unprecedented experience – and not to be tinkered with, without due cause.

Legislation shaping the current DoD has been following the path set by President Eisenhower - continually refining the concept of "Jointness" and the application of integrated force. These Legislative Acts have attempted to maintain a balancing act of delivering on a joint integrated vision while keeping intact the legacy of independent military departments. This has been further shaped by the Constitutional powers of the Executive Branch – President Reagan was not shy about reminding Congress that he was maintaining a watchful eye with respect to his "constitutional responsibilities and prerogatives of the presidency".[5] Thus implying that, even as Congress' vision of jointness, organization and structure evolves – the Office of the President has a duty under the Constitution to maintain DoD effectiveness. President Reagan saw that duty as maintaining President Eisenhower's vision as stated above.

As Congress and the President walked this "tightrope" over the years, legislation has been adopted that continues to refine and define the DoD. Some key legislative acts, with respect to the COCOMs and the Services, are:

1. The National Security Act of 1947, Public Law 80-253
2. United States Code, Title 10; Subtitle A, Part I, Chapter 6
3. Department of Defense Reorganization Act of 1958, Public Law 85-599
4. Goldwater-Nichols Department Of Defense Reorganization Act of 1986, Public Law 99-433

[5] Reagan, Ronald. President of the United States, Washington DC. "Defense Reorganization – Message From The President Of The United States; Transmitting His Views On The Future Structure And Organization Of Our Defense Establishment And The Legislative Steps That Should Be Taken To Improve Defense Reforms". (Page 2)

The list above is not all inclusive; the list was narrowed to address the key points in Federal Law that will impact the cyberspace discussion with respect to the Services and the COCOMs. Also, the original Acts have been modified by subsequent legislation – some of those modifications are included. I only comment on portions of the Acts that are applicable to the relationships under review.

The National Security Act of 1947, Public Law 80-253

> *"The teams and staffs through which the modern commander absorbs information and exercises his authority must be a beautifully interlocked, smooth-working mechanism. Ideally, the whole should be practically a single mind."*
>
> **General Dwight D. Eisenhower**

Figure 2. General Dwight D. Eisenhower (JP 0-2) [6]

Following President Eisenhower's vision, the National Security Act was passed in 1947. This legislation reshaped the military and intelligence landscape and established several independent departments and organizations. Much of the Act is still valid, but Title II, Sections 201 – 214 (the key portion of this Act with respect to DoD) have mostly been repealed and replaced with United States Code, Title 10.[7] The long standing military impacts of the Act were the creation of the United States Air Force, the unification of the independent military departments under the DoD and the first formal

[6] Joint Chiefs of Staff (JCS). *Joint Publication 0-2: Unified Action Armed Forces (UNAAF).* 10 July 2001. (Page I-1)
[7] United States Congress. National Security Act of 1947. Public Law No. 80-253, 80th Congress, first session. (Various pages)

Congressionally documented concept of a Combatant Commander (COCOM).[8] The COCOM definition was vague at best – the Act stated "…provide for the unified strategic direction of the combatant forces, for their operation under unified command, and for their integration into an efficient team of land, naval, and air forces…". This initial step did lay the groundwork for things to come.[9]

This Act was the first statute to address COCOMs, but, in doing so, Congress was sure to support independent Service operation. This was the initial step in the balancing act between combat operations and Service operations. In addressing this issue, the Act states:

> "…Department of Defense, including the **three military Departments** of the Army, the Navy (including naval aviation and the United States Marine Corps), and the Air Force under the direction, authority, and control of the Secretary of Defense; to provide that each military department shall be separately organized under its own Secretary and shall function under the direction, authority, and control of the Secretary of Defense; to provide for their unified direction under civilian control of the Secretary of Defense **but not to merge these departments or services.**"[10]

Highlighted above are the key elements of this passage – Congress does not give the Secretary of Defense or the President the authority to increase or decrease the number of military departments (Services). The Congressional intent was to protect the independent operation of the Services. At the time the Act was passed – the primary

[8] The Information Warfare Site (IWS). "Overview of National Security Structure." 2006, http://www.iwar.org.uk/military/resources/us/national-security-structure.htm. (No page number)
[9] United States Congress. National Security Act of 1947. (Section 2)
[10] United States Congress. National Security Act of 1947. (Section 2)

military establishments were the War Department and the Navy Department (along with the Marine Corps), the Act established the Air Force by splitting out the Army Air Corps from the War Department (the Army). It would be short sighted to assume that the military departments did not influence or shape Congressional intent – it would also probably be short sighted to believe that this arrangement did not meet with President Eisenhower's intent and approval, considering this effort was originally his concept, and he lobbied then President Truman to sign the Act into Law[11].

The Service Secretaries were given specific authorities which, over time must have conflicted with the Secretary of Defense's ability to operate and control DoD effectively. This management issue led to the 1949 amendment to the National Security Act; the purpose of which was to give the Secretary of Defense additional control over the military departments.[12] Apparently, the original Act stressed independent departments to the point where the DoD was not as efficient or effective as it could be.

United States Code, Title 10; Subtitle A, Part I, Chapter 6

With the initial COCOM concepts moving forward, Congress updated the premise with the United States Code, Title 10 – Armed Forces. Under this Code, Congress dedicated Subtitle A, Part I, Chapter 6 to the COCOMs. A key Congressional intent was to specifically clarify the roles of the Services and the COCOMs, which they do quite well.

---

[11] Department of State (DoS). *The National Security Act*, http://www.state.gov/r/pa/ho/time/cwr/17603.htm. (No page number)
[12] Department of State (DoS). (No page number)

Chapter 6 codifies the concept of COCOMs in great detail, spelling out that the commands exist to perform "military missions" (Section 161, subparagraph a.1).[13] The term military mission is important; its intended meaning becomes apparent in examining additional sections of the Act:

1. Section 162: The services shall assign forces to the Combatant Commanders as directed by the Secretary of Defense. Geographic Combatant Commanders shall have the forces within their geographic region assigned to their command, unless otherwise directed by the Secretary of Defense.
2. Section 164, Subsection C.2.A: The Secretary of Defense shall ensure that a commander of a Combatant Command has sufficient authority, direction, and control over the commands and forces assigned to the command to exercise effective command over those commands and forces.
3. Section 166: COCOM budgeting – Examples given for a COCOM budget are:
    a. Joint exercises
    b. Force training
    c. Contingencies
    d. Selected operations[14]

Numbered sections 1 and 2 above define the COCOMs position over the forces presented to them. In execution of the COCOMs mission (fighting a war) they have the ability to direct forces, organize forces, etc. The Congressional intent is to give to the

[13] United States Congress. United States Code, Title 10 – Armed Forces, Subtitle A – General Military Law, Part I – Organization And General Military Powers, Chapter 6 – Combatant Commands. (Section 161, subparagraph a.1)
[14] United States Congress. United States Code, Title 10. (Section 166, subparagraph b)

COCOM the authority they need to "fight and win" the engagement. The Services are not in the combat operations chain of command – Section 162, Paragraph 4.b is explicit on this issue. Combat operations chain of command runs from the President through the Secretary of Defense, then to the COCOM commander.[15]

Section 3 above, further supports the premise that the COCOMs are operations oriented – they plan, train, exercise and conduct operations for which they are funded. And, thus, their budgeting incorporates the same concept. Section 166a supplements the budgeting list – but does not get away from the operations premise.[16] COCOMs are not funded to buy aircraft, ships, tanks, or for maintenance of these systems. They are also not funded to address internal Service operations such as Service training, recruiting, installation maintenance, personnel operations, spare parts sourcing/supply/quality evaluation or information systems. These activities are internal Service operations and do not fall under the umbrella of combat operations. Information systems are important – the COCOM is not funded to purchase Service information systems, web servers, database systems, file storage systems, routers, switches, email, etc. Each Service operates its own information systems and infrastructure to support internal Service operations. Later we will discuss the overlap between information systems that address Service operations as well as COCOM combat operations. But, at this time, it is important to see that Service operations are specific to the Services – not the COCOMS. This takes us back to Congressional intent – Congress, with Presidential consent, drew

[15] United States Congress. United States Code, Title 10. (Section 162, Paragraph 4.b)
[16] United States Congress. United States Code, Title 10. (Section 166a)

the line between Service operations and COCOM operations, and Congress is maintaining that balance.

As we move forward in time, each Congressional Act continues to paint this picture of Service and COCOM operations being different activities. Congress' intent comes through again as quoted by the Army JAG web site addressing National Security Structure and Strategy, when it states;

> "These departments [Air Force, Army and Navy] are responsible for ensuring that combatant commanders have the forces and material necessary to fulfill their war fighting missions. The military departments may retain forces for their inherent service functions of recruiting, organizing, supplying, equipping, training, mobilizing, administering, and supporting the military forces."[17]

At this point Congress and the President have clearly defined the role of the COCOMs and the Services. But, Congress felt the need to tighten the wording up even more – this tightening has implicit impacts for cyberspace discussions. The DoD Reorganization Act of 1958 explicitly took the COCOMs out of certain military activities.

Department of Defense Reorganization Act of 1958, Public Law 85-599

The DoD Reorganization Act of 1958 continues as the previous legislation has – it refines the concepts already in place and explicitly "draws lines" between organizations where Congress feels it is appropriate. For example, Section 3 states, "The Secretary of a

[17] Judge Advocate General's Corps (JAGCNET), United States Army. "Chapter 24: National Security Structure and Strategy," https://www.jagcnet.army.mil/JAGCNETInternet/Homepages/AC/CLAMO-Public.nsf/0/1af4860452f962c085256a490049856f/$FILE/Chapter%2024%20-%20National%20Security%20Structure.htm. 13 October 2006. (No page number)

military department shall be responsible to the Secretary of Defense for the operation of such department as well as its efficiency".[18] Why would it be necessary for Congress to state that the Service Secretary is responsible in this way? The Congressional intent is to make it clear to the Secretary and to all other military organizations what the Service Secretary's role is. One of these roles is to address Service "operations", i.e. non-combat operations. Apparently, it needed to be specifically stated.

Congress was also concerned with duplicative operations in the DoD. These operations were Service unique activities and were seen as a possible place to save funding. In an attempt reduce spending, DoD was directed to consolidate duplicative activities under the purview of the Secretary of Defense. Section 3 states the following (emphasis added):

> "Whenever the Secretary of Defense determines it will be advantageous to the Government in terms of effectiveness, economy, or efficiency, he shall provide for the carrying out of any supply or **service activity** common to more than one military department by a single agency or such other organizational entities as he deems appropriate. For the purpose of this paragraph, any supply or service activity common to more than one military department shall ***not*** be considered a 'major combatant function'…"[19]

This paragraph is very important for two reasons. First, it implies issues of effectiveness, economy and efficiency for Service activities are not the concern of the COCOM. This

[18] United States Congress. Department of Defense Reorganization Act of 1958. Public Law 85-599, 85th Congress, second session. (Section 3)
[19] United States Congress. Department of Defense Reorganization Act of 1958. (Section 3)

continues the Congressional position of ensuring that the Services are protected and do not become lesser activities with the empowering of the COCOMs.

Second, the paragraph states that DoD may establish an agency to address common Service activities – while maintaining that these activities are not combatant functions. DoD has exercised this option in the past – for example, the Defense Finance and Accounting Service (DFAS) was established in 1991 to reduce cost and improve financial management by rolling up, to one organization, the DoD's dispersed financial infrastructure.[20] The establishment of DFAS met the intent of what Congress was trying to accomplish within this Act: the consolidation of non combatant Service duplicative activities. (The importance of this issue will become apparent shortly.)

As Congress states, Service activities that are common among Services may be combined if there is a cost, efficiency or effectiveness savings. If there are no savings, then the activities stay as Service operations. The Congressional intent was three fold:

1. Attempt to save funding.
2. Protect Service operations (if not consolidated)
3. Identify the boundary between COCOM operations and these new Agency operations.

This is a very important point as we see how cyberspace fits into the current DoD organization.

[20] Defense Finance and Accounting Service (DFAS). *Defense Finance and Accounting Service, About DFAS: Our History*. http://www.dfas.mil/about/OurHistory.html. (No page number)

Goldwater-Nichols Department of Defense Reorganization Act of 1986, Public Law 99-433

I briefly mentioned this Act earlier when I addressed the message from President Ronald Reagan to the 99th Congress. This act does not impact cyberspace discussions directly. It does, however, fit well into the legal discussion to this point. Pertinent to cyberspace discussions, the two key notions from this act are:

1. It supports Service shared procurement, which promotes system integration and is essential for DoD level cyberspace operations.
2. It continues to specify joint roles, this time for the Joint Staff. "The Joint Staff shall not operate or be organized as an overall Armed Forces General Staff and shall have no executive authority."[21]

This act restates the concept that the Service Chiefs and the Chairman of the Joint Chiefs of Staff are not in the operational chain of command.

Federal Law Wrap-Up

The President, Congress, and the Services have worked to shape the military establishment over time. What has evolved is a concept balanced between establishing joint commands to conduct joint operations and preserving the integrity of the individual Services. The above legal references specifically address the differences between "engaging the enemy" operations and "running a Service" operations.

[21] United States Congress. Goldwater-Nichols Department of Defense Reorganization Act of 1986. Public Law 99-433, 99th Congress, second session. (Section 155.e)

The key Federal Law constructs that impact the relationship between the COCOMs and the Services that will affect our cyberspace discussion are:

1. COCOMs are responsible for Warfighting (Defense and Offense) – Not the Services.
2. Services are responsible for Service operations – Not the COCOMs.
3. COCOMs do not take on Non-Combat activities – Supporting Services or Agencies provide Non-Combat support activities.
4. Services purchase weapons and provide for maintenance – COCOMs do not.
5. COCOMs ensure Services are meeting the COCOMs Warfighting requirements (capabilities).
6. Services are responsible for providing fighting forces to the COCOMs – COCOMs do not have inherent Combat forces.
7. Combatant Chain of Command bypasses Service Chiefs.

I identified the legal constraints for the Services and the COCOMs to make sure all readers are at the same level of understanding with respect to what a Service does and what a COCOM does (I am not a lawyer, and my review is from a layman's perspective shaped by operational experience). It is important that we all understand these constraints when we discuss the roles of the COCOMs and Services with respect to cyberspace.

In taking a quick look at the above, it becomes apparent that Network Maintenance is a Service activity just as aircraft or ship maintenance is. Aircraft and/or ship maintenance is never turned over to a COCOM to manage, support, or direct daily activities. And, on the other side of the fence, network attack is solely a COCOM activity

– a Service should never engage in a network attack without being under the command of a supported COCOM. A Service, of course, provides the forces for the network attack activity. All the network related constructs of cyberspace will be discussed in more detail as we fill in the rest of the puzzle.

Joint Doctrine

Joint and DoD documentation is, as expected, heavily centered on the joint view of Operations. Nonetheless, the following documents were reviewed:

1. Joint Publication 1, Joint Warfare of the Armed Forces of the U.S.
2. Joint Publication 0-2, Unified Action Armed Forces
3. DODD 5100.1, Functions of the Department of Defense and Its Major Components

The documentation is explicit on identifying the authority of the COCOM Commander, and provides more granularity than exists in Federal Law. But, there is nothing present that contradicted Federal Law as documented above. We must make sure that future revisions continue to stay balanced with Congressional Intent (and Federal Law). Service and COCOM responsibilities from Joint Publication 0-2 are in Appendices A and B respectively.

Cyberspace Domains

Combatant Commands (COCOMs)

COCOMs have a specific role in the DoD. If the U.S. is involved in a conflict, the COCOM that directs the U.S. response is pretty clear. Forces are easily allocated to the COCOM that is responsible for some geographic portion of the world. The key COCOMs that may engage in lethal combat operations are Central Command (CENTCOM), Southern Command (SOUTHCOM), European Command (EUCOM), Pacific Command (PACOM), Special Operations Command (SOCOM), Northern Command (NORTHCOM), and Strategic Command (STRATCOM). The COCOMs that are not as likely to be involved in lethal actions are Transportation Command (TRANSCOM) and Joint Forces Command (JFCOM).

The Geographic COCOMs are assigned a geographic Area of Responsibility (AOR) by the National Command Authority (NCA).[22] The Geographic COCOMs are CENTCOM, PACOM, SOUTHCOM, EUCOM and NORTHCOM seen below in the map from the Wikipedia web site (Figure 3).[23] The other lethal COCOMs are global in nature.

[22] Joint Chiefs of Staff (JCS). *Joint Publication 0-2*. (Page II-12)
[23] Unified Combatant Command (COCOM). http://en.wikipedia.org/wiki/Unified_Combatant_Command. (No page number)

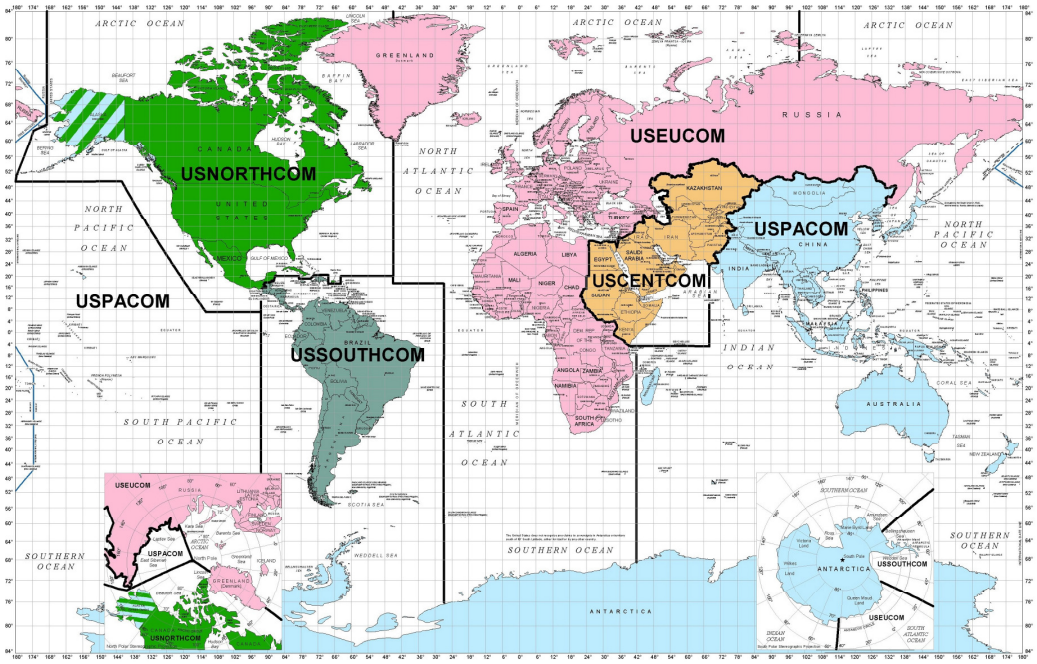


Figure 3. The Geographic COCOMs

STRATCOM uses the term NetOps all throughout their documentation. Based upon Congressional intent, a COCOM's definition of NetOps may only contain offensive and defensive operations; it does not contain Service network operations or DoD enterprise operations. STRATCOM does not operate the DoD network; they use it as a platform to attack from, and for which they are responsible to defend. STRATCOM responsibilities cannot include network infrastructure ownership, maintenance or Service specific activities (unless one of these activities introduces security issues for the enterprise). This concept will become even more apparent in the next few pages.

Geographic COCOMs and STRATCOM

STRATCOM, as a global COCOM, was given responsibility for defending the DoD Global Information Grid (GIG) which is the DoD enterprise network. They

accomplish this defense mission via the Joint Task Force – Global Network Operations (JTF-GNO). Simply put, JTF-GNO is the organization responsible under STRATCOM for defending the DoD enterprise network. STRATCOM also has the responsibility for DoD level Network Warfare via the Joint Functional Component Command - Network Warfare (JFCC-NW). The question is: how does a COCOM maintain global responsibility over AOR assets when the geographic COCOM has NCA granted authority over their AOR? Apparently, this problem has been addressed – according to the Joint Concept of Operations (CONOPS) for GIG NetOps, Version 3, dated 4 August 2006; STRATCOM was granted NCA authority over Global Network Operations.[24] Geographic COCOMs address issues within their theater to a point. This is captured in the STRATCOM decision matrix, Figure 4 below.[25]

Criteria / Incident	CROSSES THEATER BOUNDARY	IMPACTS MULTIPLE COCOMS	IMPACTS OTHER AGENCIES	BEYOND THEATER CAPABILITIES	GLOBAL EVENT?

Figure 4. Decision Matrix (Joint GIG NetOps CONOPS)

On the global side, for STRATCOM to exercise operational control over the GIG, it becomes cumbersome without some kind of network operations linkage. So, STRATCOM and the DoD appeared not to address the legal limitation of COCOM control of network operations that are outside of combatant operations. Their response was to appoint as commander of JTF-GNO, the director of the Defense Information

[24] United States Strategic Command (USSTRATCOM). *Joint Concept of Operations for Global Information Grid NetOps* (Version 3). 4 August 2006. (Page 4)
[25] United States Strategic Command (USSTRATCOM). (Page 11)

Systems Agency (DISA). DISA is one of those DoD agencies that resulted from the DoD Reorganization Act of 1958, similar to DFAS (as described previously). DISA was originally established as the Defense Communications Agency (DCA) in 1960, by Secretary of Defense Thomas Gates; its mission was to consolidate the independent long-haul communications functions of the Army, Navy, and Air Force. In 1991 DCA became DISA to reflect its role in providing information Systems Management for the DoD.[26] What is different about DISA, when compared to DFAS, is that DISA's day-to-day operations directly support/impact the COCOMs missions with immediate implications. For this reason, Defense agencies may end up in a supporting role to a COCOM. Being a DoD agency (of the type created under the authority of the 1958 DoD Reorganization Act) in a supporting role to a COCOM also means, that the support provided is not of a combatant nature – it can't be, because Federal Law directed the Secretary of Defense to "roll up" only support activities in an effort to reduce funding, not combat activities. DoD agencies created under this provision do not provide combatant forces to a COCOM, the Services do – this is a critical point with respect to non-combat network operations (Service-like network operations). If DISA's network operations were considered "combat operations" (offensive or defensive), then these activities would have to move back to the Services, and then the Services would provide network combat forces to the COCOMs.

Having the DISA director dually hatted with the JTF-GNO/CC position is an issue of legal concern, and should be addressed by the appropriate legal authorities.

---

[26] Defense Information Systems Agency (DISA). *Defense Information Systems Agency: History of DISA.* http://www.disa.mil/main/about/history.html. (No page number)

Also, any DISA forces chopped to STRATCOM for JTF-GNO would appear to be in direct violation of the 1958 DoD Reorganization Act. If this is a future intent, or has already taken place – then the appropriate authorities in DoD and in Congress should be engaged to work either a new arrangement (such as moving only these specific activities back to the Services) or to modify Federal Law. I am in favor of supporting President Eisenhower's original delineation of responsibilities and powers – these activities should be moved back to the Services. It would also be best to keep these capabilities centralized and not scatter DoD wide protection systems across the Services, thus the DoD lead for cyberspace should take over this mission. Either that, or create a cyberspace Service with the help of Congress. This independent cyberspace Service concept is not a new idea, Martin Libicki, Institute for National Strategic Studies, discusses it's implications is his publication, "What is Information Warfare?"; where he makes some good points for such a Service.[27]

STRATCOM, also, cannot absorb DISA for two primary reasons under Federal Law: 1. A COCOM does not perform day-to-day non-combat operations, and 2. Common across Service non-combat activities cannot move to a COCOM – these activities can only be rolled into a DoD agency. DISA performs non-combatant activities, thus they perform non-COCOM activities. STRATCOM is given complete control to perform operations (offensive and defensive) as required, with respect to the network. STRATCOM can not be given DISA's job, and STRATCOM was not intended to be

[27] Libicki, Martin. *What is Information Warfare?* National Defense University, Institute for National Strategic Studies, Advanced Concepts and Information Strategy, August 1995. (Chapter 11)

DoD's version of America On Line (AOL) – no COCOM can take on the role of being DoD's AOL.

STRATCOM identifies DoD Chief Information Officer Guidance and Policy Memorandum No. 10-8460 – Network Operations, 24 August 2000 as the "foundational document that established a GIG 'operational hierarchy' that promoted COCOM oversight of component network management capabilities, while providing SA (situational awareness) of the GIG."[28] The problem with this memorandum is that it may be read to imply more than what Federal Law will allow. As long as STRATCOM is specifically limited to defensive and offensive operations, the Memorandum is executable without violating Congressional intent. Situational awareness would be required for network defense operations, and is a viable COCOM activity.

STRATCOM also identifies "Presidential authority in the Unified Command Plan (UCP) and Secretary of Defense approval provided in the Forces For Unified Commands Memorandum (2006)" as the subsequent authority.[29] The issue then becomes again, are we reading more into these documents than was intended? Congressional intent, as already agreed to by the Office of the President, does not authorize STRATCOM to operate DoD networks. But, it does authorize STRATCOM to direct offensive and defensive operations. Federal Law supersedes the UCP if there is a conflict between the documents.

Geographic COCOMs are now in a familiar position with respect to global network combat operations. They have had to rely upon TRANSCOM for logistics

[28] United States Strategic Command (USSTRATCOM). (Page 4)
[29] United States Strategic Command (USSTRATCOM). (Page 4)

support and have had to rely upon STRATCOM for space asset support. These two critical support activities have placed the Geographic COCOMs in a position where their ability to execute their mission depends upon other supporting COCOMs.

Excluding the strategic nuclear option, the Geographic COCOMs have traditionally controlled all combat operations that take place within their theaters. Geographic COCOMs have been given the authority to act in their respective AORs. Federal law does not limit the Geographic COCOM commander's authority to only the physical realm. An argument can then be made that a COCOM should control the space above their AOR, federal law does not limit that aspect either.

Within the space arena, satellites do not "fly" in AOR based patterns – they fly in global patterns. Controlling the area of space above an AOR in the same manner that the Air Operations Center (AOC) controls air space today, is not feasible. If control of the space AOR changes in the future, then the relationship between DoD space forces and Geographic COCOMs may change also.

With respect to cyberspace, Geographic COCOMs can affect cyberspace operations via localized activities within their AOR – via air, ground or cyber attacks. By being able to localize these activities, a Geographic COCOM can demonstrate their capability of operating within their portion of cyberspace that is bounded by their geographic AOR. This point of detail can not be dismissed by STRATCOM or the DoD. This point is also very specific – the Geographic COCOM must, beyond any doubt, understand who owns the resources (adversary, American corporate, other nation state) they are about to attack. The legal and diplomatic implications can grow exponentially.

The above concept works fairly well from a geographic perspective. But, cyberspace advocates' primary arguments against Geographic COCOM centered cyberspace activities are based upon the following:

1. Network warriors performing network attacks may be centered in the CONUS – they may not be forward deployed or inside the Geographic COCOMs AOR
2. Legal restrictions
3. Cyberspace activities become global within seconds
4. Second and third order effects (possibly outside the Geographic COCOMs AOR) must be understood before action is taken

These issues made more sense when the DoD first moved into the cyberspace warfare arena. But, as the concepts have matured, some are no longer the "show stoppers" they were in the past. With that said, they have to be addressed properly.

Let's look at the first example above – military organizations have crossed this bridge and have guidelines on how to operate in this environment. It is fairly new, but the Geographic COCOMs understand how to make it work. For example, the Air Force has flown UAVs in CENTCOM's AOR, with the pilots sitting in the continental U.S. It is also not uncommon for an aircraft to support CENTCOM while launching and recovering from EUCOM's AOR. When the aircraft is airborne, the aircraft and its pilot are under the operational control of CENTCOM once the aircraft enters CENTCOM's AOR. What the Air Force UAVs have changed about the scenario, is the aircraft launching, flying, and recovering in CENTCOM's AOR while the pilot, that is responding to CENTCOM's directions is sitting in NORTHCOM's AOR. This was a first of its kind for the DoD, this was the first time that combat force has been directly

operated by remote control with this degree of freedom. This same concept applies to cyberwarfare activities. When actions are being taken within a COCOM's AOR – the individuals responsible for those activities may be in another COCOM's AOR. Cyberspace operations are an abstraction of AF UAV operations. Whether the pilot is controlling a UAV or a cybercraft, it does not matter – remote tactical operations are being used today, and are here to stay.

This concept also applies to combat operations; for example, AF UAVs are involved in lethal engagements – just as cyberspace activities may have lethal consequences. Near Balad, Iraq – insurgents were monitored via an AF UAV as they dug a hole, planted explosives, and then strung wire to detonate it remotely. Once it was realized that these individuals were terrorists, the UAV fired an AGM-144 Hellfire missile, eliminating the threat and killing the terrorists.[30] This is lethality by remote control over networked systems – not much different than cyber operations, except that the UAV's weapon was kinetic based. Differing ends do not limit the significance of similar means. However, this reach-back approach is not completely without its problems which will become apparent in a later section – some cyberspace activities are better suited for reach-back operations than others.

Legal restrictions have become part of normal operational concerns for all COCOMs. The military legal establishment is well aware of the legalities of military action in cyberspace. The COCOM staffs are very capable of advising their commanders. If, they find themselves in an area where they need further guidance –

[30] Sky Control: Aviation and Aerospace News, "Predator UAV Kills Terrorists", 28 April 2006 http://www.skycontrol.net/uav/predator-uav-kills-terrorists. (No page number)

STRATCOM, as the supporting COCOM and as the DoD cyberspace lead, can assist. The legal environment is evolving but is currently falling behind cyberspace developments; so it is extremely important to develop cyberspace legal authorities who specialize in this new domain – at least for the near term. The third and forth arguments against geographic COCOM cyber activity are a little different. From a DoD perspective, number three is more of a defensive activity and number four relates more to offensive activities. The dynamic nature of offensive cyberspace activities will cause the legal restrictions discussion to surface again.

Cyberspace defense has two distinct operations – active and passive. Passive defense activities are network security activities taken daily at all levels to ensure security of the enterprise. *Passive security is inherently a Service responsibility*, similar to guards at base gates, safes for classified material and flight line security. Day-to-day activities for these types of security are addressed locally. The two COCOM roles in passive security are:

1. Directing a change in the security threat level – such as moving to a higher Information Condition (InfoCon). With an increased security posture, the Service's continue to direct (operate) day-to-day passive security activities.
2. Directing security standards for the overall defense of the DoD GIG. Such as maintaining adequate patching and setting minimum standards for network monitoring and reporting.

These activities build a standardized security baseline from which a Geographic COCOM could confidently launch when implementing active defensive measures.

Active defense is primarily a Geographic COCOM responsibility to direct.

Active defense is a Geographic COCOM's direct response to an on going cyberspace attack. Active defense is not an offensive act – it is actively securing their cyberspace perimeter. This is where number three, from above, hits home; attacks in cyberspace seldom limit themselves to geographic boundaries. In attempting to attack a specific COCOM, the attackers may not even know that they are really attacking facilities outside the Geographic COCOM's AOR – and the same is true in reverse. The COCOMs must insure that their cyberspace targets are physically located where they think they are. For example: the internet naming standard for a specific country's internet addresses usually ends with the country's identifiers: France uses .fr, the United Kingdom uses .uk and Iran uses .ir. If a COCOM wanted to "tie up", for example, all key .ir (Iranian) web servers to stop information from flowing for some specific period of time – it could be easily accomplished. What if one of the primary targets was the Iranian News Agency web server? The Iranian News Agency's web server is named www.irna.ir , and the web server is located in Cary, North Carolina. What problems does this introduce?

Organization	Web Address	Location
Central Bank of Iran	www.cbi.ir	United Arab Emirates
Iranian Students News Agency	www.isna.ir	Vancouver, B.C., Canada
Mehr News of Tehran	www.mehrnews.ir	San Antonio, Texas
Iran Daily News	www.irandaily.ir	Cary, North Carolina
Iranian News Info & Research	www.iras.ir	United Kingdom
Physical Science of Iran	www.psi.ir	Toronto, ON, Canada

Figure 5. Key Iranian Web Sites[31]

Note: The Physical Sciences of Iran web site lists government sponsored articles on Iran's nuclear program.

[31]Google, www.google.com. (No page number)

As the Services provide more and more Geographic COCOM support via reachback, it is very likely that GIG defensive activities will be global at the onset of cyber hostilities (especially with adversaries not knowing the location of the systems they are attacking). The same holds true for our adversaries systems. In the above example for Iran, does it make Iranian news sources more or less secure to be scattered around the globe. An attack against the news sources above places Iran under global attack due to the distributed locations of their systems. If the adversary is a state entity, the legal establishment may intervene (number 2 from above) – especially if the adversary is the DoD and one of the news sources is in San Antonio (see Figure 5 above). It should now be easy to see that our cyberspace adversaries may not be capable of, or even care to, limit their attack to the COCOM's geographic boundaries that DoD established – the better questions is "Why should they", they don't have to play by our rules. To assume that they will, would be a big mistake.

Geographic COCOMs have legal authority to act in their AOR, but they must think global – they have to, their adversaries are; especially in cyberspace. For defensive purposes, the responsibilities should be:

	STRATCOM	Geographic COCOMs	Services & Agencies
Primary responsibility for	Global defense & GIG defense	AOR defense	Service or Agency defense
Passive & Active Defensive activities	1. Directs global security posture 2. Sets global security standards 3. Informs COCOMs, Services and Agencies of all activities	1. Directs AOR security posture 2. Sets AOR security standards 3. Informs Services & Agencies within AOR & STRATCOM of all activities 4. Not responsible for DISA GIG infrastructure	1. Directs Service or Agency security posture 2. Sets Service or Agency security standards 3. Informs STRATCOM & Geographic COCOM of all activities
Passive Defense	1. Sets Global Network Security Threat Level 2. Set Global Minimum Security Standards	1. Sets AOR Network Security Threat Level when required to exceed STRATCOM's setting 2. Sets AOR Minimum Security Standards when required to exceed STRATCOM's standards	1. Directs day to day activities 2. Primary Responsibility for implementation 3. Sets Service or Agency Network Security Threat Level when required to exceed Geographic COCOM's and/or STRATCOM's setting 4. Sets Service or Agency Minimum Security Standards when required to exceed Geographic COCOM's and/or STRATCOM's standards
Active Defense	1. Assumes operational control for global events or when the DISA GIG infrastructure is threatened 2. Informs all COCOMs, Services and Agencies when assuming control 3. Exercise operational control via the Geographic COCOMs or via the Services (Note 1)	1. Assumes Operational Control for AOR events 2. May take defensive action beyond STRATCOM's guidance 3. Becomes supporting COCOM if STRATCOM assumes operational control 4. Will address AOR responses at Service level if the Service Requests (Note 2)	1. Directs Service or Agency First Response Activities 2. Takes defensive action as required until Geographic COCOM or STRATCOM guidance is received 3. May take defensive action beyond STRATCOM or Geographic COCOM guidance

Figure 6. STRATCOM, COCOM and Service Cyber Defense Security Matrix

Note 1: STRATCOM should choose to exercise their authority via the Geographic COCOM or via the Services. The primary means should be the Services – the explanation is documented in the Services Section below.

Note 2: With reductions in manpower and Service consolidations of network support activities, the Services may not have AOR level network control facilities. In which case, the Geographic COCOM would have to engage the Service level entity.

Service or Agency security posture and standards can not negate a directed Geographic COCOM security posture or standard; just as the Geographic COCOM security posture and standards cannot negate a directed STRATCOM security posture or standard. Now, let's move from defense to offense.

As warfare changes, so must our concepts of engagement, domain, vulnerability and exploitation change – just to name a few. Any environment in which an adversary may attack the United States must be an environment in which the DoD can operate freely for the defense of the nation. The idea of challenging our concepts is also nothing new; President Reagan wrote the following in his message to the 99th Congress when they were debating the Goldwater-Nichols DoD Reorganization Act of 1986;

> "President Eisenhower observed a revolution taking place in the techniques of warfare. Advancing technology, and the need to maintain a vital deterrent, continually tests our ability to introduce new weapons into our armed forces efficiently and economically. It is increasingly critical that our forces be able to respond in a timely way to a wide variety of potential situations. These range across a spectrum from full mobilization and deployment in case of general war, to the discriminating use of force in special operations. To respond

> successfully to these changing circumstances and requirements, our defense organization must be highly adaptable."[32]

Network attack is not the killing of Net-Bots or the eradication of viruses. Network attack is an act against a cyberspace entity (computer, server, communications link or digital information) to cause a specific effect. Some attacks may have a physical result, such as opening a dam to flood an area to make roads impassable; others may just result in the loss of an adversary's information. There are, of course, subcategories of net warfare, like cyber reconnaissance and surveillance that may not be classified by some as net attack – but for simplicity, we will lump them all together for now.

Network attack within an AOR is a COCOM responsibility. As mentioned earlier;

> … Geographic COCOMs can affect cyberspace impacts via localized activities within their AOR – via air, ground or cyber attacks. By being able to localize these activities, a Geographic COCOM can demonstrate their capability of operating within their portion of cyberspace that is bounded by their geographic AOR.

If a COCOM can limit their activities to their AOR, Federal Law gives them the authority to keep control over those activities. The problem that surfaces is related to the discussion above concerning the Iranian servers being scattered around the world. The implications derived from an adversaries "smart" placement of systems could get overwhelming. If DoD were limited to attacking information systems that are physically

[32] Reagan, Ronald. President of the United States, Washington DC. "Defense Reorganization – Message From The President Of The United States; Transmitting His Views On The Future Structure And Organization Of Our Defense Establishment And The Legislative Steps That Should Be Taken To Improve Defense Reforms". (Page 3)

in our adversary's country, it could greatly limit our effectiveness. For example: what if the information manager for Iran's government placed key governmental servers in North Korea, Syria, Egypt, France, Venezuela, Cuba, Russia and China. They may just be in the local Embassy – but they could tie them into a local service provider to get a local IP address. Then, if the DoD were to try to stop information from flowing across Iranian systems, how would these other countries respond? Especially if Iran scattered their servers all around inside these countries to help make any attack appear to be an all out assault against the nations infrastructure. Worst case, the other nation states host Iranian governmental applications on their own governmental systems and servers. (More on this later)

Network attack does have a smaller, simpler side to it. It could be a small localized problem that a Geographic COCOM could address. The problem is: when is network attack a Geographic COCOM's responsibility or STRATCOM's responsibility. Or, when is it limited to only an AOR and how can we guarantee it is limited. Network attack is different than network defense, the actions are more transitory. Offensive activities at one level may not sync well with activities at another level; desired global effects may be different than AOR desired effects.

Let's now take a look at an operations parallel: when would a Geographic COCOM use tactical nuclear weapons for example? They would use them when required, under the authority of STRATCOM (assuming the President has given the go ahead). Theater level war is a Geographic COCOM's responsibility, once the Geographic COCOM uses nuclear weapons, it operates those weapons under the control STRATCOM. Because tactical nuclear events can impact the more important strategic

nuclear events, single point control is vital to ensure that the United States' Nuclear Engagement Plan is not adversely affected. This is a very simplistic view and is meant to serve only as an example.

It appears that cyberspace falls in to a similar category. We would want to make sure that tactical network attacks do not impact the DoD's ability to affect global offensive network actions. A Geographic COCOM should attack in cyberspace under the limits imposed by STRATCOM, and under the authority and control of STRATCOM. STRATCOM should reserve the right to assume authority over operations if global activities warrant – this decision would rest solely with STRATCOM for Network Attack activities. Geographic COCOM network attack forces should become supporting forces to STRATCOM, if STRATCOM assumes operational control. This then begs the question, how do you organize these forces, and where should they be located?

It would be very problematic for STRATCOM to take on network defense or network offensive activities from one central geographic location. Centralized activities are centralized targets in cyberspace, geographic dispersal is essential. Network defense activities are generally dispersed due to their tie to network operations (more on that later). Network attack capabilities need to be centered on STRATCOM and the Geographic COCOMs, with the Geographic COCOMs being the primary physical locations for the forces (even if they are supporting STRATCOM in a global event). ***Geographic COCOMs can not perform network attack activities without Service provided local forces in their AOR.*** Consider the following: assume network attack forces were located in San Antonio, Texas, and CENTCOM requested all email servers in Iran be brought off line. As soon as action was under way, Iran could start retaliating

against their attackers. Our network warriors are in Texas – outside the Geographic COCOM's AOR, hence the effort instantly becomes a STRATCOM issue and the Geographic COCOM loses the authority almost instantly because Iran is attacking a location (Texas) outside its AOR. STRATCOM would not have a choice – they may not know from where the attack against facilities in Texas originated, and they may have no proof that our attack against Iran is related to the Texas event; so, immediate action is required on STRATCOM's part to defend the DoD GIG. This defensive action may also end up offensive in nature – thus the Geographic COCOM could lose effective control in almost all cases.

The Service that assumes the DoD role as the Service cyberspace primary must establish network attack cells in every Geographic COCOM's AOR. STRATCOM must also establish liaison cells to work with the Service lead and the Geographic COCOMs. If these network attack cells are not established, then the Geographic COCOMs may essentially never control network attack scenarios – even in their AOR. This does not mean to imply that these cells may be small and plused up by deployments as required, time is too critical in this domain, and influence operations are a full-time on-going activity.

TRANSCOM

TRANSCOM has no role in network attack. They do, however, have a role in network defense. Their role should be similar to a Service role (refer to Figure 6 above, the Services and Agencies column). TRANSCOM's supporting forces work to defend the information systems that are needed for TRANSCOM's mission. TRANSCOM's

logistics support is global and their information systems are global for resource tracking. These TRANSCOM systems that the supporting Services use are local to the base. In most cases they are partitioned apart from the normal base infrastructure to some degree. And, activities that take place in one theater may also severely impact TRANSCOM operations in another theater due to their systems global nature.

Geographic COCOMs have the responsibility to help protect TRANSCOM's systems as a second line of defense – they are the supporting COCOM to TRANSCOM for network defense in the local AOR. TRANSCOM should have the right and authority to request support from STRATCOM when they feel it's necessary. STRATCOM is the final authority in defending TRANSCOM's networks. STRATCOM has the authority to move to a higher security level and to take control of TRANSCOM's active network defense as the threat dictates. The decision matrix should be similar to Figure 7 below.

	Simple Network Security	Elevated Network Security	Network Security Emergency
Primary	TRANSCOM	TRANSCOM	STRATCOM
Supporting		Geographic COCOMs and STRATCOM	TRANSCOM

Figure 7. TRANSCOM Escalation Table

SOCOM

SOCOM's defense role should be identical to TRANSCOM's. It is understood that tactical network security may solely rest upon SOCOM's forces if they are deployed. In this case STRATCOM should be the supporting COCOM for these small tactical parties, if applicable.

SOCOM has two distinct subcategories with respect to network attack, tactical and non-tactical (Home Base). STRATCOM has full authority over global activity, hence network attack activity from a non tactical location would have to be coordinated with, and should be approved by, STRATCOM.

SOCOM's tactical network attack activities must be coordinated with and approved by the Geographic COCOM or STRATCOM, which ever is applicable based upon the target. What's different about this mission is that it gives DoD forces the ability to act within our adversaries' domain even if it is isolated from the internet. Special Operations Forces behind our adversaries' lines could introduce problems within their networks, gather information, or plant information – for a multitude of desirable effects. These capabilities teamed with Geographic COCOM and STRATCOM capabilities may be very effective in future engagements. This means that some component of Special Operations Forces need advanced networking skills so that they may be employed to their maximum extent.

Services

The Services are a protected entity based upon Federal Law, the DoD can not merge or dissolve them. The relationship with the COCOMs is also clarified in law to protect the missions of the Services and to establish the COCOMs as the DoD war fighting commands. Both of these concepts are important to understand before we move forward with the Service discussions. In an effort to clarify the key points of Service activities, I will use the Air Force (AF) as the Service cyberspace primary basis for my examples.

The Services organization and internal operations have an impact on network defense and attack. It is important to view networks based upon ***all*** the daily activities that take place. We can neatly carve Service network activities into five discernable capabilities;

1. Network Attack (Net-A) – Discussed previously
2. Network Defense (Net-D) – Discussed previously
3. Network Operations (Net-O) – Activities that are undertaken to operate the network. The, not fully inclusive, list is:
    a. Maintain Situational Awareness and report network status
    b. Manages configuration of all infrastructure equipment
    c. Directs work-around activities for outages
    d. Directs and Schedules Network Maintenance Activities
    e. Performs real-time adjustments for flow control problems
    f. Manages all E-Mail servers and data servers
    g. Manages authentication systems (Active Directory, etc)
    h. Manages remote access systems (OWA, VPNs, etc)
4. Network Maintenance (Net-M) – Activities that are undertaken to maintain the network. The, not fully inclusive, list is:
    a. Replacement of faulty hardware or software
    b. Upgrade in hardware or software
    c. Repairing faults in software, hardware, or circuits
    d. Installation of expansion equipment and software
    e. Initial configuration of systems

f. Maintains all network diagrams

g. Establishes network accounts

h. Troubleshooting problems and operates Help Desk

i. Assist with Network Criminal Investigations

5. Network Criminal Investigations (Net-CI) – Any actions undertaken to assist with law enforcement activities, criminal investigations or evidence gathering.

Taking each of the numbered items above and assigning them to the Services or the COCOMs (not distinguishing between Geographic COCOMs and STRATCOM) produces the matrix below;

	Service	COCOM
Net-A	Provides Capability to COCOM	Primary Responsibility
Net-D	Provides Capability to COCOM (Services Perform Passive Defensive Activities As Part Of Daily Ops)	Primary Responsibility (Active Defense)
Net-O	Service Activity (May Provide Capability to COCOM)	Local To COCOM Infrastructure (Note 1)
Net-M	Service Activity (May Provide Capability to COCOM)	Local To COCOM Infrastructure (Note 1)
Net-CI	Service Activity	Local To COCOM (Note 1 and Note 2)

Figure 8. Service vs. COCOM Network Responsibilities (Service Perspective)

Note 1: The COCOMs will also need to be made aware of any major Service Net-O, Net-M or Net-CI activities.

Note 2: At the national level, STRATCOM will be the DoD interface to DHS; and, as such, the national level interface to the civil legal authorities. Net-CI activities referred to a Service via STRATCOM become a Service issue to work. The Net-CI activity is not a COCOM activity, STRATCOM just serves as the intermediary between the Service and the DHS.

Net-CI is self explanatory, so we will not get into the details of the subject in this section; there will be more on this issue when we discuss the military and civil authority relationship. Net-M is a Service activity that will impact Net-O from time to time. As discussed earlier, Net-M is an activity like on board ship maintenance or aircraft maintenance – these are not COCOMs activities.

Net-O is the activity that a Service performs each day to keep the network functioning correctly. This is the key distinction between Service operations and COCOM operations, which is centered around Net-A and Net-D. Service Net-O activities are more closely linked to Met-M activities. Service operations are specific to the way each Service functions, which helps explain why the networks were built in the first place.

The Air Force built their network to address internal operating issues. As the network infrastructure expanded into the combat operations realm, the network became essential to operations that support COCOMs. On a typical AF installation – the vast majority of network users are supporting AF operations and not COCOM combat operations. This should be true for each of the Services. Lost in the cyberspace discussions is that fact that Service networks are primarily used for Service operations. Loss of the use of the network may be a severe impact to one Service, and only a nuisance to another (which I would expect to change over time). What must be understood is that we are taking – what has been a non-military commercially driven tool that has been used to streamline and improve business processes – and, we are militarizing it. By doing so, does not mean that this "tool" still is not used primarily for its original purpose, business processes. This is an important concept for the COCOMs

to remember. The point to this dialog is that the Services built their networks to facilitate internal operations. As networks began to facilitate COCOM operations, the environment changed. Even though the environment shifted, the Services still predominantly use their Service networks for internal operations and support. This leads to the next major point, the future of Service networks and their impacts on the COCOMs.

Over time, the AF migrated many internal Service functions onto the network due to manning cuts, funding cuts, etc. As the AF is forced to draw down, it has to scale back on Service network support. With a large infrastructure, the only option available to the AF was consolidation of Net-M, Net-O and Net-D activities. Much of the Net-O and Net-D activities were accomplished in the AF Major Command's (MAJCOM) Network Operations and Security Centers (NOSCs). As the consolidation continues to move forward, the NOSCs will be consolidated until there are two primary NOSCs in the continental United States. The NOSCs in Europe and in the Pacific will be scaled down to small operations support centers. These two large NOSCs will be under the direct operational control of the AF NOSC at Barksdale AFB, which is the AF direct interface with STRATCOM for cyberspace activities.[33]

The next step for the AF is to build an AF wide intranet with all AF bases being a part of the logical structure (see Figure 9). All AF bases are logically re-homed into one AF network, which changes network management and security roles and responsibilities

[33] 8th Air Force (8AF). "Air Force NetOps Transformation Migration Plan." Presentation to Air Force Major Commands. 10 March 2006. (No page number)

for everyone.[34] The AF is also linking all of the AF bases together via a directory system that will allow all users to be part of one logical AF enterprise network, regardless of AOR affiliation (see figure 10).[35] This will allow all AF systems and information to be

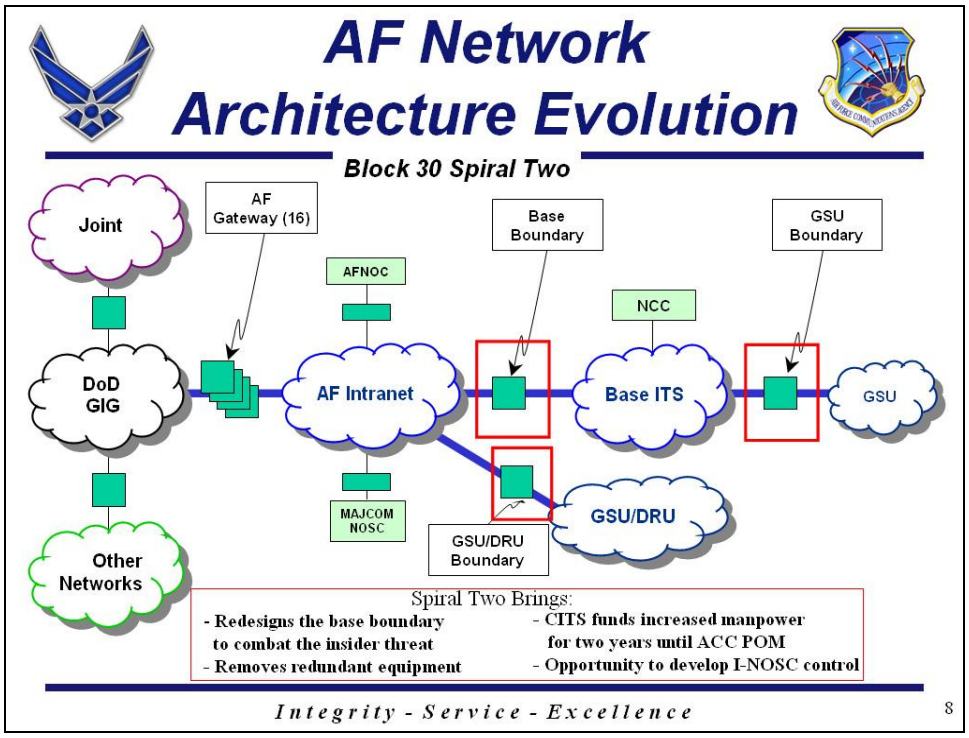


Figure 9. CITS Design For All AF Locations

available to all AF users worldwide. This begs the question, how can one COCOM in one AOR affect AF wide security? The implication of this action is that all Geographic COCOMs will have to interface with the AF NOSC for all cyberspace activities. (Ref. Figure 6, Note 1.) If a Service has one interface for all Net-D and Net-A support, does it make sense for STRATCOM to go to each of the Geographic COCOMs so they, in turn,

[34] Combat Information Transport System (CITS) Program Office. "CITS Block 30 MAJCOM AO Update." Presentation to Air Force Major Command CITS Action Officers (AO). 28 September 2006. (No page number)

[35] Air Force Communications Agency (AFCA). "Active Directory (AD) Program Management Review." Presentation to Air Force Major Commands. 17 April 2006. (No page number)

Figure 10. AF AD PMR Overview

can all go to the one AF NOSC with the same directions? Or, should STRATCOM go directly to the Service entity and inform the Geographic COCOMs of their action. The answer is: if a Service provides one point of entry for cyberspace exchanges with that Service, then the logical choice is to have STRATCOM go directly to the Service and inform the Geographic COCOMs. If any one Service chooses not to establish a single entry point, then STRATCOM must continue to work through the Geographic COCOMs when dealing with that Service. The single point of entry for a Service should be the preferred method of exchanges with all COCOMs, once consolidated.

If a Service agrees to the single point of entry, why go with the Service anyway? The reason is speed. STRATCOM's (time sensitive) primary exchanges with the Services would be for Net-D activities. Net-A activities would probably not involve all Services at the same time, and would be pre-coordinated with the Geographic COCOM

via the planning process. With Net-D, it is essential that the Services be able to respond as soon as possible. The single point of entry streamlines the DoD's ability to respond to global threats in cyberspace.

Net-A and Net-D have been discussed in detail in prior sections. But, one issue with respect to Net-D that has not been discussed yet is that it also relates to some activities in Net-O. This overlap is important to understand. If a Service establishes a unit for Net-A and Net-D activities in support of STRATCOM, then that unit must be careful to ensure that Net-M and Net-O activities imbedded within it are distinct from Net-A and Net-D activities to the point that when STRATCOM exercises OPCON over the unit, that STRATCOM does not gain direct operational control of Services activities of Net-O and Net-M. Establishing a unit where STRATCOM gains this type of authority leads back to the issue of violating Federal Law (multiple Statutes). It also leads back to the discussion of STRATCOM inadvertently becoming DoD's AOL.

Think of it this way – when CENTCOM needs a capability and the AF is tasked to provide it, the AF may respond by sending a squadron of fighters to the CENTCOM AOR. The AF also sends aircraft support personnel for planning, maintenance, fuels, etc. The aircraft maintenance squadron is there as part of the deployment in support of the deployed aircraft. The pilots, flying joint directed missions, are supporting COCOM taskings and are eligible for joint awards. They are performing a COCOM mission. The aircraft maintainers, on the other hand, are also deployed – but they are there as a support activity performing an AF mission, not a joint mission; thus, they are providing a Service mission, not a COCOM mission. And, as such, are only eligible for Service level awards, with respect to their Service mission, not joint awards. A COCOMs mission can never be

maintenance of aircraft, or maintenance of ships, or maintenance of tanks, or maintenance of networks. The COCOM should not interfere with Service level activities.

Intelligence Community's Changing Role

As the Services move more into cyberspace, the question becomes – "What is the role of the intelligence community in cyberspace?" For a long time, the Services were absent from the cyberspace arena due to it not being considered a significant warfare domain. The Services had networks and were working on advancements to military operations via IP based enhancements, but the Net-A game had rested with the intelligence organizations. The environment in DoD has changed, and intelligence's role has changed as well.

The four reasons for the intelligence communities' role change are:

1. Information and the ability to affect it are now elements of national power. (This is covered in more detail in Section 3, National Military Strategy and Cyberspace)
2. Secretary of Defense's authorization for the Air Force to move into cyberspace.
3. United States Code, Title 50.
4. Executive Order 12333, United States Intelligence Activities.

Information as an Element of National Power

The role of information has changed. And, part of this change is the separation of information from intelligence. They are now distinct, and each is now treated as its own

element of national power. It is a given that the intelligence community has purview over the intelligence element of national power. But, the intelligence community is just one user of information and information resources. Information as an element of national power is data, the systems that store and process data, and the systems and infrastructure that move the data from one location to another. The removal of information was not arbitrary. Information was removed from intelligence due to its growth as a fundamental power at the national level. The activities of managing and maintaining these capabilities in DoD are the responsibility of the Communications Directorates (the J6, A6, etc); and these same systems are also the components that make up cyberspace. Exploiting these systems is similar to ground troops exploiting information they find in a building. It is not the responsibility of intelligence troops to storm every building because intelligence may be found there. Now that information has been split from intelligence, cyberspace has moved with it – and falls squarely in the lap of the Communications Directorates (of course, with the understanding that directing Net-A and active Net-D activities are under the Operations Directorate).

Secretary of Defense and the U.S. Air Force

As cyberspace was evolving into an instrument of national power and the DoD suffered more and more cyberspace security problems – it became apparent that DoD needed a way to tie Net-A and Net-D more effectively. Net-A primarily rested with the intelligence community and Net-D rested with the Services as a support activity. At the same time there was a need to associate Net-O, Net-M and Net-CI with the Net-A and Net-D community. Thus the transformation began.

Next was the direction from President George W. Bush that brought cabinet level positions together under the Department of Homeland Security for the protection of national cyberspace assets. At that time, STRATCOM was given the role as the DoD Interface – and DoD was the only cabinet position given authority to do Net-A. When DoD moved into this high profile position and with Net-D and Net-A now seen as national cyberspace combat power – it transitioned to a Service force provided activity to the COCOMs. A supporting governmental organization or DoD agency can not maintain the nations combat power – this power rests with the Services via Federal Law.

The Army and the Navy already had cyberspace commands, so the Air Force started down the road to build their own. The Air Force went one step farther they intended to build a command around the Electromagnetic Spectrum, not just around IP based systems. Then identifying DoD level concerns, the Joint Staff started working to redefine cyberspace operational and organizational constructs. In originally starting this action, the President basically moved cyberspace from the intelligence community to the Services as the provider of combat power. By becoming an element of national power, it was moving in this direction anyway (see Section 3).

United States Code, Title 50

The position of the intelligence community has been that the cyberspace issue is a Title 10 vs. Title 50 issue – and that cyberspace is a Title 50 venue. At first, I felt this argument was overcome by events because the discussion in the two paragraphs above would negate any Title 50 position. The President and Secretary of Defense have the authority to define combat power that is an extension of the elements of national power,

and this is what they did. After reviewing Title 50, Chapters 1 through 42 – I found no provisions or text that placed cyberspace in the realm of intelligence.[36] This does not mean that the National Security Agency does not maintain their role in cyber security or their own role in Net-A for intelligence purposes, it just means the cyberspace as a combat domain now falls under one of the Services, with cyberwarfare activities executed under the direction and authority of STRATCOM.

Executive Order 12333, United States Intelligence Activities

This executive order outlines each governmental organization's roles and responsibilities with respect to intelligence. This order places signals intelligence under the National Security Agency (NSA). The order does not state any intelligence relationship to cyberspace, nor does it state that cyberspace is a component of signals intelligence. So, it could be interpreted that cyberspace is a signals intelligence activity – and as such would fall under the NSA. But, the order also states in paragraph 1.12.b.1 that no other organization shall engage in signals intelligence activities unless otherwise directed by the Secretary of Defense.[37] And, since the Secretary of Defense (and the President) has directed DoD to address cyberspace warfare, this direction would negate any position that cyberspace is a component of signals intelligence for cyber operations. Cyberspace is now a Warfighting domain with the Services providing forces to the COCOMs.

---

[36] United States Congress. United States Code, Title 50 – War And National Defense. (No page number)
[37] Reagan, Ronald. President of the United States. *Executive Order 12333: United States Intelligence Activities.* Federal Register 8 December 1981, Federal Registry Page 46 FR 59941. 4 December 1981. (No page number)

III. National Military Strategy and Cyberspace

Diplomacy, Information, Military and Economic (DIME)

For a long time I debated how to include this section of the paper. My concern was that I may distract the reader from the incremental concept building I have been attempting to accomplish up to this point. I eventually decided it would be best to explain the strategy linkage at the concept level; because, it is important for the reader to understand that military power is a tool of national strategy, and that military power is linked to diplomacy, economics and information. And, most of all, this section is essential in demonstrating the linkage between strategy and military action. These links also require interagency integration and affect many aspects of military planning and philosophy.

After trying to come up with a brief explanation of DIME, I decided to use an example from the web site named Strategy Page, and their story line called "The DIME Ballet". In a brief article about North Korea, it creates a mental image that is worth a thousand words. Here is a portion of the 2006 article:

> "North Korea is rattling its nuclear saber – and we're witnessing the DIME ballet as it nears the nuclear brink.
>
> The United States has pursued a 'python strategy' designed to squeeze North Korea economically, politically and diplomatically. The 'six nation' talks (Russia, South Korea, North Korea, Japan, China and the United States) serve as the stage for exercising the diplomatic, information and economic power.

Military power is explicit – North Korea with its army and its could-be nuke, South Korea with its army, the United States and, yes, Japan, with their ability to strike North Korean weapons sites.

China is absolutely central to American policy. The United States believes China is the only nation that can truly squeeze impoverished North Korea. For Example, China supplies North Korea with oil.

But, on May 10, China backed off, when Chinese foreign ministry spokesman Liu Jianchao said, 'We are not in favor of exerting pressure or imposing sanctions' on North Korea. 'We believe that such measures are not necessarily effective.'

China undermined the 'D' and 'E' in Washington's North Korea policy.

So what did the Bush administration do? On May 17, the U.S. Treasury Department began discussing China's 'over-valued currency.' Treasury reported to the U.S. Congress that 'Current Chinese policies are highly distortionary and pose a risk to China's economy, its trading partners and global economic growth.' The U.S. message was delivered in what diplomats call 'tough language,' marking a 'change in tone.' A tone change is Informational – a signal human beings understand in both finance ministries and honky-tonks.

The trade and currency issues Treasury raises are very real. A bipartisan group on Capitol Hill argues that Chinese trade and currency policy is harming their constituents.

Military security issues are intimately tied to economic issues. The Chinese know this. A North Korean nuke striking Seoul or Tokyo would instantly revalue everyone's currency.

But you can bet DIME is at work. Bush administration free-traders are not so quietly telling China that they will step back and let Congress enact trade restrictions unless China cooperates on North Korea. If China cooperates, then the U.S. administration will use political capital to fight a 'free trade versus protectionism' domestic battle."[38]

The above example does a great job of showing how one component of the DIME relationship impacts another and how each can leverage one another to achieve the desired ends. Now, the task is to show the relationship between DIME and military planning and operations.

General Peter Pace, Chairman, Joint Chiefs of Staff, explains some of the linkage between DIME and Effect Based Planning (EBP) in his Memorandum on Joint Professional Military Education:

"Effects-based planning enhances the current planning process that emphasizes the clear linkage of desired objectives to the effects within the operational environment, characterized as an integrated system-of-systems – political, military, economic, social, infrastructure, and information (PMESII) – that must be created to achieve those objectives. It further links the individual joint, combined, and interagency actions associated with the diplomatic, information,

[38] Bay, Austin, "The DIME Ballet", *Strategy Page: On Point*. 24 May 2005 http://www.strategypage.com/on_point/2005524.aspx. (No page number)

military, and economic (DIME) instruments of national power that are required to create the behavior or capabilities within those systems necessary to achieve those effects."[39]

After reading the above two passages, the reader's first inclination may be to think that to attempt true EBP seems impossible; there are just too many moving parts and too many players – especially when looking at all the activities associated with DIME. And, how do we move along the link in cyberspace between PMESII and DIME. Taking into account all of these complexities – how do we account for the cyberspace thread that may affect all the components of PMESII and DIME as well as EBP?

Answering the above question is another complete paper within itself. But, in narrowing the cyberspace discussion with respect to national military strategy issues and military targeting, I am going to cover my perspective of the relationship between DIME and EBP first, and then address their linkage with PMESII in the section below on Warden's Five Rings.[40] With respect to DIME, EBP and interagency interaction – three topics come to mind:

1. In the age of instant information, "the war of words and pictures are of greater importance over 'traditional' metrics of warfighting."[41]

[39] Pace, Peter, Chairman, Joint Chiefs of Staff. Memorandum of 2006 Joint Professional Military Education (JPME) Special Areas of Emphasis (SAEs). Pentagon, Washington DC 17 January 2006. (Page 4)
[40] Warden, John A. *Air Theory for the Twenty-first Century*. September 1995 http://www.airpower.maxwell.af.mil/airchronicles/battle/chp4.html. (No page number)
[41] Mountain Runner: Public diplomacy, unrestricted warfare, privatization of force, and civil-military relations. *Of Information Operations, DIME, and America's Ambassadors.* 29 August 2006 http://mountainrunner.us/2006/08/of_information_.html. (No page number)

2. Governmental agencies most actively employing DIME power view the global environment differently.[42] This complicates General Pace's agenda from above.

3. The concepts of "Hard Power" and "Soft Power".

In the cyberspace domain, the response to any action can unfold in real-time – which can be especially problematic when the governmental agencies exercising DIME influence do not have the same view or understanding of the environment.

A War of Words and Pictures

This concept is probably best understood when looked at via the Global War on Terrorism (GWOT). What makes terrorist organizations so resilient? Why is it that they seem to continue to get funding as well as volunteers to join their cause? Their processes have nothing to do with what's best for their followers – it is centered on promoting and selling their product – an ideology, and in gaining power for themselves. As access to technology grows, so does the capability of any individual or group to gain global recognition and support. They build their plan, build their message, then work to deliver and sell both – sure sounds similar to state level activities. What we are talking about is, terrorist organizational diplomacy using information to their economic advantage to gain recruits and military capabilities to wage their private war – this is the Terrorist DIME at work – and their primary tools are technology and cyberspace. For the terrorist, military confrontation is not just a means to an ends – it is also an activity supporting their overall

[42] Puglisi, Matthew and others. *A Common Interagency Regional Framework*. Joint Forces Staff College, Joint and Combined Warfighting School, Class 7-01, November 2006. (Page 3)

DIME objectives. For the audience the terrorists are interested in, once you remove the "M" from DIME – the terrorists appear to be winning. What's worse – without cyberspace as a tool – this would not be so – we own the "M", we need to own the rest.

Cyberspace is the terrorist safe-haven for globally executing their DIME objectives. Which leads to the question – who is more effective, the United States at killing and capturing terrorists – or the terrorists at using the internet to gain funding and recruits? If this question causes you to think for a second, as it did me – then the problem is our approach to cyberwarfare – the terrorists should not have this kind of capability – it should have been eliminated a long time ago.

Solving the problem is time consuming, but not overwhelming. The responsible COCOM Commander must think of the engagement in the terms of DIME and the environment in which the terrorist DIME is carried out. The military portion should be easy – but, at this time, the DoD is not organized to operate in cyberspace from the DIME perspective. A COCOM Commander needs the ability to interface directly with the other governmental agencies that affect DIME power. The problem is that this approach requires tight integration that does not exist today. Establishing this relationship is essential to help avoid another "9/11 Report" type of document pointing to our inability to communicate in the event of another catastrophe. Integration would further enable the military commander to achieve the desired military effect by other than kinetic means – which will lead us into our "Soft Power" discussions later in this document.

The same DIME issues hold true for our adversary. And, in this arena, some of these activities are already taking place. For example, with respect to the terrorist DIME, the Department of Treasury is working with other governments to chase down terrorist

cash flow (economic). An effective DoD cyberwarfare capability may help improve the Treasury Departments effort as well as possibly leveraging Treasury's resources to assist with DoD priorities. We have one component of DIME being affected by one governmental player, possibly without fully understanding the relationships across the full spectrum of DIME power. As General Pace stated above, we are addressing a system of systems, lone activities without understanding all aspects of our actions may have effects not understood for years to come, if ever. We are making progress, but not the progress we could be making with a tighter coupling of Soft Power activities.

The military is often recognized as the last resort of national power. In cyberspace, that is no longer true – the military can take action, short of killing people or destroying things. This arena is ripe for the development of the right application of force; this force in cyberspace must be capable of exercising varying capabilities in affecting the DIME activities of our adversaries as well as support our national DIME concerns as directed by the National Command Authority. General Pace referred to the relationship DIME builds across agencies as a system of systems; DoD is only one component of this system and has to support this relationship in order to be effective in the cyberspace domain, or the system can fail.

Differing Global Views

> *"The most urgent task of our government is getting interagency coordination & cooperation right. The interagency process was largely a failure prior to September 11, 2001, but has only marginally improved since that time in effecting successful planning and action for accomplishing specific U.S. policy objectives overseas."*
>
> *-- Ambassador William Bellamy, Senior VP, National Defense University*

Figure 11. Ambassador William Bellamy[43]

Government organizations that have DIME influence must find a way to share information to ensure that DIME power is seen as a single voice. As the previous section pointed out and the above quote states, interagency processes are not as seamless as they could be. One of the reasons for this is the way that each organization sees the globe – basically, through their "window on the world". Specific organizations have divided the globe into regions based upon their operational requirements. Operations within various governmental organizations are not based upon the same activities or needs – thus, there are bound to be differences.

The three primary players in this discussion are the DoD, the Department of State (DoS) and the Central Intelligence Agency (CIA). Each represents a component of DIME; DoD for military, DoS for diplomatic and CIA for information (CIA's role has now changed to intelligence – which is explained later). Their three different global boundaries complicate the flow of information to and from the correct parties within the different organizations.[44] The primary concern is how each views the globe, and thus

[43] Puglisi, Matthew and others. (Page 2)
[44] Puglisi, Matthew and others. (Page 3)

divides the globe geographically based upon their sub-departments (a geographic subdivision is known as an Area of Responsibility (AOR)). For a quick comparison:

1. DoD's geographic division is into five AORs (Figure 3).
2. DoS's geographic division is into seven AORs, with only a minor resemblance to DoD AORs (Figure 12).
3. CIA's geographic division is into three AORs, which is not similar to DoD's or DoS's AORs (Figure 13).

The forces that have shaped the geographic AORs are linked to history, perceived organization mission requirements, cultural boundaries, political boundaries and religious boundaries. But, as with DoD, the AORs change as the need arises or mission dictates. Each organization also has unique entities within each AOR, so the subdivisions are not similar in nature either. As long as these three organizations continue to work within differing boundaries; the possibility of loss of information due to convoluted process threads is excessive – again, this is what we have been trying to avoid since 9/11.

An analogy to bring this into perspective would be, if each state in the United States to divide up their court systems differently. Some states only have county courts; others have district courts (not based upon counties); others only have state level courts; others allow their townships to have courts; while still others allow local communities to establish courts even if not incorporated into a township; and lastly some allow mixtures of variations of all of the above. To get information to the right person in another state – you need a map, as well as an organizational directory explaining who and where your counterparts are in the other organizations. And, lest we forget, since we are in government organizations – we will reorganize every two or three years.

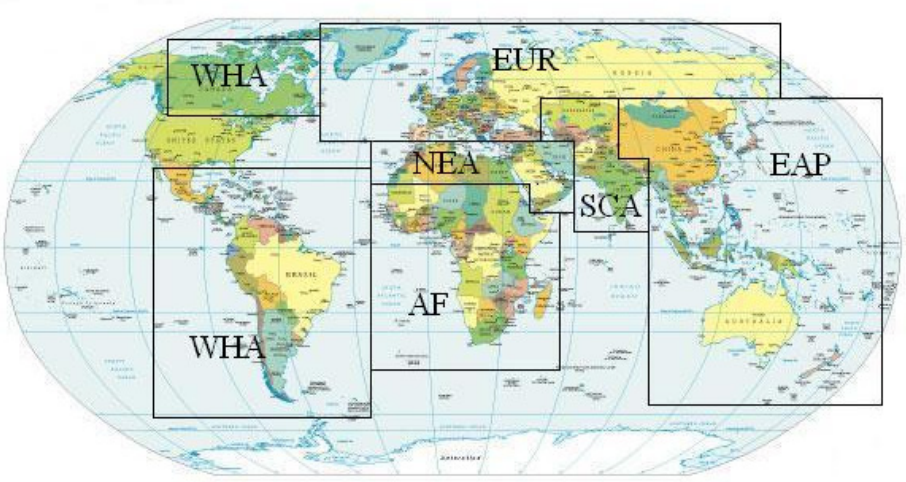


Figure 12. Department of State Regional Offices [45]

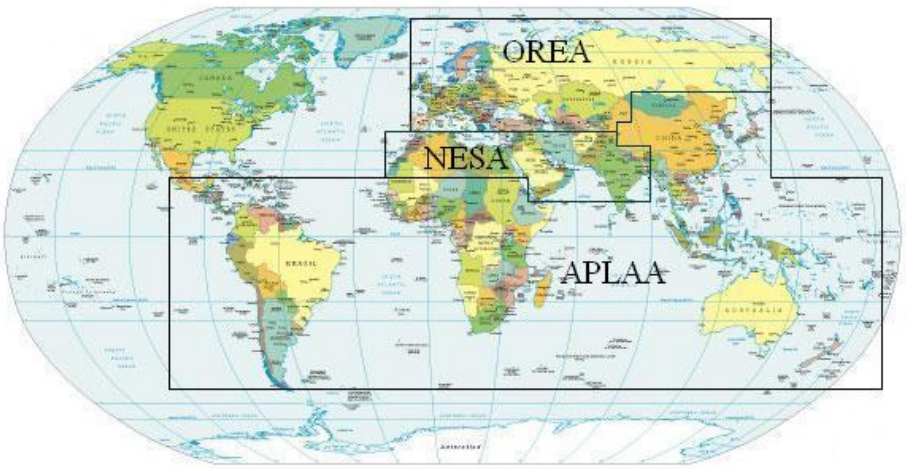


Figure 13. CIA Regional Offices [46]

If it is not realistic to align these organizations in a manner to facilitate information flow, then the next best approach is to build a detailed plan explaining the

[45] Puglisi, Matthew and others. (Page 4)
[46] Puglisi, Matthew and others. (Page 5)

information processes, the coordination processes and the critical information threads. This may not have been an issue before the onset of cyberwarfare; but, if it has not become an issue already, it will become one very soon. Engagements in cyberspace will be rapid and require the immediate sharing of information across organizations. Some of the information sharing is already being fostered with the help of the Department of Homeland Security (primarily for homeland defense – we will discuss this more in the next section). But, it is not to the degree required in a cyberwarfare military conflict where the DoD must defend itself and respond in kind as needed. Seamless integration sometimes means that the differing organizations must, at some level, look at the problem from the same perspective; basically, look at the problem from the other organizations "window on the world".

Hard and Soft Power

Hard and Soft Power is nothing new, but it is getting more emphasis lately due to cyberspace. The ability of Soft Power to be covert and immediate is bringing the concept to the forefront of cyberpower discussions. Soft Power has reemerged to the point that it is being taught at institutions such as West Point – the reason being, it is an often misunderstood and overlooked form of military power.

Hard Power is something we are familiar with; it is military force, economic sanctions, trade restrictions, tactical diplomacy, etc. Philip Taylor, from the University of Leeds in the United Kingdom, stated in his presentation titled Concepts of Information Warfare – "Hard power is the ability to get others to do what they otherwise would not do

through threats or rewards. Whether by economic carrots or military sticks, the ability to coax or coerce has long been the central element of power".[47]

Soft Power is the diplomatic "Nirvana" that Nations want to reach. It achieves the end goal without the use of Hard Power. Phillip Taylor's presentation states – "Soft Power is the ability to get desired outcomes because others want what you want. It is the ability to achieve goals through attraction rather than coercion. It works by convincing others to follow or getting them to agree to norms and institutions that produce the desired behavior."[48]

Cyberspace delivers Soft Power more effectively than any other military capability. For example, to just name a few, it gives a commander the ability to do the following:

1. Diplomacy:
    a. Affect diplomatic/organizational decisions by inciting disharmony among adversaries
    b. Negotiate from within the other nation's information stream
    c. Insertion of diplomatic options into the other nation's information stream
    d. Deny the adversary information that may affect their choices in a manner not in line with our intentions
2. Information:

[47] Taylor, Philip M. (No page number)
[48] Taylor, Philip M. (No page number)

a. Inject disinformation by creating cloned terrorist web sites and chat rooms
b. Cyber-Herding (See section 4)
c. Modify adversary information streams to plant/deny information
d. Deny access to information resources

3. Military:
    a. Influence Command and Control
    b. Tailor intelligence
    c. Affect the ability of an Integrated Air Defense Systems to function correctly
    d. Modify military email streams to limit unwanted information flow
    e. Retarget the organization's recruitment
    f. Affect the supply chain
4. Economic:
    a. Impact the ability to raise funds
    b. Arrange for raw materials to be unavailable
    c. Collect donations from terrorist supporters
    d. Disrupt terrorist supporters cash flow

With respect to these activities, they all must be executed covertly. The full list is extensive, and can continue to grow the more creative you are. It gives the organization that uses a Soft Power approach in cyberspace the ability to very effectively target an adversary's information threads. Covert Soft Power is at the heart of cyberspace DIME, and exercising DIME components in cyberspace avoids implementing Hard Power

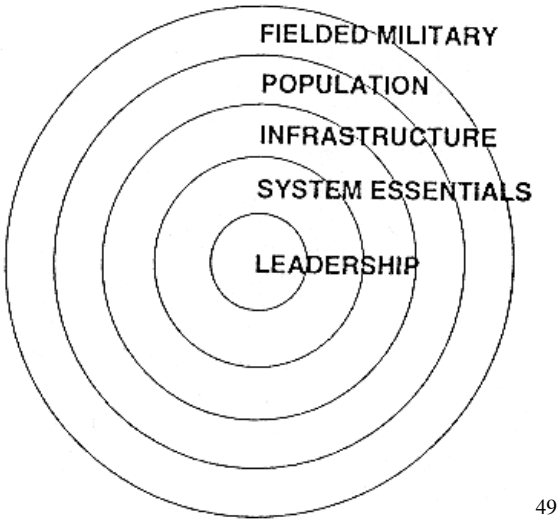
choices. The best part is, if the operation is successful at being covert, the target audience may support your position without knowing their decision making processes were influenced and/or compromised. This is *influence operations via information dominance*, and will be one of the key military powers of nation states in the future, thus it must a primary component in our military cyberspace operations today.

The effectiveness of Soft Power is proportional to the cohesiveness of the target. Nation States that have a robust communications and information infrastructure will have to have narrow targets with specific objectives. Terrorist targets are less cohesive, and thus more vulnerable due to the variation in information threads within the organizations and to the general public – all of which are vulnerable. Terrorists and Nation States are targets; we just have to tailor our approaches based upon our adversary and the desired effect.

Wardens Five Rings – A Cyberspace Perspective

The Current Five Rings

If you have ever attended any Air Force sponsored Professional Military Education (PME), you have heard of Col Warden's Five Rings. Basically, Col Warden divided the adversary into five systems, Fielded Military, Population, Infrastructure, System Essentials and Leadership.



[49]

Figure 14. Colonel Wardens Centers of Gravity

Each of these systems are called centers of gravity, that can best be explained as target groupings that impact national power and national will. By targeting the centers of gravity, you gain the desired effect you are looking for. The original concept implied that, for example, that fielded forces may not have to be engaged if you were able to convince the adversary to quit via eliminating leadership or system essentials. The debates continue with respect to how the "rings" should be viewed, and whether the approach should be from the outside in, or the inside out[50] I consider the debates useful for determining how best to use the process, which will ultimately add to its effectiveness as a concept for developing a campaign plan, situationally dependent of course. The question is – what adjustments need to be made when we add the cyberspace domain into the mix?

---

[49] Warden, John A. (No page number)
[50] Smith, Russell J. "Developing an Air Campaign Strategy," *Air & Space Power Journal*. 23 November 1999 http://www.airpower.maxwell.af.mil/airchronicles/cc/smith.html. (No page number)

The Seven Rings of Combat Power

> *"The first priority, the best way to defeat an adversary, Sun Tzu tells us, is to defeat an adversary's strategy. Air campaigners do not appear to be strategists."*
>
> *-- Colonel Richard Szafranski*

Figure 15. Colonel Richard Szafranski[51]

Col Szafranski's comments have not withstood the test of time. Strategy is no longer a quantity that only Army and Naval officers bring to the engagement.

Col Warden tried to quell his skeptics, and continued to refine his concept. He later produced a target class version to show how his approach could be used against differing target types (Figure 16). But, all the while missing the key points of how the environment was changing. The reason why so many individuals felt it necessary to examine, dissect and write about his process was that everyone understood that something was missing, everything just did not fit as cleanly as it should – and the missing components were not as obvious as they could have been, until recently.

Roll back to the previous section for a moment. Once the military component of DIME is engaged, it is acting as the nation's diplomatic power. Military force is often referred to as the last act of diplomacy, thus once engaged is a part of the diplomatic act. This leaves the "I" and the "E" of the DIME equation. Let's take each one individually. (This did not mean that other diplomatic activities are not underway, just that the military action is the predominant diplomatic activity when engaged.)

[51] Smith, Russell J. (No page number)

	Body	State	Drug Cartel	Electric Company
Leader	Brain -eyes -nerves	Government -communication -security	Leader -communication -security	Central Control
Organic Essential	Food/oxygen -conversion via vital organs	Energy (electricity, oil, food), money	Coca source plus conversion	Input (heat, hydro) Output (electricity)
Infrastructure	Vessels, bones muscles	Roads, airfields, factories	Roads, airways sea lanes	Transmission lines
Population	Cells	People	Growers, distributors, processors	Workers
Fighting Mechanism	Leukocytes	Military, police, firemen	Street soldiers	Repairmen

[52]

Figure 16. Warden's Five Centers of Gravity by Target Class

Col Warden refers to lines of communication under the leadership center of gravity. These are the traditional communications systems – the ability to make a phone call or make a radio contact. There is nothing that targets the information thread for cyberspace. Thus, entire target sets that may be critical to the campaign may not be valued for their true contribution to the engagement. The full use of cyberspace domain means that we should be able to use cyberspace to affect land, sea and air – as well as using land, sea and air to affect cyberspace. The rings concept was ahead of the introduction of the cyberwarfare domain, but that does not mean that Col Warden didn't recognize this. He referenced Don Simmons' book Hyperion, when he said "Information will become a prominent, if not predominant, part of war to the extent that whole wars may well revolve around seizing or manipulating the enemy's datasphere".[53] The

[52] Warden, John A. (No page number)
[53] Warden, John A. (No page number)

storage, movement, control and flow of information are the tools of the information warrior in cyberspace.

Economics in cyberspace refers to the ability to affect an organization's trade and financial well being. This one should be apparent, since most significant transactions today are via an electronic means. The ability to disrupt these transactions just requires insertion into or the breaking of the information stream. This leads to one of the shortfalls of the original rings concept; which is the absence of targeting financial institutions as a key specific center of gravity – which is something I never understood. A nation runs on its economy and its ability to buy goods, supplies, and feed its people. We would want to limit their means to barter before we eliminate the organic essentials, especially in support of the rebuilding process. If the population loses its ability to engage in fair trade, or access to its monetary resources – how long can the nation state last? The point here is that stock markets, commodity markets, currency mints, treasuries and banks should be targets in an effort to affect the adversaries will to fight – whether the attack is kinetic or non-kinetic. We currently use a form of an "attack" against financial organizations that control funds for terrorist organizations – we confiscate the funds or freeze the accounts. This is a form of applying financial economics as a center of gravity, and these types of process should be accounted for in the rings concept.

The updated rings concept "The Seven Rings of Combat Power" are below in Figure 17. The final product is similar to the original, the only differences are that the Information Systems and Financial Organizations centers of Gravity are inserted between the Leadership and System Essentials positions. The definitions, with a few examples are:

1. Information Systems (Electronic and Traditional):
    a. Data Storage and Processing Facilities (Government and Commercial)
    b. IP based communication nodes – for example: Tier 1 and Tier 2 facilities and IP based lines of communication (trunk lines, microwave, satellite, etc).
    c. IP based telephones and supporting systems
    d. Government and Public records (paper or binary) – for example: Birth Records, Property Deeds, Marriage Records, Tax Records, etc.
2. Financial Organizations:
    a. Any type of facility or entity that controls the collection of currency, stores currency or produces currency – for example: Banks, Mints, Treasuries or Foreign Exchanges.
    b. Any type of financial market – for example Stock Markets or Commodities Markets.
    c. Market Regulatory Organizations – similar to our Security and Exchange Commission.

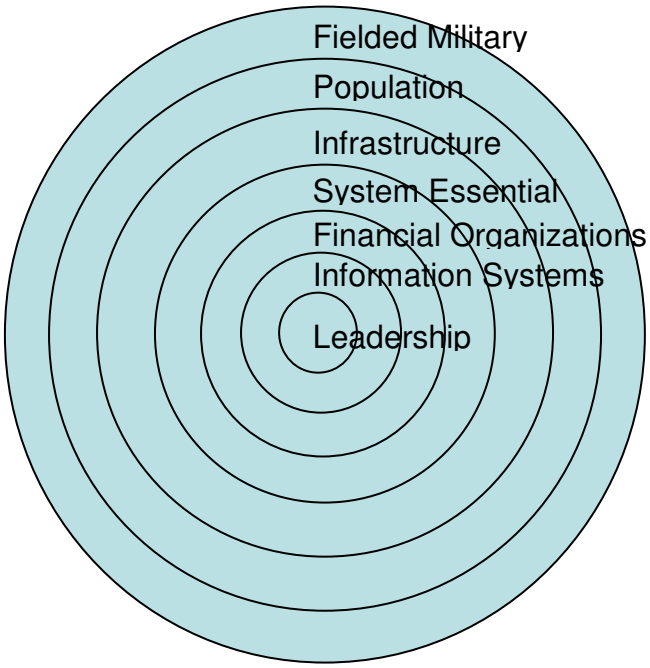


Figure 17. The Seven Rings of Combat Power

These two additions (Information Systems and Financial Organizations) help segment the centers of gravity in a way that makes it easier to see the contributions that cyberwarfare brings to the fight via the new elements of national power, which is discussed next.

DIME Plus Intelligence, Legal and Finance (MIDLIFE)

MIDLIFE, the New DIME

President Kennedy addressed the importance of understanding the use and relationships between the components of national power (DIME):

"You must know something about strategy and tactics and logistics, but also economics and politics and diplomacy and history. You must know everything you can know about military power, and you must also understand the limits of military power. You must understand that few of the important problems of our time have, in the final analysis, been finally solved by military power alone."[54]

As the elements of national power have transformed with technology, it has become increasingly impossible to define the changes in the context of the original DIME construct. What has emerged is an updated DIME construct, adding in Finance, Intelligence and Legal; thus creating the new acronym MIDLIFE.[55]

Finance was extracted from the Economic component due to its independent ability to represent significant power in the global community. The Finance element, by itself, has the ability to affect a nation's or an organization's ability to pursue activities that are contrary to our national interests. The Information element included Intelligence, and caused many questions about its true link to national power. Was all information subjugated under Intelligence or was Intelligence a subcomponent of Information. This is now clear. Information is all information, electronic and traditional, regardless of what the information is to be used for. Intelligence is an activity that uses information to find actionable components, support planning, persuade friends, dissuade adversaries, etc. Intelligence is a service – Information is data and its supporting infrastructure.

---

[54] Sellin, Lawrence, Ph.D. "Outside View: Short-changing Iraq," *Spacewar: Your World at War.* Washington (UPI) 18 December 2006 http://www.spacewar.com/reports/outside_view_short-changing_iraq_999.html. (No page number)

[55] Forest, James J.F., Ph.D. "Teaching Counterterrorism in the 21st Century," Presentation facility and students, United States Military Academy, Combating Terrorism Center, West Point. July 2005. (No page number)

The new granularity provided by MIDLIFE makes it easier to identify responsible governmental organizations as well as the activities associated with each. What helps to make it attractive is that it grew out of the DIME construct, supported by individuals working in governmental organizations that exercise DIME power. This new granularity also fits together well with the Seven Rings of Combat Power.

MIDLIFE and the Seven Rings of Combat Power

National level coordination is not anything new – Joint Publication 1 states: "The Armed Forces are responsible for conducting defensive and offensive information operations, protecting what should not be disclosed, and aggressively attacking adversary information systems. Information operations may involve complex legal and policy issues that require approval, review, and coordination at the national level."[56]

This leads back to the discussion we have been having through the third section of this paper, interagency coordination is not an option – it is a necessity. And, in executing this coordination – national and military strategy must be at the heart of the effort. "An individual must analyze the National Strategy for Combating Terrorism from a MIDLIFE perspective, noting that effective counter terrorism requires integration of all dimensions".[57] What Dr. Forest says with respect to terrorism applies equally to any adversary; I go back to General Pace's comments – DIME and its relationship to National Strategy and the impact that both have on effects based planning must be taught as part of

[56] Joint Chiefs of Staff (JCS). *Joint Publication 1, Joint Warfare of the Armed Forces of the United States.* 14 November 2000. Page I-7
[57] Forest, James J.F., Ph.D. (No page number)

Joint PME. What is so important about his document – is that he understands the significance of these relationships, and he is in a position to make sure others are taught the significance also.

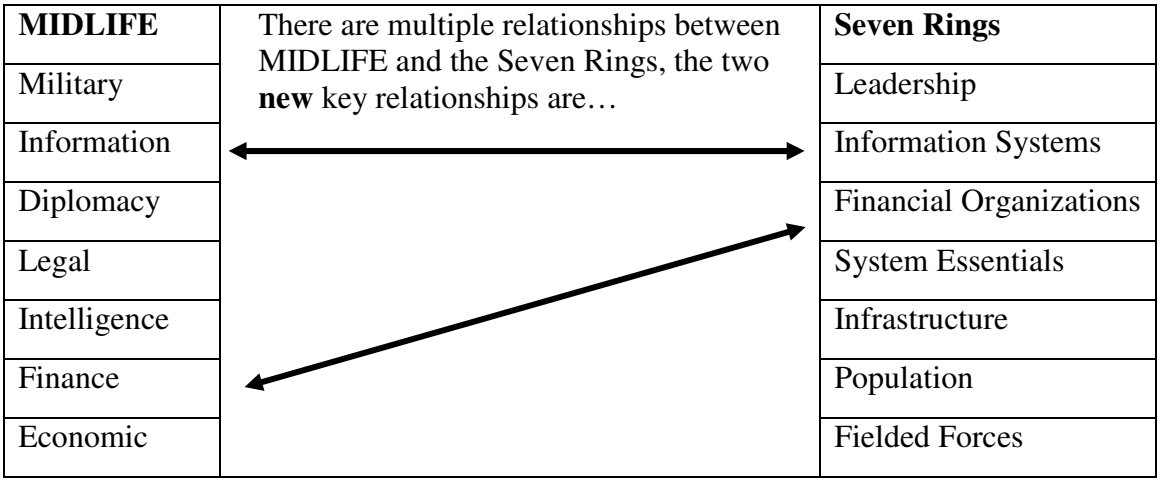


Figure 18. MIDLIFE and the Seven Rings Similarities

The parallels between MIDLIFE and the Seven Rings are not a coincidence. The key elements of Finance and Information have become important enough for them to be recognized as individual elements of national power – which is the basis for formulating our effects based planning (as General Pace stated above) – how can they not be singled out as elements of combat power. Relating elements of combat power to elements of national power facilitates effects based planning that can be directly linked to our national strategy, as a COCOM commander – what more could you ask for.

Taking all of this one step further; cyberspace is prevalent in all the MIDLIFE elements of power, but especially in information and its seven rings counterpart, information systems. This identifies a direct tie between cyberspace and MIDLIFE, which then implies that cyberspace must be a part of effects based planning if we are to

take the MIDLIFE perspective. And we must take a systems perspective, at least that is the view of Dr. Forest, General Pace and President Kennedy – as noted above and in the previous sections. Recently, even the Secretary of the Air Force stated; "[future technologies]… assume that we have cyberspace dominance, making cyberspace a center of gravity to protect and defend".[58] It then becomes easy to draw a line from cyberspace to our national strategy. Cyberspace has arrived, and is now an element of national power and a center of gravity.

[58] Wynne, Michael W., Secretary of the Air Force. "Cyberspace Dominance, the information Mosaic and Precision Strike." Address to the Precision Strike Association, John Hopkins University, Baltimore MD. 19 October 2006. (No page number)

IV. Military Freedom of Response

Before moving too much farther, it would be best to put a framework in place that communicates a view that I have been using to evaluate differing cyberspace concepts. So, here are my: "Cyberspace Truths";

A. Cyberspace is not unlimited; It has boundaries.

B. Every node operates for its own purpose/reason.

C. Architecture is extremely dynamic.

D. Response times must be immediate.

E. Adversarial capabilities lead increases in security.

The above statements are nothing new if you have had experience building large networks, operating large networks or had to defend enterprise networks. I included the Cyberspace Truths, because not everyone has the same level of experience – and it will help in explaining some of the concepts further in this paper.

The military's future with respect to cyberwarfare has been a topic of many papers and research studies. One paper in particular, from the RAND Corporation stated the following:

> "Cyberwarfare may also imply developing new doctrines about the kinds of forces needed, where and how to deploy them, and what and how to strike on the enemy's side. How and where to position what kinds of computers and related sensors, networks, databases, and so forth, may become as important as the question once was for the deployment of bombers and their support functions.

Cyberwar may also have implications for integrating the political and psychological with the military aspects of warfare.

In sum, cyberwar may raise broad issues of military organization and doctrine, as well as strategy, tactics, and weapons design. It may be applicable in low- and high-intensity conflicts, in conventional and non-conventional environments, and for defensive or offensive purposes."[59]

What's very interesting about this particular paper is that they predicted in 1993 the environment we are just now questioning today. After 14 years, we still don't have a complete grasp of the situation; but, we have started to take steps in the right direction.

Past Responses

The USS Cole, Embassy Bombings and September 11

How do we respond to events today? If another nation state were to attack the U.S. as Japan did in 1941, the response would be to go to war. If a non-state organization attacks the U.S. government or its people – our first response is to treat it as a criminal act. When the USS Cole was bombed, one of the first things we saw on CNN was the FBI showing up to start the investigation; the same was true for our Embassy bombings in Africa. The first response to 9/11 was also the legal authorities – the military was used to fill the gaps in capabilities of the legal establishment. If the event is deemed a civil

[59] Arguilla, John and David Ronfeldt. Rand Corporation, International Policy Department. "Cyberwar is coming." 1993 http://gopher.well.sf.us:70/0/Military/cyberwar.

matter – the military assists when and where needed because the events are seen as crimes; and not a military defense issue.

We have the same approach to cyberspace, the National Strategy to Secure Cyberspace says;

> "Many cyber-based attacks are crimes. As a result the Justice Department's Computer Crime and Intellectual Property Section, the FBI's Cyber Division, and the U.S. Secret Service all play a central role in apprehending and swiftly bringing to justice the responsible individuals. When incidents do occur, a rapid response can stem the tide of an ongoing attack and lessen the harm that is ultimately caused. The Nation currently has laws and mechanisms to ensure quick responses to large incidents. Ideally, an investigation, arrest, and prosecution of the perpetrators, or a diplomatic or military response in the case of a state-sponsored action, will follow such an incident."[60]

This approach treats cyber events in a very similar manner as non-cyber events. The approach is understandable, but problematic. The time it takes to determine the origin of the adversary, whether it was terrorists or a nation state, and how to stop the event; could be a lot longer than the time we have to prevent a serious event from unfolding.

Just as during 9/11, the military had the resources that the civil authorities did not have due to differing missions – the same is true for cyberspace. The military must be the premier cyberspace capability, that when needed can assist the legal authorities as required. The military may even see requirements to be part of the "First Responders" in

[60] Department of Homeland Security (DHS). *The National Strategy To Secure Cyberspace*. February 2003. Page 28

future critical cyberspace events. These capabilities must be built on the premise of protecting the military's ability to conduct cyberspace operations (defensive or offensive) at the discretion of the appropriate authority.

How does the DoD protect the entire American cyberspace domain in the same manner that they currently protect the U.S. against nation states? Based upon the technology of today, the problem space is too large for one organization. The Department of Homeland (DHS), the organization tasked with cyberspace homeland defense[61] agrees, and has adopted the approach of in depth multithreaded defense based upon the national activities aligned under the applicable cabinet positions (more on this shortly). Their approach divides the problem space into manageable portions based upon the knowledgebase of like activities – one of the biggest problems is they left out the American populace – who defends them?

Cyberspace Events

A property of cyberspace events is that they can take place very quickly, and affect very large numbers of people (and systems). And, due to this speed and breadth, these events are highly visible. For this reason alone, would-be attention-getters find it an easy way to make a statement. And, the bigger these events get, the more our potential adversaries pay attention to them, and the further our adversaries move into the cyberwarfare domain. For example, look at China – the web is filled with articles talking about Chinese hackers attacking government systems. One unofficial hacker

[61] Bush, George W. President of the United States. *Critical Infrastructure Identification, Prioritization, and Protection.* Homeland Security Presidential Directive-7. 17 December 2003. (No page number)

organization in China is called the "Honker Union", whose members are called Honkers, have built a package called "KillUSA" for their members to help them with their cyberattacks against U.S. systems.[62] And, not all of the Chinese attacks are ad-hoc; Chinese spies in the U.S. have been gathering information that would help with future cyberattacks from China.[63] So, what does this mean? Well, there are literally millions of would-be hackers – as they learn to breach systems and inflict damage – our adversaries are watching and learning. The question is, how much cyber intelligence can an organization/nation gain if they exploit the activities of the millions of hackers on the internet today? The even better question is – when will they put that intelligence to good use?

Many organizations think of cyberspace attacks from the perspective of what they see the most – viruses, Trojan horses, root kits, worms, etc. These types of malware do cause a lot of problems, and can cost organizations literally thousands of dollars in lost production and clean up time. The NIMDA virus alone, infected 86,000 computers and went from nonexistent to nation-wide in one hour.[64] It attracted a lot of attention, for its wide spread affects – but it should have attracted even more attention for its technical sophistication. "It demonstrated that the arsenal of weapons available to organized attackers now contains the capability to learn and adapt to its local environment. NIMDA was an automated cyber attack, a blend of a computer worm and a computer virus. It propagated across the Nation with enormous speed and tried several different

---

[62] Delio, Michelle. "It's (Cyber) War: China vs. U.S.," *Wired News*. 30 April 2001 http://www.wired.com/news/politics/0,43437-1.html?tw=wn_story_page_next1.
[63] Dunnigan, James. "China in a Cyberwar Arms Race," Strategy Page :Dirty Little Secrets. 8 March 2005 http://www.strategypage.com/dls/articles/2005389.asp.
[64] Department of Homeland Security (DHS). *The National Strategy To Secure Cyberspace*. February 2003. (Page 5)

ways to infect computer systems it invaded until it gained access and destroyed files."[65] This type of malware should have us concerned – it was the blending of multiple cyber weapons into a single package, and we should expect more of these advanced malware products in the future. This type of virus scenario is what we normally hear about; it is what ends up on CNN and in news magazines. But then we have the other end of the spectrum, and on many occasions low-tech attacks can be just as lethal to operations.

As we think we advance in technology, there is always someone who can dedicate only a few minutes to show us that we are not as prepared as we thought. One of these techniques that flowed around the internet a few years ago was the simple "One Email" denial of service (DOS) attack. Email systems, or their email filtering firewalls, would examine the inbound email traffic to validate that the recipient existed at that site and would send a rejection notice back to the sender if there was an issue. A version of the low-tech attack would be to send an email to your site with a TO: address of john.doe@anyAFB.af.mil with a FROM: address of john.doe@anyAFB.af.mil. When your system validates that the user is not at your site – based upon the FROM: address, where do you send the rejection; you send it back to your site – and of course the rejection is sent to that same non-existent individual – so you reject the rejection, and so on, and so on until your system becomes overloaded and fails.

The first solution to this problem was to make sure you do not reject to yourself; because, you should never have to since your filter is examining email coming from the internet. So, the low-tech adversary simply changes the FROM: address to read

[65] Department of Homeland Security (DHS). *The National Strategy To Secure Cyberspace*. February 2003. (Page 5)

john.doe@anyAFB2.af.mil – so the two sites send rejections to each other, back and forth, and so on and so on, and both sites eventually fail. Of course – now you stop your system from rejecting rejections – and all is good until the adversary wants you to come down again. With this kind of attack, you will continually chase your tail – there are more ways to perform an email DOS attack than we currently have solutions for. The point is – we can keep the ship afloat, but it will be taking on a lot of water.

The above few paragraphs were not an attempt to turn someone into a cyberspace specialist. It was supposed to communicate two very important concepts; once an incident (virus, Trojan, etc) starts, its impact can be immediate (nation-wide infection within one hour); and, we can spend a lot of money building our cyberspace "Maginot Line" around our systems – but it will be the five cent effort that will eat up most of our time and distract us from the adversary's primary goal; and, due to their low-cost – these low-tech attacks can barrage us in the thousands.

This is not even the worst part; currently in an effort to control infrastructure spending and to keep from building duplicate infrastructures on our bases for unclassified traffic and classified traffic – we encrypt our classified data (at the secret and top secret levels) and transmit it over our unclassified networks. This is common knowledge, not treated as classified information and discussed openly at meetings and via internet emails – we have to assume our adversaries know this. For example, with the Top Secret network configuration, a port is opened on the firewall so this encrypted traffic can pass through – what would happen to this traffic if an adversary were to keep the firewall so busy that it could not service the traffic in the encrypted tunnel?

Usually the encrypted tunnel is a point to point connection with static IPs (internet addresses), what if the adversary determines the static IP address of the encryption devices – and keeps them busy with DOS traffic that supposedly originated from the correctly mated IP address (IP spoofing). These encrypted tunnels are susceptible to the same denial of service attacks that can cripple other internet systems. There are many ways to deny or limit the ability of the encrypted packets to get from point to point. If this were to take place, what happens to the essential information needed for real time, real world mission execution? The Secretary of the Air Force refers to cyberspace providing this "Information Mosaic" that enables our warfighters by bringing together the elements of the information needed at the right time…so much for the mosaic if our encrypted tunnels are down.[66]

The Next Response

The terrorist as an enemy:

> "The Internet provides an inexpensive, anonymous, geographically unbounded, and largely unregulated virtual haven for terrorists. Our enemies use the Internet to develop and disseminate propaganda, recruit new members, raise and transfer funds, train members on weapons use and tactics, and plan operations. Terrorist organizations can use virtual safehavens based anywhere in the world, regardless of where their members or operatives are located. Use of

[66] Wynne, Michael W. (No page number)

the Internet, however, creates opportunities for us to exploit. To counter terrorist use of the Internet as a virtual sanctuary, we will discredit terrorist propaganda by promoting truthful and peaceful messages. We will seek ultimately to deny the Internet to the terrorists as an effective safehaven for their propaganda, proselytizing, recruitment, fund-raising, training, and operational planning."[67]

The nations state as the enemy:

"In peacetime America's enemies will conduct espionage against our government, university research centers, and private companies. Activities would likely include mapping U.S. information systems, identifying key targets, lacing our infrastructure with "back doors" and other means of access. In wartime or crisis, adversaries may seek to intimidate by attacking critical infrastructures and key economic functions or eroding public confidence in information systems. They may also attempt to slow the U.S. military response by disrupting systems of the Department of Defense (DoD), the Intelligence Community, and other government organizations as well as critical infrastructures."[68]

The approach we are taking against terrorism is the same approach we should take against all adversaries – deny them any capability that could prove harmful to our objectives in and out of cyberspace.

Civil Authorities

[67] "The National Strategy For Combating Terrorism." September 2006. Page 17

[68] Department of Homeland Security (DHS). *The National Strategy To Secure Cyberspace*. February 2003. (Page 49-50)

In January 2001, President George W. Bush directed a review of governmental information systems and cybersecurity. Once that review was completed, the President issued Executive Order 13231 establishing a program to protect information infrastructure and systems. This Executive Order along with the Federal Information Security Act formed the foundation for Presidentially directed cyberspace security activities.[69] The President followed this up, in October 2001, by establishing the National Infrastructure Advisory Council (NIAC) via Executive Order 13385. The purpose of the NIAC is to advise the President on security issues with respect to "critical infrastructure sectors and their information systems."[70]

With the stand-up of the Department of Homeland Security (DHS) after 9/11, these cyberspace activities found a home. The DHS was tasked with protecting both portions of the "Homeland"; the physical and the cyber. This established a new critical infrastructure chain of command; it placed the Secretary of Homeland Security between the President and the NIAC. Basically, all NIAC recommendations now flow through the DHS Secretary's office.

The DHS produced the "National Strategy To Secure Cyberspace"; and, it basically reads like a cook book and is very thorough. The key points in this document are:

---

[69] Department of Homeland Security (DHS). *The National Strategy To Secure Cyberspace*. February 2003. (Page 14)

[70] Bush, George W. President of the United States. *Executive Order 13385: Continuance of Certain Federal Advisory Committees and Amendments to and Revocation of Other Executive Orders.* Federal Register 4 October 2005, Volume 70, Number 191, Presidential Documents, Pages 57987-57991. 29 September 2005. (Section 5)

1. It ***links physical security with cybersecurity – Issue of Presidential interest***[71]
2. It ties directly to the National Strategy for Combating Terrorism, the National Infrastructure Protection Plan and the National Response Plan.
3. It identifies cyberspace security as a societal issue at all levels; federal, state and local governments, private industry and the populace.
4. It identifies the critical key sectors (public and private) that rely upon cyberspace as:

Information and Telecommunications	Agriculture	Food
Chemicals and Hazardous Materials	Government	Water
Banking and Finance	Energy	Public Health
Defense Industrial Base	Transportation	Emergency Services
Postal and Shipping		

Figure 19. Critical Key Sectors (Public and Private)[72]

The DHS has become the governmental body providing oversight over securing cyberspace and ensuring that agency to agency coordination is taking place for homeland defense. The organization established under the DHS that directs these activities is the National Computer Response Coordination Group (NCRCG), and the DoD's representation to this group is STRATCOM. The NCRCG's role is primarily defensive in nature (DoD is the offensive arm if needed), with a slate toward viewing cyberspace events as criminal activities.

[71] National Infrastructure Advisory Council. *Meeting Minutes, Convergence of Physical and Cyber Technologies and Related Security Management Challenges Working Group*. 11 April 2006. (Page 20)
[72] Department of Homeland Security (DHS). *The National Strategy To Secure Cyberspace*. February 2003. (Page 1)

This sets the stage for DoD's defensive role with respect to other governmental agencies. The President set into motion a chain of events that has built a cyberspace response and support protocol that places new responsibilities on DoD's tray. The military's responsibilities have grown considerably and must be addressed in the very near term.

Military Support to Civil Authorities

> *"The Americans, with minimum losses, attacked and seized a relatively weak area, constructed air fields, and then proceeded to cut the supply lines to troops in that area. The Japanese army preferred direct assault, after German fashion, but the Americans flowed into our weaker points and submerged us, just like water seeks the weakest entry to sink a ship. We respected this type of strategy for its brilliance because it gained the most while losing the least."*
>
> *-- Lieutenant Colonel Matsuichi Lino, Japanese Eighth Area Army, WW II*

Figure 20. Lieutenant Colonel Matsuichi Lino[73]

As the President moved forward to build the cyberspace response activities under DHS – everyone came to agree that the total responsibility for the nation's cyber infrastructure could not be adequately addressed by one organization and nor should it be. As the National Strategy to Secure Cyberspace stated; "Cyberspace is the nervous system of these [critical] infrastructures – the control system of our country".[74] It would be institutionally impossible for one government organization to understand the cyberspace needs of all the branches of government. So, the plan implemented divides the

[73] Joint Chiefs of Staff (JCS). *Joint Publication 1, Joint Warfare of the Armed Forces of the United States.* 14 November 2000. (Page V-3)
[74] Department of Homeland Security (DHS). *The National Strategy To Secure Cyberspace*. February 2003. (Page 1)

responsibilities among the branches of the executive portion of the government. It is important to understand DoD's full cyberspace mission and what DHS and the President expects of the DoD.

The first issue that DoD must address stems from executive order 13286 which states – "…the Secretary of Defense and the Director of Central Intelligence shall develop policies, principles, standards, and guidelines for the security of national security information systems that support the operations of other executive branch departments and agencies with national security information."[75] This is a huge undertaking. There is bound to be information that meets the above definition that the CIA and the DoD don't use or need to have access to. The silver lining in this cloud, if there is one, is that all that is required is policy and documentation; the CIA and DoD do not perform enforcement activities.

Second is the assignment of critical infrastructure lead agencies (see Appendix C). Basically, DHS approached this by taking the critical key sectors of infrastructure from Figure 19 above and divide them up across governmental organizations, doing their best to pair the sectors with their governmental affiliations. As it ended up, all the governmental organizations are cabinet positions except for the Environmental Protection Agency, and DoD ended up with the U.S. "Defense Industrial Base". DoD's job as a sector lead agency is to "Assess their respective sectors' vulnerabilities to cyber or physical attacks and, accordingly, recommend plans or measures to eliminate significant exposures…sectors and lead agencies should frequently assess the reliability,

[75] Bush, George W. President of the United States. *Executive Order 13286: Amendment of Executive Orders, and Other Actions, in Connection With the Transfer of Certain Functions to the Secretary of Homeland Security.* Federal Register 5 March 2003, Volume 68, Number 43, Presidential Documents, Pages 10619-10620. 28 February 2003. (Section 2b)

vulnerability, and threat environments of the Nation's infrastructures and employ appropriate protective measures and responses to safeguard them".[76] This is more than just documentation as required for the intelligence issue above.

The DoD has to identify the "Defense Industrial Base", establish an organization to address these issues with this base and start the vulnerability assessments – as well as start reporting back to DHS on our status, weaknesses, and our proposed solutions for the weaknesses. This is not a job for STRATCOM, this is not offensive in nature – nor is it active defense. This is passive defense, and as such not in the COCOM's realm for execution. The DoD must designated an organization as lead Service for these types of overall passive defense responsibilities. If our support of this sector did turn to active defense, then STRATCOM would get involved – and execute via the Service forces appointed for sector support. Back to the passive and support activities, this task larger than any Service forces currently has allocated to Service network defense. A Service cyberspace command should establish a subordinate organization dedicated to this role. A logical approach would be to bring in the Army, Navy, Marines and Air Force to support their respective sector components under the authority of the lead Service. The longer we wait, the more the DoD allows the "Defense Industrial Base" of the U.S. to potentially be at risk, and the longer we are ignoring the Homeland Security Act, which is the authority basis for this tasking.

[76] Department of Homeland Security (DHS). *The National Strategy To Secure Cyberspace*. February 2003. (Page 17)

Third, the concept of linking Defense Support of Civil Authorities (DSCA) and cyberspace critical infrastructures. The DoD has a long history of helping civil authorities in the event of some type of disaster, this support comes about via the DSCA. All support provided by the military, via the DSCA must be approved by the President and the Secretary of Defense; and for all military forces deployed – the chain of command runs up appropriate military channels.[77]

Now, with respect to the DSCA support, let's look at the following;

> "Immediate Response Authority: Imminently serious conditions resulting from any civil emergency may require immediate action to save lives, prevent human suffering, or mitigate property damage. When such conditions exist and time does not permit approval from higher headquarters, local military commanders and responsible officials from DOD components and agencies are authorized by DOD directive and pre-approval by the Secretary of Defense, subject to any supplemental direction that may be provided by their DOD component, to take necessary action to respond to requests of civil authorities consistent with the Posse Comitatus Act (18 USC. § 1385). All such necessary action is referred to as 'Immediate Response.'"[78]

This places, within the authority of the appropriate military representative, the ability to act when they deem it to be in the best national / situational interest. What does this mean for cyberspace?

Now, taking the above reference, how does it fit with the following;

---

[77] Department of Homeland Security (DHS). *National Response Plan*. December 2004. (Page 10)
[78] Department of Homeland Security (DHS). *National Response Plan*. December 2004. (Page 42-43)

"DOD entities responsible for computer security and computer network defense may exercise those duties in support of the national response effort in four primary roles:

1) Defense Support of Civil Authorities

2) Intelligence and information-sharing

3) Law enforcement investigations

4) Military operations to defend the homeland

DOD capabilities include Intelligence components (the National Security Agency, the Defense Intelligence Agency, the National Geospatial-Intelligence Agency, the National Reconnaissance Organization, and military intelligence components), Defense criminal investigative organizations (law enforcement and counterintelligence), Network Operation Security Centers, and Computer Emergency Response Teams. These entities, in cooperation with other Federal entities, as appropriate, provide attack sensing and warning capabilities, gather and analyze information to characterize the attack and to gain attribution of the cyber threat, participate in information-sharing, offer mitigation techniques, perform network intrusion diagnosis and provide technical expertise. DOD capabilities also include military operational units, which defend the DOD global information grid. DOD can take action to deter or defend against cyber attacks which pose an imminent threat to national security, as authorized by applicable law and policy."[79]

[79] Department of Homeland Security (DHS). *National Response Plan*. (Page - Cyber Incident Annex)

This condenses into something simple; outside of DoD's inherent right to protect themselves; the DoD is now required ***to be able to*** assist with any cyberspace defense activity that may be seen as a threat to national welfare or security across all sectors, with primary responsibility for their own sector. DoD is also responsible for Net-A for the government; any response that requires cyberspace offensive force will flow to the DoD for execution. This leads back to my earlier assertion that DoD must maintain the US' premier cyberspace capabilities.

These activities require the sharing of information and close integration with the other departments of the executive branch. For severe attacks in cyberspace, these other departments will need the support of the DoD. This places the DoD in a great position; the DoD needs tight integration with these other components of government to be able to coordinate cyberspace activities in concert with the other elements of national power – leading back to the MIDLIFE discussion before. Close integration will help the DoD to meet their DHS requirements as well as facilitate DOD effects based planning, which was General Pace's original goal. Even the DHS comments on this issue (with the approval of the President) – "When a nation, terrorist group, or other adversary attacks the United States through cyberspace, the U.S. response need not be limited to criminal prosecution. The United States reserves the right to respond in an appropriate manner. The United States will be prepared for such contingencies."[80] The DoD is the governmental organization that must be prepared to respond to such contingencies in a non-criminal prosecution fashion, i.e. a military fashion in cyberspace.

[80] Department of Homeland Security (DHS). *The National Strategy To Secure Cyberspace*. February 2003. (Page 50)

Military Action

In the cyberspace environment itself, we must make sure we are prepared to fight and win. Each Service works with industry in an effort to secure their respective infrastructures as best as possible. But, on this point, the Office of Management and Budget identified to Congress six common government wide security weaknesses that we must make sure are addressed appropriately within the DoD at all levels. "These weaknesses included:

1. Lack of senior management attention.
2. Lack of performance measurement.
3. Poor security education and awareness.
4. Failure to fully fund and integrate security into capital planning and investment control.
5. Failure to ensure that contractor services are adequately secure.
6. Failure to detect, report, and share information on vulnerabilities."[81]

Any activities we intend to take must first be proceeded with "know thyself", and to accomplish that we have to address the above weaknesses as well as all other Service identified security and process problems.

As we move forward in cyberspace, we must remember that this is a new domain, and not everything passes its first test with flying colors. And, just because it is not completely successful during the first campaign does not mean it will always be that way. I was reminded of this issue while reading the "Scientific American" magazine. They

[81] Department of Homeland Security (DHS). *The National Strategy To Secure Cyberspace*. February 2003. (Page 44)

have a section that references articles from past magazines; it gives a snapshot of history to remind the reader of how things have changed over time. In the November, 2005 issue, they have one of these snapshots titled "Torpedo Miss" from November 1905 issue – which states:

> "The Whitehead torpedo has exercised a greater controlling influence upon naval construction and tactics than perhaps any other single weapon of naval warfare. However, it cannot be denied that the torpedo has, at times, been greatly overrated. Indeed, the experience of the recent war seems to prove that only under exceptional and very favorable conditions can the torpedo get in its blow. In the fleet engagements on the high seas it seems to have exercised very little, if any, influence upon the battle formations. Consequently, we think it unlikely that torpedo tubes will be fitted into future warships."[82]

Concepts, weapons and tactics mature over time, and cyberspace will not be an exception to this paradigm.

Common Military Activities

Several common military cyberspace or cyber related activities that should be underway at all times, and during almost all circumstances are listed here – they are not identified as particularly offensive or defensive in nature. These are military necessities for future actions and should target all the elements of national power:

Cyber Surveillance: Maintaining constant awareness of all potential adversaries' cyberspace activities to the best of our ability.

[82] "Torpedo Miss" *Scientific American*, Page 16 (November 2005).

Non-Intrusive Reconnaissance: Maintaining constant awareness of all potential adversaries' cyberspace infrastructure to the best of our ability, without letting them know we were looking at their systems.

Intrusive Reconnaissance: The same as above, but with the intent of letting the adversary know we were there.

Blue Doors: Establishment of private "backdoors" at locations of our choosing within an adversary's systems.

Non-Destructive Viruses and Worms: Malware that can track activities, capture passwords, disable security features on demand, etc.

Global Infrastructure Ownership: Document global as well as U.S. based ownership of all key IP based service providers. Also, identify U.S. corporate ties to non U.S. owners.

National IP "Choke Points": Identify and monitor "choke points" in U.S. based IP infrastructure. Help identify national level impact of outages and possible alternatives in case of an outage. Also identify critical "choke points" for each element of national power if they exist.

Foreign Ownership And Control: Identify all IP based communications systems in the U.S. owned and/or operated by a foreign corporation. Help monitor potential undue influence or control by foreign governments and identify national level impact of outages and possible alternatives in case of an outage. Identify relationships to the elements of national power if they exist.

The same problem exists for all governmental activities that are located outside the U.S. to include overseas military bases. The DoD must identify all IP based communication systems that use foreign owned corporations or governments

infrastructure and develop alternative means for communication if these services are unavailable.

Conference Attendance: Attend conferences (globally) on computer hardware and software, IP security, hacking and future technologies. This should not be limited to research personnel; it must include personnel from attack, defense, operations, maintenance, criminal investigations, and general staff.

Offensive Activities

This is another area where there are varying opinions as well as a lot of research. I will limit my comments to just a few very effective activities before I move on to my primary premise, the Combat Power Matrix.

Civil Recruitment: The first approach is to learn from the civil sector. There are many very talented individuals across our nation that may be perfect as hired consultants who would bring much needed expertise with them. It would be something similar to what happened to Frank Abagnale Jr., the individual that the movie "*Catch Me if You Can*" was loosely based upon. He was a check forger that managed to steal a lot of money until he was caught. After leaving prison, he was hired by the banking industry to help them prevent future forgery crimes.[83] This hiring approach tends to target the individuals with similar capabilities as our adversaries. Over time this may change, but currently the military is not training cyberwarriors to be more effective than cybercriminals.

Cyber-Herding: There are multiple types of information influence operations. Changing the information within the adversary's systems can influence decisions in many ways: it

[83] "Frank Abagnale," http://en.wikipedia.org/wiki/Frank_Abagnale. (No page number)

can lead them to make movements we desire; it can convince them they are overwhelmed and can't win; or, just distort their perception to the point that they trust no information – even the information we have not modified.

For the ultimate in cyberspace influence operations, a paper by Captain David B. Moon at the Naval Post Graduate School speaks to cyber-herding[84], an influence operations process. This concept is basically a step by step process of shaping the information space to your advantage. Let's take a look at a set of steps that could be used against a terrorist organization;

1. Identify the terrorist's web sites and chat rooms.
2. Blue team members interact with individuals in the chat rooms posing as supporters to build relationships and use this process to identify key individuals in the extremists' links.
3. Using the information gathered from these web sites – the blue team builds similar web sites with similar messages. The blue team infiltrators promote these new blue team web sites in the extremists' chat rooms to lure individuals over to the blue team systems.
4. Attempt to bring down the original extremists' web sites.
5. Slowly change the message the web site delivers in an attempt to negate the original message.
6. Start bringing down some of the duplicative web sites, leaving just a few for monitoring purposes.[85]

[84] Moon, David B. "Cyber-Herding: Exploiting Islamic Extremists use of the Internet," Naval Postgraduate School, Department of Defense Analysis, Joint Information Operations Student. (Page 6-7)
[85] Moon, David B. (Page 6-20)

The blue team web sites and chat rooms can help identify terrorist suspects, possible operations, collect extremist cell donations, and possibly direct activities away from U.S. forces and allies.

A primary challenge to cyber-herding and the other approaches listed above is that cyberspace organizations must have foreign linguists and foreign area experts. It is impossible to conduct cyberspace influence operations to the degree discussed above without having the correct cultural knowledge and ability to converse in the appropriate "street slang".

Cyber-herding is one type of misinformation campaign and is not anything new: it is just more formalized. Louis Miguel's article in the January 2006 Scientific American magazine references Gabreil Weinman, a professor of communications at the University of Haifa in Israel, and Marc Sageman, a psychologist at the University of Pennsylvania and a former CIA officer, in his discussion of misinformation types of operations. Both professors believe that due to the informal terrorist web site organizations and the vast number of new web sites that have emerged, it should not be that difficult to change the messages being delivered and help shape the consciousness of this web environment.[86]

Search Engine Bombs: This one is a little time consuming but can very quickly direct individuals looking for terrorist web sites to your web servers. All that is required is to build web pages that contain all the usual catch phrases of your targeted audience. Be sure to make the web pages appear legitimate. The servers do not need to have too many pages – just enough to seed the search engines. The next step is to replicate the web

[86] Miguel, Luis A. "Virtual Jihad: The Internet as the Ideal Terrorism Recruiting Tool," *Scientific American*, Pages 18-21 (January 2006).

server hundreds of times – and give each virtual copy its own address and name. Then modify the messages on these web pages, and use different pictures as much as possible to try to keep visitors from becoming suspicious. You can have exact copies for some of the pages – it is unlikely that a visitor will visit too many pages while searching – they will most likely find what they are looking for after a short period of time.

When web search organizations canvas the web looking for sites to catalog, they will discover your systems and create registry entries for each page. When the would-be terrorists visit the search engine, most of the links they receive will be your web pages – this process then can be linked to Cyber Herding or can support any other cyber identification activity underway.

Combat Power Matrix (CPM): There are literally thousands of approaches to cyberspace offensive activities. More are being dreamed up each day by hacker organizations, commercial security organizations, DoD laboratories, and bored high school students. I intend to document an approach for planning purposes that links our National Strategy, National Military Strategy, Effects Based Planning (General Pace's concerns) and a variance of one of the military targeting strategies currently used by the Air Force.

As discussed earlier, we can link the National Strategy to the National Military Strategy via the military element of national power (Figure 21). There is also a relationship between the other elements of national power and the military element, each element affects one another – so, there is a military thread across all elements as well as an elemental thread of each with in the military element. This is demonstrated shortly.

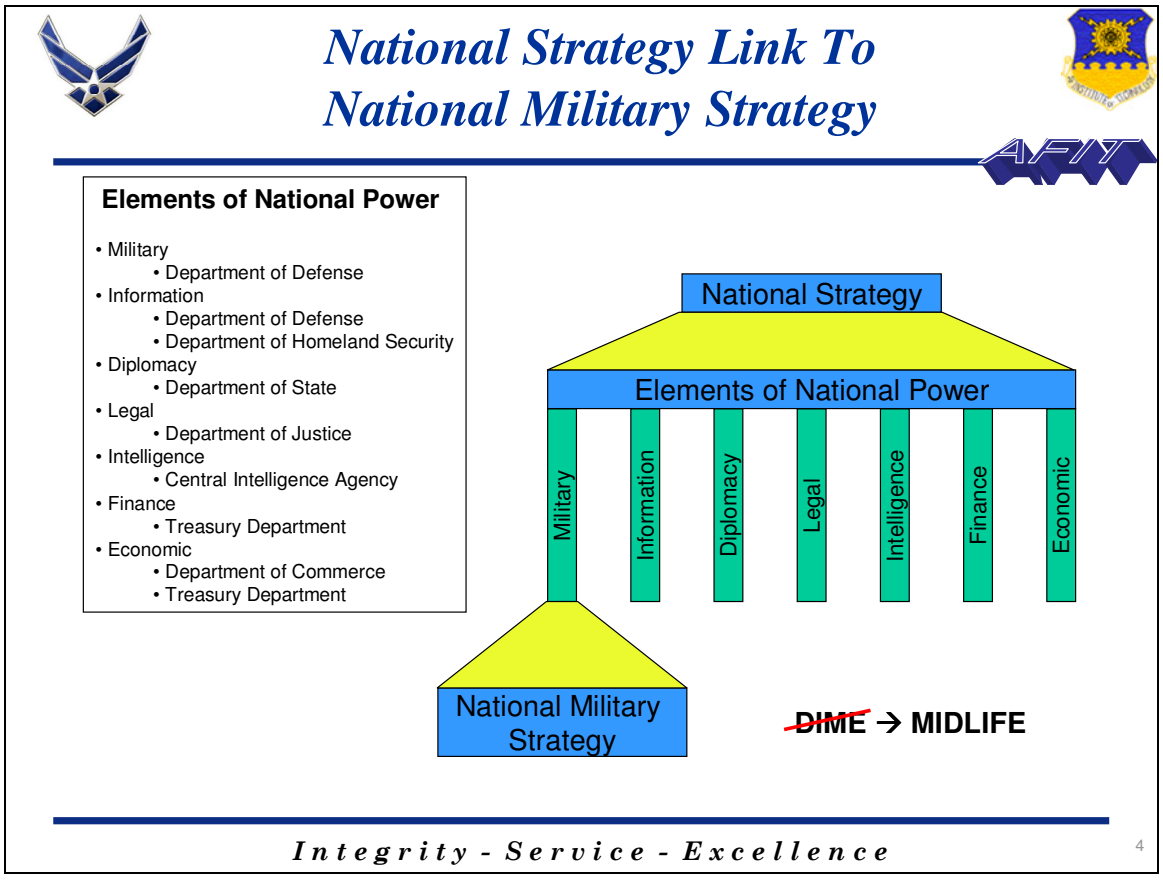


Figure 21. National Strategy Link To National Military Strategy

The next logical link in the chain is to tie the National Military Strategy and the Air Force targeting model to demonstrate the "strategy to battlefield" linkage. The first step is via the effects based planning process, of which the effects are directly derived from the National Military Strategy. From here, we identify what targets we need to attack to achieve the desired effects – and evaluate these choices via PMESII in an attempt to validate the selections based upon those original desired effects. During this process, we divided these targets into groupings or classes that we call "centers of gravity" – which is part of the segmentation process of target identification. The Air

Force targeting model I used for this discussion was Wardens Five Rings. I then modified the model to produce the "Seven Rings of Combat Power" as seen in Figure 22.

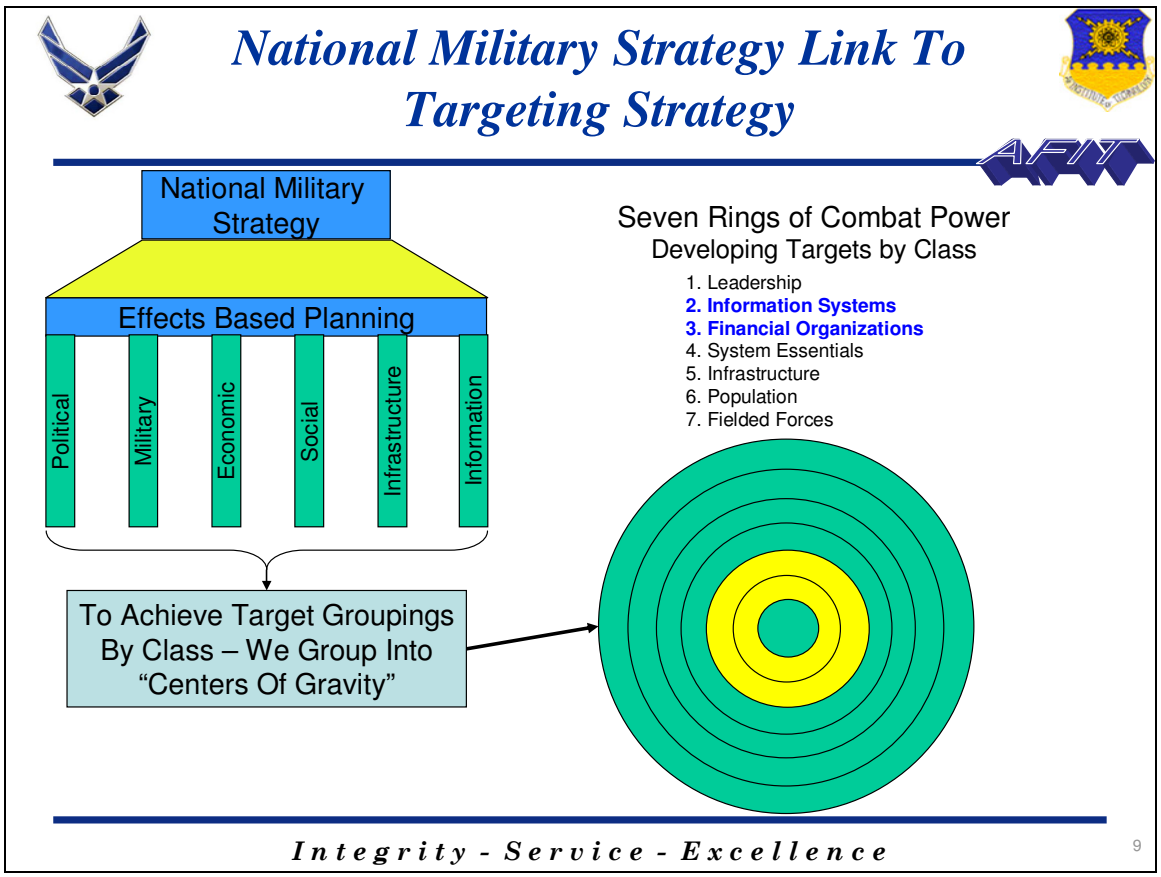


Figure 22. National Military Strategy Link To Targeting Strategy

The linkage is now straight forward, but we still did not have a way to show a direct correlation between target choices and their relationship to the elements of national power. The next logical step was to produce that linkage. Without such a capability, to draw conclusions with respect to targets versus National Strategy would require tracing the intent from the target, through its PMESII validation to National Military Strategy, and back to the National Strategy. Issues complicating this trace would include

subjectivity in the target selection and PMESII validation processes as well as the dynamics of the interagency interaction from the other elements of national power.

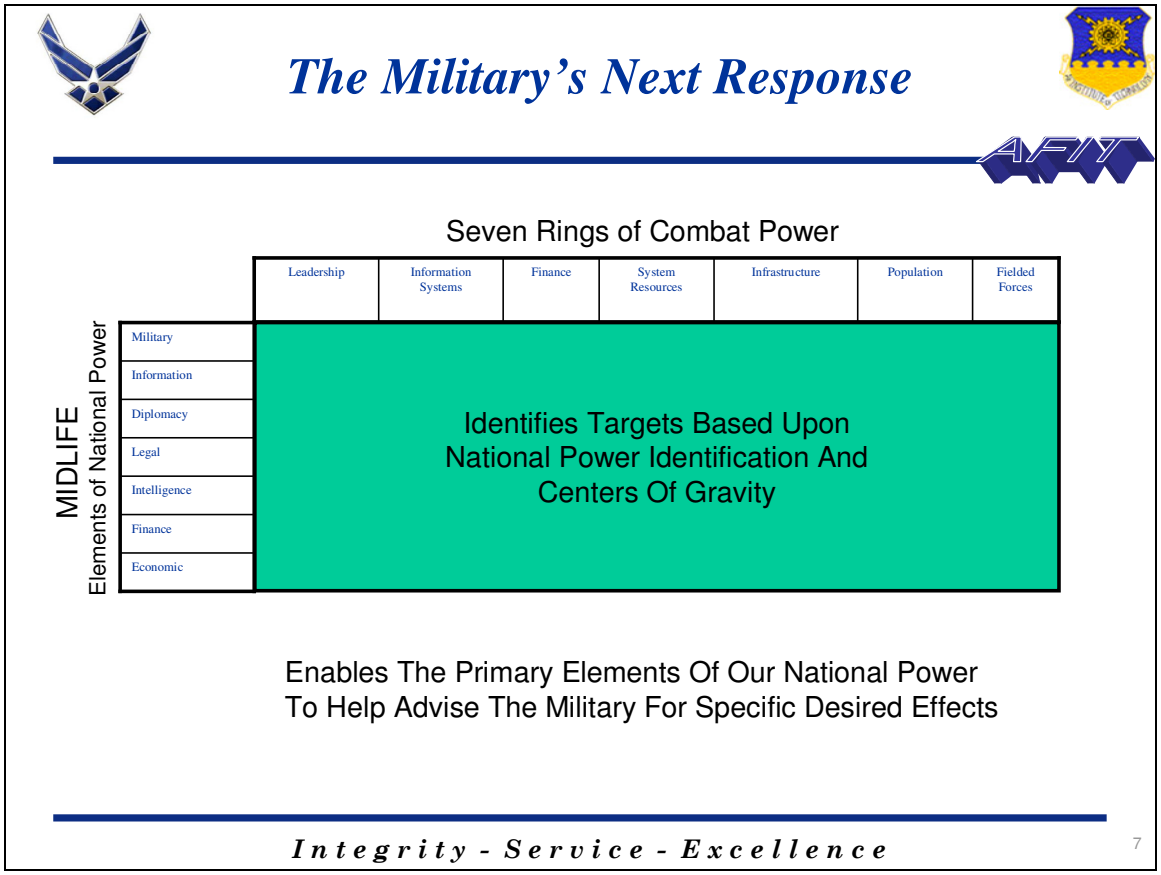


Figure 23. Combat Power Matrix (CPM)

In an attempt to provide a support tool for targeting and PMESII validation processes, and a tool that documents a linkage between a targeting model and the elements of national power – I developed the "Combat Power Matrix" (CPM). This matrix can be built based upon any targeting model; I chose to use the Seven Rings of Combat Power as described earlier. This matrix identifies targets based upon the national power element identification and centers of gravity. It enables the primary elements of

our national power to help advise the military for specific desired effects. It also gives us the capability to trace any target to an element of national power.

From a defensive perspective, this matrix can help identify which portion of the federal government should take lead and help in determining the adversary's strategy. From an offensive perspective it identifies targets as well as which area of the federal government the military should be interacting with to validate their assumptions about the effects this target choice may have. This interagency interaction may also assist with the PMESII validation. The CPM concept is valid across all military domains, but especially in cyberspace. It is essential that interagency cooperation and coordination reach a new plateau, due to the possible effects felt across all the elements of national power. And, we must be able to show explicit detail and linkage in our cyberspace target selection; because in cyberspace the military can not act alone for true effectiveness.

Figure 23 provides an overview of what the CPM should look like. The seven rings of combat power can be replaced with the preferred targeting model if desired. The hard part comes in when you populate each individual square. The model is easier read from the column perspective. For example, using the notation (row,column), (*,1) would be read as looking for Leadership targets in each element, and (4,1) would be national level legal leadership. For the United States, this would be, for example, Congress, Supreme Court Justices, Directors of DEA, FBI, and the Secret Service, Appeals Court Judges, etc. The intersection of Diplomacy and Infrastructure, (3, 5), would yield Department of States Facilities, Embassies and Consulates. A baseline CPM for the matrix depicted in Figure 23 is in Appendix D; detailed CPMs may be needed for specific nations, regions or terrorists groups.

Defensive Activities

> *"When the next big disruption comes, the biggest potential danger is that it won't make complete sense…"*
>
> *-- David L. Margulius, Senior Contributing Editor, InfoWorld Magazine*

Figure 24. David L. Margulius, Senior Contributing Editor, InfoWorld Magazine[87]

There are currently several cyberdefense obligations for the DoD. Each one has a different set of responsibilities and each requires attention to ensure those responsibilities are being addressed appropriately.

Intelligence Systems: The President established this requirement via executive order 13286 – "…the Secretary of Defense and the Director of Central Intelligence shall develop policies, principles, standards, and guidelines for the security of national security information systems that support the operations of other executive branch departments and agencies with national security information."[88]

This obligation reaches across all components of the executive branch of the government. The CIA is included to help identify the information systems and validate their level of protection; the DoD is included for their experience and expertise in cyberdefense. Together they must also develop a process that allows for updates to this doctrine to accommodate rapid technology and threat changes.

A proposal for a way ahead;

---

[87] Margulius, David L. "Crisis Management 101: Preparing for disaster means preparing yourself to act decisively when little is known," *InfoWorld*, (8 March 2007) (No Page Number)

[88] Bush, George W. President of the United States. *Executive Order 13286: Amendment of Executive Orders, and Other Actions, in Connection With the Transfer of Certain Functions to the Secretary of Homeland Security*. (Section 2b)

1. Establish a CONUS based permanent military unit to be co-located with their CIA counterparts.

2. This is a passive defense issue, thus it is a project outside of a COCOM's role. Since the Secretary of Defense was tasked specifically and not the DoD – that implies the President wanted some degree of direct oversight. This leaves the Secretary with primarily two options. First, the Secretary could establish an Office of Secretary of Defense (OSD) level organization to address this responsibility. Second, the Secretary could direct the establishment of the unit within one of the Services to take on this task. Either way, any organization would need to keep the Secretary and STRATCOM current on all obligations and activities. The OSD level office has the benefit of being closer to the Secretary which would allow a direct interface and possibly less "red tape". The Service level office has the possible benefit of being part of a larger cyberspace organization with direct daily access to cyberspace experts for extremely fluid and rapid responses if required.

Both options are viable, but the Service option establishes a tie between one of the Services and the CIA that will be needed in the other cyberspace defense obligations. This will support the building of bridges with the CIA as well as all the other components of the executive branch of government which is essential for helping them support their sectors. It appears the best solution is the Service level unit since these types of activities are not the responsibilities of a COCOM and it will not fit within an OSD office unless that OSD office is going to address the rest of the DoD cyberdefense obligations, which they currently

can't do because it is a Service activity. The unit should be with the Service's cyberspace command organization.

Defense Industrial Base: This activity is a Service level activity, with oversight from STRATCOM, much of which was discussed earlier. Whichever Service were to become the Service lead should establish an organization within its cyberspace command to address this issue. It may prove beneficial that this unit be the same unit as described above for intelligence systems.

The details of this organization will be developed over time, but the responsibilities are already defined – at least at a high level. There are two key inputs that should be addressed at the beginning of this process. First, is that each Service should be responsible for identifying their own Industrial Base. And, second, the Service lead and the DoD should examine the possibility of including the National Guard or Air National Guard (ANG) for this activity. It could be feasibly argued that the Guard may be best equipped to address the Defense Industrial Base within their respective states, under the authority of the Service cyberspace command.

No matter the final solution – this will have to be a partnership with industry to a level not seen before in the DoD.

Civil, DSCA and Law Enforcement Responsibilities: The DoD must be ready, capable and authorized to come to the aid of any of the civil sectors in the case of a cyber event, to support law enforcement requirements (especially for criminal versus state level determinations), and to be capable of rapidly responding to national emergencies in the cyberspace domain – probably from a defensive or possibly a service restoral role.

Governmental Responsibilities: The DoD is the fall-back organization for all governmental organizations that may fall prey to cyberspace events. The DoD will have to support all governmental organizations as well as their responsible sectors identified in the DHS documentation.

Military Facilities and Systems: This is an inherent responsibility for the DoD to be able to support and protect itself, including full restoral capabilities.

Support For Allies (Military and Civil Emergency /Natural Disaster): As other nations share our information and information systems, and as more and more weapon systems become IP addressable, it will eventually be necessary to establish cyberspace support and cyberspace defense agreements. This will entail exploring new levels of relationships between us and our allies. This particular problem will not be solved in the short term, but here are a few items to start the ball rolling;

1. There will most likely be permanent and temporary cyberspace relationships. The permanent relationships are those with long time allies with whom we share IP based weapon systems and are involved with our coalition planning processes. The temporary relationships will probably result from natural disasters or other related emergencies where integrated support is required. Our future processes and systems must be able to support and defend permanent and temporary allies to the best of our ability. This may include helping defend our allies independent systems, especially if our operational plans need their systems operational.
2. This will most likely require Service by Service integration. The U.S. Navy would be better able to support a foreign Navy's requirements over the USAF.

However, all activities should still be rolled up under the lead Service. Again, STRATCOM would engage on behalf of the foreign organizations based upon negotiated parameters for active defense purposes.

3. Support of a foreign nation's civil sector or defense industrial base is more complicated, but may be essential if involved in a major conflict in or out of cyberspace. This kind of support is not unprecedented, American fighters defended English military facilities, manufacturing facilities, and the general population during WWII. The legal issues must be agreed to in advance, and pre-approved before any such emergency takes place. Failure to do so could cost valuable time that we may not be able to afford.
4. Such emergencies may be solely of a cyberspace nature. Suppose for example, an adversary cyber attacks Canada. The Canadian government may be intact, as well as their military and their industrial base – but all may come to a halt due to a massive cyberspace attack. In this case, 100% of the response may be in cyberspace itself and we must be prepared for that case.
5. We must establish pre-coordinated responses to second order cyberspace attacks with host nation governments and service providers. A second order attack, for example, would be to bring down all U.S. bases in Japan by attacking NTT, the primary IP based service provider for U.S. forces in Japan. The attack on NTT would not be seen by U.S. forces since our data leaves our facilities via bulk encryption. Due to a loss of services, we would engage NTT and the Japanese government – and thus may be requested to support the

host nation. Due to the necessity of a rapid response, pre-coordinated agreements need to be established.

Nation Building Support: The Army currently provides a Civil Affairs type of function for the DoD. These activities help the local communities re-establish themselves in the event of war or a natural disaster. The DoD also assists the host nation with governmental rebuilding efforts in much the same way. In future conflicts, cyberspace reconstruction will be a requirement, regardless of whether or not kinetic weapons are used. The question is: should this fall under the Army's Civil Affairs, or somewhere else? I propose that it fall under a Service cyber command. Civil Affairs deals with the land domain and the cyber command deals with cyber domain. During governmental cyber reconstruction, the fledgling infrastructure must be defended – the best way to defend this new infrastructure is to turn its defense and development over to an organization of dedicated cyberspace professionals.

This issue is the newest territory to be examined. At this time, I could not find any documentation in the civil or military domains addressing this issue. So, basically, we will have to start from scratch. My suggestions are;

1. Recover as much as possible from the previous architecture.
2. Concentrate on military, revenue, utilities and legal systems first.
3. Get the commercial ISPs up and operational as soon as possible; they can serve as information outlets for the government to communicate with the population and help stimulate e-commerce activities.

The more a nation has moved commercial operations into the cyberspace domain, the more the nation is reliant upon the cyber infrastructure being up and operational. The

faster this effort is addressed, the faster the other portions of reconstruction can get established.

Federal Law Shortfalls With Respect To Military Activities:

Cyberspace activities have been moving faster than Federal Law has the ability to keep pace. Currently, the more inventive an adversary is – the more complex they can make the legal environment; even to the point of using our own Constitution against us. The context of future cyberspace legislation should not be written solely based upon non-cyberspace concepts and principles. This is a new domain, and we must establish guidance that is suited to an environment where the measurement of distance is no longer relevant, time is essential and scalability can be exponential. And, where legal code may have to be different based upon your cyber location (domain) and not necessarily your geographic location.

Commercial Web Servers And The First Amendment: In an earlier section I mentioned the web servers that Iran has placed in different countries. What are the legal implications of us targeting one of these systems? We may just want to stop an organization's message from getting to the public – such as a radical Islamic web site. If Iran places these web servers in China or Russia, what are the legal issues? If the adversary realizes that our Constitution could be used against us, they could hire local supporters who are also American citizens. Then, they could advertise via their web site that it is owned and operated by these individuals. If the military would then target this

web site, it could be seen as violating the individual's first amendment right to freedom of speech.

Free speech applies to the spoken as well as the written word (paper or electronic). And, it applies to postings on web servers as well as email. Here is a section from bill HR 4741, from the 109th Congress, Second Session (the bill is in committee):

> "Freedom of speech, freedom of the press, and freedom of association are fundamental characteristics of a free society. The first amendment to the Constitution guarantees that `Congress shall make no law…abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble…'. These constitutional provisions guarantee the rights of Americans to communicate and associate with one another without restriction, including unfettered communication and association via the Internet. Article 19 of the Universal Declaration of Human Rights of the United Nations explicitly guarantees the freedom to `receive and impart information and ideas through any media and regardless of frontiers'."[89]

The above bill is still in committee, but this section was in the introduction stating how Congress and International Law sees individual rights to communicate over the internet. It also points out that the United Nations' view, under Article 19 of the Universal Declaration of Human Rights, may pose problems that also need to be addressed in Congress.

[89] Ros-Lehtinen Ms. and other Representatives. *Global Internet Freedom Act*. House of Representatives Bill 4741, 109th Congress, Second Session. 14 February 2006. (No page number)

Now, taking the freedom of speech example a little farther, Iran could place their web servers within their borders in American citizen hands also, thus pushing them off of the target list. Current law will require our military to know if any "commercial" or "private" system in any country is owned and operated by American citizens, and keep current on this information. Not staying current could drag the military into court for years, and the military may even find itself in civil law suits that they cannot win. Depending upon the actions taken, the military may even find itself embroiled in civil actions from citizens of ally nations. For example, if some of the servers in Iran were owned by British citizens. One of the best enemy defenses may be to identify a large number of American allies and then find individuals in your country who are citizens of those nations and disperse your commercial systems across this group. This would tie the hands of the U.S. military as they deal with law suits and complaints form multiple nations as well as American citizens.

If the U.S. had a military conflict with another nation, the military would not be held responsible for incidental deaths of Americans if the Americans were in the adversary's key military facilities. The military is not capable of knowing the whereabouts of American citizens in a specific nation at all times. The military is also not limited in targeting American owned facilities if they are legitimate military targets within the adversary nation. Crossing into the cyberspace domain, this is no longer true because we are basically talking about destroying the written word, and the person's right to communicate that word to others. The context of the right of freedom of speech is the "word", written or spoken. Our laws are not written to treat this target (words and their medium) as a legitimate military target. This limitation ties the military's hands in

cyberwarfare confrontations. The problem Congress must deal with is how to reconcile the conflict between our first amendment rights and our need to operate militarily within the cyberspace domain by targeting a first amendment medium. There may be very limited American military influence operations or Net-A operations in cyberspace if this legal issue is not addressed and our adversaries take advantage of the situation. In a search, I found several articles supporting the freedom of speech via web servers, many of which were validated in the courts.

Multinational Governmental Systems: The above discussion inevitably leads to the issue of multinational military systems. For example, suppose British, Canadian and American air war planning systems became integrated to facilitate joint nation operations and the British were to have another conflict with Argentina over the Falklands. If Argentina conducted cyberwarfare operations against the British, what impact would this have on American systems, and how should we respond? What legally can we do? The same holds true for our adversaries. If China and Iran were to develop a cooperative relationship where Iranian governmental systems were integrated with Chinese governmental systems – does this mean that during a conflict with Iran, that these Iranian and Chinese linked systems are off limits to cyberwarfare?

Cyberspace Domain Ownership: The domains of land, sea and air are physical constructs that can been seen, measured and owned – but, who owns cyberspace? Some concepts of cyberspace portray it as an evolving man-made universe, not too dissimilar in nature from the virtual reality game constructs currently played over the internet. Step-back from the science fiction version for a second and consider, the physical realm, consisting of the routers, switches, circuits, multiplexers, and signal modulators, etc. All

of these components are owned by someone; and in the U.S. we are now talking about corporations like American Telephone and Telegraph (AT&T), Qwest, Sprint, etc. These companies own this hardware, their systems help create this new domain. This is completely different from airspace for example; who owns airspace? If we engage another nation – the airspace is "owned" by that other nation, and we are infringing upon that nation's ownership rights. This infringement is expected during hostilities between nations. Is this corporate system infringement legal in cyberspace under today's current laws?

By waging cyberwarfare we are designating the battlefield domain as cyberspace. In doing so, we are waging war across infrastructure the military does not own. In many cases, it is commercially owned infrastructure, and as such, does the military have any legal basis to wage cyberspace warfare via commercial infrastructure? By using this infrastructure, we are making it a target for our adversaries. Did these corporations sign up to this use of their systems? Is it documented in their contracts that we will be putting them at this level of risk? Are they being compensated for it? If these American corporations choose not to agree to these requirements, how would the U.S. military get its cyberspace connectivity? By federal law, can these corporations be forced to allow the military to use their infrastructure for cyberwarfare? And, is the military obligated to then protect the service providers as they do themselves?

Does using this infrastructure open the military to law suits from these corporations? A few years ago AT&T lost a key node in Atlanta and the military lost connectivity to several military bases, and it is probably a good guess that several commercial facilities also lost connectivity. If this were caused by an adversary

retaliating against the military, does this open the military to civil action from the service provider? What about civil action from the service provider's other customers who were also affected by the outage? Is the DoD currently protected via federal law?

Taking this even farther, what about overseas military bases? Are there agreements with these foreign service providers to allow the military to use their infrastructure for cyberwarfare? Even if we don't use the infrastructure for Net-A activities it does not mean our adversaries will not see those bases as targets. And see those foreign service providers as targets also. What protections exist in the Status of Forces Agreements or in the treaties with these nations? Is there an international law implication, and will this open the military to international civil actions? In some instances, it is also possible that some services are provided by corporations not within the host nation. They may even reside in a nation where we do not have forces stationed; and because of such do not have the correct treaties in place for full protection under international law. This leads back to the previous discussion – we must know who all the foreign service providers are – as well as all of their sub-contractors, even from third party nations.

Future Cyberspace Issues: This domain will not be stable for some time to come. General Ronald Keys, commander of Air Combat Command, understands this – "This is an area where technology has outstripped our ability to make policy."[90] I contend that his comment applies to policy and legislation equally. The DoD must work with Congressional leaders to prepare legislation that will address legal concerns as this

[90] Rogin, Josh. "DoD Issues New Policy On Electronic Warfare: Policy Could Be The First Of Many For Dealing With Cyberthreats From Chinese Hackers," *Federal Computer Weekly (FCW.COM)* (26 February 2007). http://www.fcw.com/article97749-02-26-07-Print. (No Page Number)

domain develops. We must work to push this legislation to lead current cyberspace activity, not respond to it. Professor Ruth Wedgewood, from Yale University, recently brought up a possible future where cyberspace creates internet-based micro-nations, nothing like we seen yet in history.[91] This could open up entirely new issues for Congress to work (Referring to the earlier statement that legal code may have to be different based upon your cyber location (domain) and not necessarily your geographic location) – what legal constructs exist for relations with "Virtual Nations".

[91] Wedgewood, Ruth, Meeting Minutes from "Panel on Internet and Public International Law", http://www.uky.edu/Law/aals-int/y2k Wedgewood, Ruth. Yale University Professor. Panel on Internet and Public International Law. *Meeting Minutes: Effects of the Information Revolution on Public International Law, 2000*. http://www.uky.edu/Law/aals-int/y2k.htm. (No page number)

V. Conclusion

Throughout this project, we have reviewed the relationship between the Services and the COCOMs with respect to cyberspace. Many discussions center around empowering the COCOMs to take on activities that they are restricted from pursuing based upon Federal Law. The majority of joint documents don't even address the issue.

I hope it is now clear that there are Service operations and COCOM operations in Cyberspace. And that the COCOMs can not take over Service operations, nor can STRATCOM absorb DISA activities. The Congressional intent documented in Federal Law is based upon President Eisenhower's intent – the father of the DoD joint structure – which is that there are Services to build, maintain, and train forces; and there are COCOMs to engage and fight the enemy. They are separate and distinct, each with their own independent reason for existence. I believe it is an internal DoD check and balance system that works well.

Service consolidation is confusing the cyberspace issue even more. Funding and manpower are no longer readily available, and as the Services struggle with how to accomplish their mission, they increasingly look to industry for answers. Today, in the technical centers around the world, consolidation is driving innovation and changing the commercial sector. The military is using the same systems, adopting the same principles, and changing the way the DoD does business in cyberspace – it was inevitable. The relationships between the Services and the COCOMs need to be structured upon the original intent of what a COCOM's mission is – to fight and win wars.

Cyberspace has helped to cause an evolution in the way governments see their national powers. This evolution has changed DIME into MIDLIFE, thus placing information (cyberspace) in the position of being an element of national power. This requires a change in how we plan for engagements, it requires a change in how we think about targeting our adversaries, and it requires a change in how we evaluate our choices in warfare. The Combat Power Matrix provides us a tool to demonstrate a linkage between our targeting choices and the elements of national power. This fills a fundamental need in identifying what we need to protect as well as identifying detailed and specific targets to achieve our desired effects. Moving forward in cyberspace demands less ambiguity and more granularity to achieve the system-of-systems level effects that General Pace spoke of.

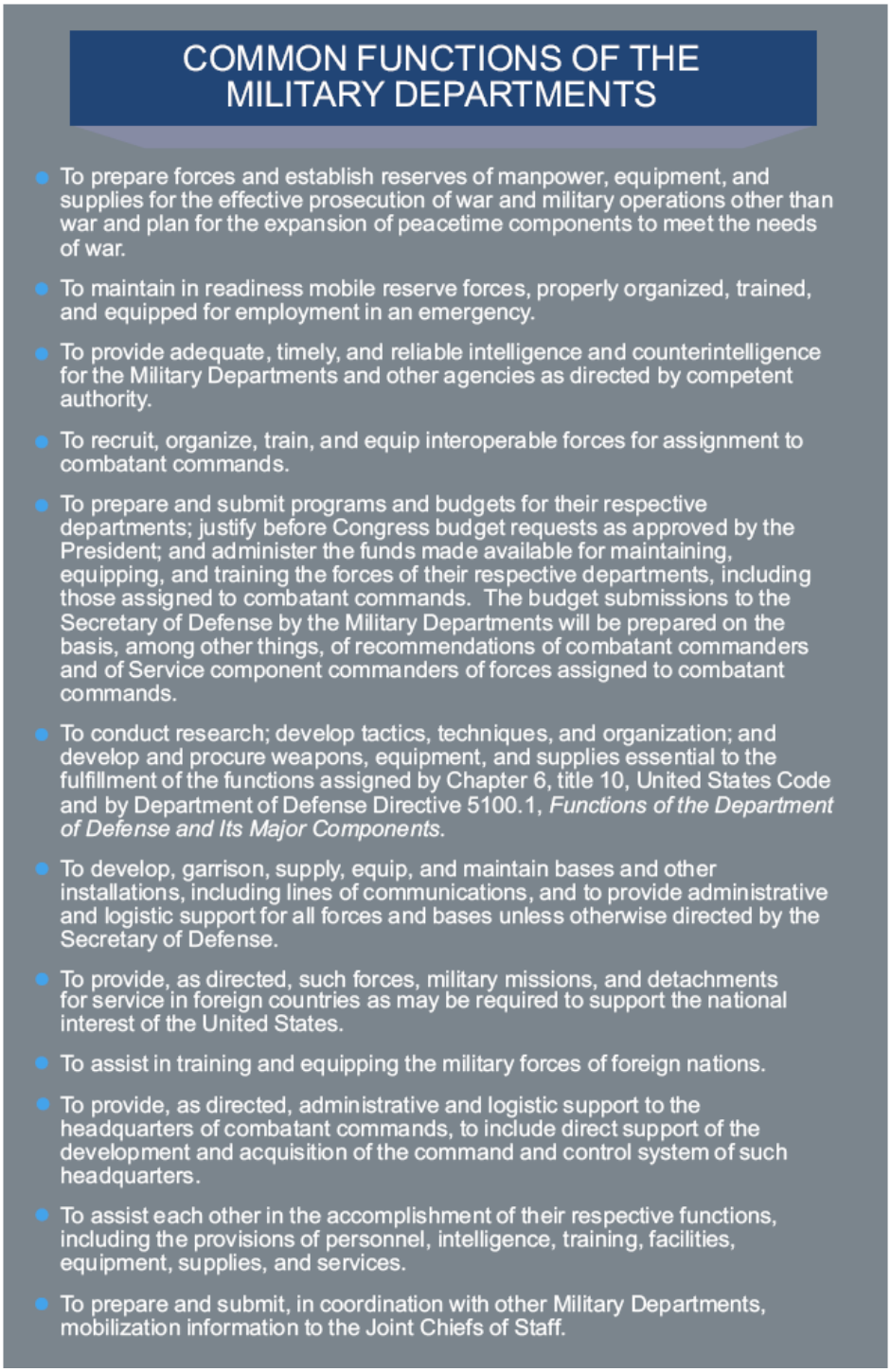
The DoD obligations in cyberspace appear to be extremely difficult. The support requirements of our allies, the civil sector, the American populace and the DoD weapons and infrastructure is too large of a problem to take it all on at one time. We have to divide and conquer, while addressing all concerns across the board. This new environment will require the DoD to establish new and closer relationships with the other components of our government and our allies than DoD has ever before. This will mean that the DoD will have to learn to depend upon these relationships in order to operate effectively, and this too will be a new domain for some well established sectors within the DoD. In the end, these new relationships will lead to the environment that the President was trying the achieve.

As the DoD moves into the cyberwarfare arena, it is very important that we remember that this is a new domain for warfare – and that many of the old axioms do not

apply. As Dr. Lani Kass, Director of the AF Cyberspace Task Force, stated, "This allows, for the first time in history, global effects to be delivered at the speed of light…" – so, our engagement process must be lean and streamlined.[92] This is not a time to examine what works in ground combat, air combat or naval combat – it is a time to examine what cyber combat can bring to the DoD's arsenal and how that arsenal can affect those other domains as well as give us freedom to act and win in the cyber domain.

[92] Kenyon, Henry S. "Task Force Explores New Military Frontier," *Signal: Armed Forces Communications and Electronics Association (AFCEA) Journal*, 55-57 (October 2006). (Page 57)

Appendix A: Common functions of the Military Departments[93]



[93] Joint Chiefs of Staff (JCS). *Joint Publication 0-2: Unified Action Armed Forces (UNAAF).* 10 July 2001). (Page II-13)

Appendix B: General Functions of a Combatant Commander[94]

[94] Joint Chiefs of Staff (JCS). *Joint Publication 0-2: Unified Action Armed Forces (UNAAF).* 10 July 2001. (Page II-14)

Appendix C: Critical Infrastructure Lead Agencies[95]

CRITICAL INFRASTRUCTURE LEAD AGENCIES	
LEAD AGENCY	**SECTORS**
Department of Homeland Security	• Information and Telecommunications • Transportation (aviation, rail, mass transit, waterborne commerce, pipelines, and highways (including trucking and intelligent transportation systems) • Postal and Shipping • Emergency Services • Continuity of Government
Department of the Treasury	• Banking and Finance
Department of Health and Human Services	• Public Health (including prevention, surveillance, laboratory services, and personal health services) • Food (all except for meat and poultry)
Department of Energy	• Energy (electric power, oil and gas production, and storage)
Environmental Protection Agency	• Water • Chemical Industry and Hazardous Materials
Department of Agriculture	• Agriculture • Food (meat and poultry)
Department of Defense	• Defense Industrial Base

[95] Department of Homeland Security (DHS). *The National Strategy To Secure Cyberspace*. February 2003. (Page 16)

Appendix D: Combat Power Matrix (CPM)

Parts 1 & 2 contain a large version of the CPM, which must be combined to complete the matrix. Part 3 is a single page version which is easier viewed when printed.

Seven Rings of Combat Power (Part 1)

MIDLIFE Elements of National Power

	Leadership	Information Systems	Finance
Military	Military Commanders, National Level Military Headquarters, National Leaders (President, Prime Minister, Congress, Parliament), National Security Advisors, COCOM Commanders, CEOs of Military Industrial Base Corporations, Terrorist Organization Leadership, Military Support Corporations	Command and Control Systems, Critical Military Communications Systems and Networks, ISR Systems, Logistics Systems, Critical Informational Systems of Military Industrial Base Corporations, Commercial Communications Systems	Military Budgeting & Programming, Congressional Budgeting, Pay Role, Finance and Accounting Organizations, Contract Records, Financial Systems of Military Industrial Base Corporations, Foreign Military Sales, E-Commerce Systems
Information	Leadership of critical information organizations (News Headquarters, Government Public Affairs, Information Bureau, Information Minister, Major ISP Headquarters, Television & Radio Studios)	Government and Public Records (paper & Binary), Data Storage Systems, Archives, Back-Ups, Commercial Informational Web Systems, Network Architecture Records	Bank Account Records, Individual Loan Records, Escrow Accounts, Internet Banking Systems, Tax Revenue Records, Mortgage Records
Diplomacy	President or Prime Minister, Ambassadors, Diplomatic Liaisons, State Level Diplomats, Secretary of International Affairs, Attachés	Passports &and its Registration Systems, Green Cards and its Registration Systems, Work Permits and its Registration Systems , Visas and its Registration Systems, Foreign Visitor Systems & Data, State Department Messaging Systems	Foreign Debt, International Loans, Tariffs, Trade Restrictions, International Aide, Trade Agreements, Foreign Military Sales
Legal	National Level Court, Supreme Court, Justice Department Secretary, National Level Appeals Courts, National Circuit Courts, National Level Law Enforcement, Attorney Generals, Congress or Parliament, Regulatory Agencies	Legal Libraries, Court Records, Dockets, Jury Lists, Conviction Records, Criminal Records, Fingerprint & DNA Databases, INTERPOL & National Law Enforcement Communication Systems, Firearms Registration Records, Drivers License, Birth Certificates/Records, Marriage & Divorce Records, CCTV Camera Systems	Loan Records, Mortgage Records, Stock Ownership Records, Bond Records, Tariff Records, Import & Export Records, Tax Records, Records of Fines, Security Exchange Commission Records, Contract Records
Intelligence	National Intelligence Agencies (Military & Civilian), Intelligence Advisors to National Leadership	ISR Systems/Platforms, Intelligence Networks, ELINT Systems, Mapping Databases & Systems, Targeting Systems, Tasking Systems	Budgeting & Finance, Intelligence Disbursement Records, Contract Records
Finance	Treasury Department Secretary, Federal Reserve Chairman & Board, Chief of National Banking Structure, Mint Chairman	Bank Account Database Systems, Loan Database Systems, Internet Banking Systems, ATM Networks, Tax Revenue Systems, International Banking Network, Currency Exchanges, Credit Records, Investment Records	Bond Ratings, Currency Valuation, Stock Valuations
Economic	Commerce Department Secretary, Chiefs of Primary Stock Exchanges and Commodities Markets, CEOs of Major Corporations (DOW Top 30, or Military Industrial Base CEOs), Fuel Corporation CEOs, Congress or Parliament	Stock Exchange Systems, Commodity Market Systems, Security Exchange Commission Systems, Trade Records (Quotas & Restrictions), Security Exchange Commission Records, Credit Records	Stock Exchange, Commodity Markets, Security Exchange Commission, Loan Institutions

Seven Rings of Combat Power (Part 2)

MIDLIFE Elements of National Power

	System Essentials	Infrastructure	Population	Fielded Forces
Military	Information, Fuel, Oil, Electricity, Food, Water, Spare Parts, Ammunition, Raw Materials	Air Fields, Ports, Command and Control Facilities, Armories, Fuel Depots, Rail Heads, Railroads, Highways, Roads, Radio & SATCOM Facilities/Antennas, Telephone Systems, Power Generation and Distribution Facilities, Alert Warning Systems, Infrastructure of Military Industrial Base Corporations	Reserve Forces, Draft Age Population, Employees of Military Industrial Base Corporations, DoD Civilians, DoD Contractors, General Population	All Uniformed Military Forces, Aircraft, Ships, Vehicles, Spacecraft, Cybersystems
Information	Information, Electricity, Food, Water	Data Storage and Processing Facilities (Commercial & Government), IP Tier1 and Tier2 Facilities, Trunk Lines, Microwave, Satellite, Telephone Systems, Libraries, TV & Radio Stations, News Papers & Magazine Facilities, Civil Defense Alarms	Bloggers, Commercial Web System Employees, Neighborhood Watch Volunteers, General Population, Journalists, News Casters	Information Technology Personnel, Public Affairs, Combat Camera, Weapon Systems Video Personnel, ELINT Resources & Personnel, Satellite Operators
Diplomacy	Information, Electricity, Food, Water	Embassies, Consulates, Department of State Facilities, Capitol Building, White House	Curriers, Diplomatic Envoys, Staffs At Diplomatic Facilities, General Population	POLMIL Officers, International Affairs Specialists, Foreign Area Officers, Attachés, COCOM Commanders
Legal	Information, Electricity, Food, Water	Court Buildings, Police Stations, Law Enforcement Facilities & Headquarters, Prisons and Jails, CCTV Cameras, Radio Repeaters, Police Helicopters, Hangers, Boats & Docks	Congressmen, Judges, Lawyers, Police, Legal Support Staff, Port Authority, Border Patrol, FBI, DEA, ATF, TSA, General Population	Provost Marshal, Judge Advocate General, Military Special Investigation, Security Forces, Military Law Enforcement, Shore Patrol, Military Port Authority
Intelligence	Information, Electricity, Food, Water	Radio & SATCOM Facilities/Antennas, ELINT Facilities, Intelligence Facilities, Cryptographic Facilities, Collection Facilities, Imaging Facilities, Private Facilities	Private Intelligence Corporation Staff (Satellite Imagery & Data Miners), General Population	Military Intelligence Officers, Counter Intelligence Officers, HUMINT Officers, Annalists, ELINT Personnel & Resources, ISR Platforms & Operators (Aircraft, Satellites & Cyber)
Finance	Information, Electricity, Food, Water	Bank and Treasury Buildings, National Reserve, Mint Facilities	Auditors, Bank Staff, Accountants, Tax Revenue Staff, General Population, Currency Curriers	Accounting and Finance Officers, Contracting Officers, Currency Curriers
Economic	Information, Electricity, Food, Water, Fuel, Oil, Raw Materials	Raw Materials Facilities, Railroads, Highways, Critical Manufacturing Facilities, Distribution Centers	Stock Exchanges Staff, Commodities Markets Staff, Raw Materials Support Facilities Employees, Critical Manufacturing Facilities Employees and General Population	Restricted Material Control Office, Foreign Military Sales, Acquisition Officers

Seven Rings of Combat Power

MIDLIFE Elements of National Power

	Leadership	Information Systems	Finance	System Essentials	Infrastructure	Population	Fielded Forces
Military	Military Commanders, National Level Military Headquarters, National Leaders (President, Prime Minister, Congress, Parliament), National Security Advisors, COCOM Commanders, CEOs of Military Industrial Base Corporations, Terrorist Organization Leadership, Military Support Corporations	Command and Control Systems, Critical Military Communications Systems and Networks, ISR Systems, Logistics Systems, Critical Informational Systems of Military Industrial Base Corporations, Commercial Communications Systems	Military Budgeting & Programming, Congressional Budgeting, Pay Role, Finance and Accounting Organizations, Contract Records, Financial Systems of Military Industrial Base Corporations, Foreign Military Sales, E-Commerce Systems	Information, Fuel, Oil, Electricity, Food, Water, Spare Parts, Ammunition, Raw Materials	Air Fields, Ports, Command and Control Facilities, Armories, Fuel Depots, Rail Heads, Railroads, Highways, Roads, Radio & SATCOM Facilities/Antennas, Telephone Systems, Power Generation and Distribution Facilities, Alert Warning Systems, Infrastructure of Military Industrial Base Corporations	Reserve Forces, Draft Age Population, Employees of Military Industrial Base Corporations, DoD Civilians, DoD Contractors, General Population	All Uniformed Military Forces, Aircraft, Ships, Vehicles, Spacecraft, Cybersystems
Information	Leadership of critical information organizations (News Headquarters, Government Public Affairs, Information Bureau, Information Minister, Major ISP Headquarters, Television & Radio Studios)	Government and Public Records (paper & Binary), Data Storage Systems, Archives, Back-Ups, Commercial Informational Web Systems, Network Architecture Records	Bank Account Records, Individual Loan Records, Escrow Accounts, Internet Banking Systems, Tax Revenue Records, Mortgage Records	Information, Electricity, Food, Water	Data Storage and Processing Facilities (Commercial & Government), IP Tier1 and Tier2 Facilities, Trunk Lines, Microwave, Satellite, Telephone Systems, Libraries, TV & Radio Stations, News Papers & Magazine Facilities, Civil Defense Alarms	Bloggers, Commercial Web System Employees, Neighborhood Watch Volunteers, General Population, Journalists, News Casters	Information Technology Personnel, Public Affairs, Combat Camera, Weapon Systems Video Personnel, ELINT Resources & Personnel, Satellite Operators
Diplomacy	President or Prime Minister, Ambassadors, Diplomatic Liaisons, State Level Diplomats, Secretary of International Affairs, Attachés	Passports &and its Registration Systems, Green Cards and its Registration Systems, Work Permits and its Registration Systems , Visas and its Registration Systems, Foreign Visitor Systems & Data, State Department Messaging Systems	Foreign Debt, International Loans, Tariffs, Trade Restrictions, International Aide, Trade Agreements, Foreign Military Sales	Information, Electricity, Food, Water	Embassies, Consulates, Department of State Facilities, Capitol Building, White House	Curriers, Diplomatic Envoys, Staffs At Diplomatic Facilities, General Population	POLMIL Officers, International Affairs Specialists, Foreign Area Officers, Attachés, COCOM Commanders
Legal	National Level Court, Supreme Court, Justice Department Secretary, National Level Appeals Courts, National Circuit Courts, National Level Law Enforcement, Attorney Generals, Congress or Parliament, Regulatory Agencies	Legal Libraries, Court Records, Dockets, Jury Lists, Conviction Records, Criminal Records, Fingerprint & DNA Databases, INTERPOL & National Law Enforcement Communication Systems, Firearms Registration Records, Drivers License, Birth Certificates/Records, Marriage & Divorce Records, CCTV Camera Systems	Loan Records, Mortgage Records, Stock Ownership Records, Bond Records, Tariff Records, Import & Export Records, Tax Records, Records of Fines, Security Exchange Commission Records, Contract Records	Information, Electricity, Food, Water	Court Buildings, Police Stations, Law Enforcement Facilities & Headquarters, Prisons and Jails, CCTV Cameras, Radio Repeaters, Police Helicopters, Hangers, Boats & Docks	Congressmen, Judges, Lawyers, Police, Legal Support Staff, Port Authority, Border Patrol, FBI, DEA, ATF, TSA, General Population	Provost Marshal, Judge Advocate General, Military Special Investigation, Security Forces, Military Law Enforcement, Shore Patrol, Military Port Authority
Intelligence	National Intelligence Agencies (Military & Civilian), Intelligence Advisors to National Leadership	ISR Systems/Platforms, Intelligence Networks, ELINT Systems, Mapping Databases & Systems, Targeting Systems, Tasking Systems	Budgeting & Finance, Intelligence Disbursement Records, Contract Records	Information, Electricity, Food, Water	Radio & SATCOM Facilities/Antennas, ELINT Facilities, Intelligence Facilities, Cryptographic Facilities, Collection Facilities, Imaging Facilities, Private Facilities	Private Intelligence Corporation Staff (Satellite Imagery & Data Miners), General Population	Military Intelligence Officers, Counter Intelligence Officers, HUMINT Officers, Annalists, ELINT Personnel & Resources, ISR Platforms & Operators (Aircraft, Satellites & Cyber)
Finance	Treasury Department Secretary, Federal Reserve Chairman & Board, Chief of National Banking Structure, Mint Chairman	Bank Account Database Systems, Loan Database Systems, Internet Banking Systems, ATM Networks, Tax Revenue Systems, International Banking Network, Currency Exchanges, Credit Records, Investment Records	Bond Ratings, Currency Valuation, Stock Valuations	Information, Electricity, Food, Water	Bank and Treasury Buildings, National Reserve, Mint Facilities	Auditors, Bank Staff, Accountants, Tax Revenue Staff, General Population, Currency Curriers	Accounting and Finance Officers, Contracting Officers, Currency Curriers
Economic	Commerce Department Secretary, Chiefs of Primary Stock Exchanges and Commodities Markets, CEOs of Major Corporations (DOW Top 30, or Military Industrial Base CEOs), Fuel Corporation CEOs, Congress or Parliament	Stock Exchange Systems, Commodity Market Systems, Security Exchange Commission Systems, Trade Records (Quotas & Restrictions), Security Exchange Commission Records, Credit Records	Stock Exchange, Commodity Markets, Security Exchange Commission, Loan Institutions	Information, Electricity, Food, Water, Fuel, Oil, Raw Materials	Raw Materials Facilities, Railroads, Highways, Critical Manufacturing Facilities, Distribution Centers	Stock Exchanges Staff, Commodities Markets Staff, Raw Materials Support Facilities Employees, Critical Manufacturing Facilities Employees and General Population	Restricted Material Control Office, Foreign Military Sales, Acquisition Officers

This Page Intentionally Left Blank

Bibliography

8th Air Force (8AF). "Air Force NetOps Transformation Migration Plan." Presentation to Air Force Major Commands. 10 March 2006.

Air Force Communications Agency (AFCA). "Active Directory (AD) Program Management Review." Presentation to Air Force Major Commands. 17 April 2006.

Allard, Kenneth. *Command, Control, and the Common Defense* (Revised Edition). Washington DC: National Defense University. 1996.

American Heritage® Dictionary (AHD) of the English Language, Fourth Edition. Copyright 2002, 2000 by Houghton Mifflin Company.

Arguilla, John and David Ronfeldt. Rand Corporation, International Policy Department. "Cyberwar is coming." 1993 http://gopher.well.sf.us:70/0/Military/cyberwar.

Bay, Austin, "The DIME Ballet", *Strategy Page: On Point*. 24 May 2005 http://www.strategypage.com/on_point/2005524.aspx.

Bush, George W. President of the United States. *Executive Order 13286: Amendment of Executive Orders, and Other Actions, in Connection With the Transfer of Certain Functions to the Secretary of Homeland Security.* Federal Register 5 March 2003, Volume 68, Number 43, Presidential Documents, Pages 10619-10620. 28 February 2003.

Bush, George W. President of the United States. *Executive Order 13385: Continuance of Certain Federal Advisory Committees and Amendments to and Revocation of Other Executive Orders.* Federal Register 4 October 2005, Volume 70, Number 191, Presidential Documents, Pages 57987-57991. 29 September 2005.

Bush, George W. President of the United States. *Critical Infrastructure Identification, Prioritization, and Protection.* Homeland Security Presidential Directive-7. 17 December 2003.

Combat Information Transport System (CITS) Program Office. "CITS Block 30 MAJCOM AO Update." Presentation to Air Force Major Command CITS Action Officers (AO). 28 September 2006.

Defense Finance and Accounting Service (DFAS). *Defense Finance and Accounting Service, About DFAS: Our History*. http://www.dfas.mil/about/OurHistory.html.

Defense Information Systems Agency (DISA). *Defense Information Systems Agency: History of DISA*. http://www.disa.mil/main/about/history.html.

Delio, Michelle. "It's (Cyber) War: China vs. U.S.," *Wired News*. 30 April 2001 http://www.wired.com/news/politics/0,43437-1.html?tw=wn_story_page_next1.

Department of Homeland Security (DHS). *National Response Plan*. December 2004.

Department of Homeland Security (DHS). *The National Strategy To Secure Cyberspace*. February 2003.

Department of State (DoS). *The National Security Act*, http://www.state.gov/r/pa/ho/time/cwr/17603.htm.

Dunnigan, James. "China in a Cyberwar Arms Race," Strategy Page :Dirty Little Secrets. 8 March 2005 http://www.strategypage.com/dls/articles/2005389.asp.

Forest, James J.F., Ph.D. "Teaching Counterterrorism in the 21st Century," Presentation to facility and students, United States Military Academy, Combating Terrorism Center, West Point. July 2005.

"Frank Abagnale," http://en.wikipedia.org/wiki/Frank_Abagnale.

Google, www.google.com.

The Information Warfare Site (IWS). "Overview of National Security Structure." 2006, http://www.iwar.org.uk/military/resources/us/national-security-structure.htm.

Joint Chiefs of Staff (JCS). *Joint Publication 0-2: Unified Action Armed Forces (UNAAF).* 10 July 2001.

Joint Chiefs of Staff (JCS). *Joint Publication 1, Joint Warfare of the Armed Forces of the United States*. 14 November 2000.

Judge Advocate General's Corps (JAGCNET), United States Army. "Chapter 24: National Security Structure and Strategy," https://www.jagcnet.army.mil/JAGCNETInternet/Homepages/AC/CLAMO-Public.nsf/0/1af4860452f962c085256a490049856f/$FILE/Chapter%2024%20-%20National%20Security%20Structure.htm. 13 October 2006.

Kenyon, Henry S. "Task Force Explores New Military Frontier," *Signal: Armed Forces Communications and Electronics Association (AFCEA) Journal*, 55-57 (October 2006).

Libicki, Martin. *What is Information Warfare?* National Defense University, Institute for National Strategic Studies, Advanced Concepts and Information Strategy, August 1995.

Margulius, David L. "Crisis Management 101: Preparing for disaster means preparing yourself to act decisively when little is known," *InfoWorld*, (8 March 2007).

Miguel, Luis A. "Virtual Jihad: The Internet as the Ideal Terrorism Recruiting Tool," *Scientific American*, Pages 18-21 (January 2006).

Moon, David B. "Cyber-Herding: Exploiting Islamic Extremists use of the Internet," Naval Postgraduate School, Department of Defense Analysis, Joint Information Operations Student.

Mountain Runner: Public diplomacy, unrestricted warfare, privatization of force, and civil-military relations. *Of Information Operations, DIME, and America's Ambassadors.* 29 August 2006 http://mountainrunner.us/2006/08/of_information_.html.

National Infrastructure Advisory Council. *Meeting Minutes, Convergence of Physical and Cyber Technologies and Related Security Management Challenges Working Group*. 11 April 2006.

"The National Strategy For Combating Terrorism." September 2006.

Pace, Peter, Chairman, Joint Chiefs of Staff. Memorandum of 2006 Joint Professional Military Education (JPME) Special Areas of Emphasis (SAEs). Pentagon, Washington DC 17 January 2006.

Puglisi, Matthew and others. *A Common Interagency Regional Framework*. Joint Forces Staff College, Joint and Combined Warfighting School, Class 7-01, November 2006.

Reagan, Ronald. President of the United States. *Executive Order 12333: United States Intelligence Activities.* Federal Register 8 December 1981, Federal Registry Page 46 FR 59941. 4 December 1981.

Reagan, Ronald. President of the United States, Washington DC. "Defense Reorganization – Message From The President Of The United States; Transmitting His Views On The Future Structure And Organization Of Our Defense Establishment And The Legislative Steps That Should Be Taken To Improve Defense Reforms". The 99th Congress, 2nd Session, House Document: 99-209. 28 April 1986.

Rogin, Josh. "DoD Issues New Policy On Electronic Warfare: Policy Could Be The First Of Many For Dealing With Cyberthreats From Chinese Hackers," *Federal Computer Weekly (FCW.COM)* (26 February 2007). http://www.fcw.com/article97749-02-26-07-Print.

Ros-Lehtinen Ms. and other Representatives. *Global Internet Freedom Act*. House of Representative Bill 4741, 109th Congress, Second Session. 14 February 2006.

Sellin, Lawrence, Ph.D. "Outside View: Short-changing Iraq," *Spacewar: Your World at War*. Washington (UPI) 18 December 2006 http://www.spacewar.com/reports/outside_view_short-changing_iraq_999.html.

Sky Control: Aviation and Aerospace News, "Predator UAV Kills Terrorists", 28 April 2006 http://www.skycontrol.net/uav/predator-uav-kills-terrorists.

Smith, Russell J. "Developing an Air Campaign Strategy," *Air & Space Power Journal*. 23 November 1999 http://www.airpower.maxwell.af.mil/airchronicles/cc/smith.html.

Taylor, Phillip M., Professor, Institute of Communications Studies, University of Leeds, United Kingdom. "Concepts of Information Warfare." Presentation Slide Lecture to the Norwegian Staff Defense College students and faculty. Norwegian Staff Defense College, Oslo Norway. November 2006. http://ics.leeds.ac.uk/papers/pmt/exhibits/2669/Oslo06.ppt

"Torpedo Miss" *Scientific American*, Page 16 (November 2005).

Unified Combatant Command (COCOM). http://en.wikipedia.org/wiki/Unified_Combatant_Command.

United States Congress. Department of Defense Reorganization Act of 1958. Public Law 85-599, 85th Congress, second session.

United States Congress. Goldwater-Nichols Department of Defense Reorganization Act of 1986. Public Law 99-433, 99th Congress, second session.

United States Congress. National Security Act of 1947. Public Law No. 80-253, 80th Congress, first session.

United States Congress. United States Code, Title 10 – Armed Forces, Subtitle A – General Military Law, Part I – Organization And General Military Powers, Chapter 6 – Combatant Commands.

United States Congress. United States Code, Title 50 – War And National Defense.

United States Strategic Command (USSTRATCOM). *Joint Concept of Operations for Global Information Grid NetOps* (Version 3). 4 August 2006.

Warden, John A. *Air Theory for the Twenty-first Century*. September 1995 http://www.airpower.maxwell.af.mil/airchronicles/battle/chp4.html.

Wedgewood, Ruth. Yale University Professor. Panel on Internet and Public International Law. *Meeting Minutes: Effects of the Information Revolution on Public International Law, 2000*. http://www.uky.edu/Law/aals-int/y2k.htm.

Wynne, Michael W., Secretary of the Air Force. "Cyberspace Dominance, the information Mosaic and Precision Strike." Address to the Precision Strike Association, John Hopkins University, Baltimore MD. 19 October 2006.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
30-06-2007	Graduate Research Project	May 2007 – June 2007

4. TITLE AND SUBTITLE

Cyberspace as a Theater of Conflict:
Federal Law, National Strategy and the Departments
Of Defense and Homeland Security

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Arwood, Sam, Major, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/IC4/ENG/07-01

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Joint Staff/J6
Attn: Lt Col Jodine K. Tooke
Pentagon, Washington D.C. 20318

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The research is divided into three distinct parts, each linked and dependent upon one another. First is a review and an evaluation of the legal relationships between the Combatant Commanders, the Services, and DoD Agencies with respect to cyberspace. What roles are tasked to each and what limitations are in place based upon those assigned roles. And are any of these current relationships at odds with federal law? Second, linked National Strategy to a Service's targeting strategy via the Effects Based Planning process. This demonstrates the ability to link target selection to the elements of national power as well as identify possible desired effects based upon adversary target selection. Last, is an evaluation of military cyberspace activities and responsibilities based upon the conclusions and observations of the first two sections. Included in this evaluation is a brief look at cyberspace activities not yet addressed by the DoD but soon to be a responsibility of the Department.

15. SUBJECT TERMS

Cyberspace; Federal Law; Department of Homeland Security; Department of Defense; Nat-A; Net-D; Net-O; Net-M; Net-CI; First Amendment; Combat Power matrix; seven rings of combat power; MIDLIFE; DIME.

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. Robert F. Mills, Professor, USAF (ENG)
U	U	U	UU	120	19b. TELEPHONE NUMBER *(Include area code)* (937) 255-3636, ext 4718 email: robert.mills@AFIT.edu

Reset

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18