REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
31 Oct 2008	FINAL	

4. TITLE AND SUBTITLE
Words Mean Things: The Case for Information System Attack and Control System Attack

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Lt Col Mark J. Matsushima, USAF

Paper Advisor (if Any): CAPT Stephanie A. Helm

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

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

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

War fighters in the United States Department of Defense (DOD) need a more precise, focused lexicon and a common understanding of "cyberspace" related terminology; the term computer network attack (CNA) is too broad. DOD should incorporate two new terms into the DOD information operations (IO) lexicon: Information Systems Attack (ISA) and Control System Attack (CSA) as CNA subcategories. These two new terms will help the oint force commander (JFC) and others in DOD precisely define effects and determine command relationships than the current overarching term, CNA. This paper begins with a discussion and analysis of current CNA-related definitions and builds the case for incorporating two new terms, ISA and CSA. It also covers a new term, "cyberspace", and suggests that a more restrictive definition of the term issued by the Deputy Secretary of Defense (DepSecDef) is more appropriate than a broader and less precise definition. Second, this paper gives a brief overview of CNA effects as outlined by Lt Col Russell Mathers in his JMO thesis, Cyberspace Coercion in Phase 0/1: How to Deter Armed Conflict, expands on his thesis, and also builds the case that operations in cyberspace are no different than operations conducted in any other domain. The third section discusses command relationships for ISA and CSA. United States Strategic Command (USSTRATCOM) should conduct ISA in support geographic Combatant commands (GCCs) via forces TACON to USSTRATCOM, but GCCs should exercise TACON over forces conducting CSA.

15. SUBJECT TERMS
Computer Network Attack, Cyberspace

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Chairman, JMO Dept
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		24	19b. TELEPHONE NUMBER *(include area code)* 401-841-3556

Standard Form 298 (Rev. 8-98)

NAVAL WAR COLLEGE
Newport, R.I.

WORDS MEAN THINGS: THE CASE FOR INFORMATION SYSTEM ATTACK AND CONTROL SYSTEM ATTACK

By

Mark J Matsushima

Lieutenant Colonel, United States Air Force

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature:_____

31 October 2008

Contents

List of Tables

Abstract

This paper introduces two new terms into the Department of Defense (DoD) Information Operations (IO) lexicon: Information Systems Attack (ISA) and Control Systems Attack (CSA) as subcategories of Computer Network Attack (CNA). These two new terms will help the joint force commander and others in DoD more precisely define effects and determine command relationships more clearly than the current overarching term, "computer network attack" (CNA).

This paper begins with a discussion and analysis of current CNA-related definitions and builds a case for incorporating two new terms, ISA and CSA. It also covers a new term, "cyberspace", and suggests that a more restrictive definition of the term issued by the Deputy Secretary of Defense is more appropriate than previous, broader definitions.

Next, this paper gives a brief overview of CNA effects as outlined by Lt Col Russell Mathers in his thesis, *Cyberspace Coercion in Phase 0/1: How to Deter Armed Conflict*, and also builds the case that operations in cyberspace are no different than operations conducted in any other domain; they are simply another method of achieving effects.

Finally, this paper analyzes possible command relationships for ISA and CSA, including the proposition that in conducting information system attacks, United States Strategic Command should provide support via TACON forces to another Combatant commander or subordinate JFC, and when conducting control system attacks the geographic JFC should exercise TACON over CSA forces.

INTRODUCTION

War fighters in the United States Department of Defense (DOD) need a more precise, focused lexicon and a common understanding of "cyberspace" related terminology. The term computer network attack (CNA) is too broad. DOD should incorporate two new terms into the DOD information operations (IO) lexicon: Information Systems Attack (ISA) and Control System Attack (CSA) as CNA subcategories. These two new terms will help the joint force commander (JFC) and others in DOD precisely define effects and determine command relationships than the current overarching term, CNA. Some believe that DOD needs to broaden its collective thinking, and embrace a far more encompassing definition of cyberspace; however, such an approach creates a wicked problem for the JFC.

First, this paper begins with a discussion and analysis of current CNA-related definitions and builds the case for incorporating two new terms, ISA and CSA. It also covers a new term, "cyberspace", and suggests that a more restrictive definition of the term issued by the Deputy Secretary of Defense (DepSecDef) is more appropriate than a broader and less precise definition. Second, this paper gives a brief overview of CNA effects as outlined by Lt Col Russell Mathers in his JMO thesis, *Cyberspace Coercion in Phase 0/1: How to Deter Armed Conflict*, expands on his thesis, and also builds the case that operations in cyberspace are no different than operations conducted in any other domain. The third section discusses command relationships for ISA and CSA. United States Strategic Command (USSTRATCOM) should conduct ISA in support geographic Combatant commands (GCCs) via forces TACON to USSTRATCOM, but GCCs should exercise TACON over forces conducting CSA.

CYBERSPACE, CNA AND NEW DEFINITIONS

JFC planners must know the definitions of cyberspace, CNA, and related definitions in order to understand the "state of play" in this emerging discipline. The definitions of CNA and cyberspace are fundamental building blocks for defining command relationships, drawing areas of responsibility---exercising operational art. As computer technology evolves at an exponential rate, doctrine and definitions struggle to keep pace.

Some believe modern technology is transformational enough to change the accepted terms and definitions. They speak of "cyber operations" as an emerging type of unique military operation. Adherents of this school of thought suggest that the nation might need a "strategic cyber war fighting force", because cyberspace is an actual, physical domain.[i]

Others are more conservative, and believe that DOD should first build upon an established framework, modifying existing definitions as necessary. They believe that operations in cyberspace are conducted as they are in other domains. The first group of thinkers are revolutionary, the second evolutionary. This paper advocates the latter approach. In planning definitions are foundational. Without a common lexicon, the JFC, his superiors and his staff could well "talk past one another."

To understand why the terms ISA and CSA add value as subsets of CNA, it is necessary to understand the larger context and the definitional debate surrounding cyberspace. See Table 1 for the complete listing, noting that the term "cyberspace" is not currently defined in joint doctrine, while CNA is defined. First, let us examine the term cyberspace, and discuss how the term relates to CNA. The National Military Strategy for Cyberspace Operations (NMS-CO) defines cyberspace as "a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and

associated infrastructures."[ii] This expansive definition includes the notion that cyberspace is a domain on par with air, land, sea, and space, and that the domain is virtually boundless, spanning the entire electromagnetic spectrum. Using the NMS-CO definition, Mathers logically concludes that cyberspace operations include things like signals intelligence collection, control of the Global Positioning System satellite constellation, as well as computer network attack. In his paper, he describes all of those things as "cyberspace operations." One author summarized the NMS-CO definition of cyberspace by stating, "cyberspace can occur within the other physical domains, (and) should be recognized as a physical domain, occurring any place where the electromagnetic spectrum and electronic systems interlink."[iii] Thus, to someone who accepts the NMS-CO definition, arguing about CNA and subcategories misses the point. These thinkers feel the argument (and related discussions about COCOM missions) is much broader, deeper and fundamental.

War-fighting JFCs need more precise language to fight in this emerging domain, not broad definitions. More recently (and after Mather's paper), the DepSecDef issued a more focused definition of cyberspace, calling it "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications, networks, computer systems, and embedded processors and controllers."[iv] This definition, written on 12 May 2008, acknowledges cyberspace as a domain, but focuses on computers, without mention of the electromagnetic spectrum or any functions associated therein. Therefore, someone who supports this definition would likely contend that current doctrinal definitions of CNO and CNA are a solid foundation for understanding at least a portion of the military mission in

cyberspace. The JFC can build on this definition better than one which begins, "A domain *characterized by*…"

How could the NMS-CO definition of cyberspace affect a joint force commander? The NMS-CO definition is broad and indeed, revolutionary. It implies that cyberspace is a global, encompassing domain that crosses geographic boundaries. Thus, an AEGIS destroyer conducting surveillance, a soldier electronically jamming improvised electronic explosive device detonators, and a computer operator collecting intelligence against Al Qaida operatives in internet cafes are all conducting "cyberspace operations" according to the NMS-CO. All the other domains (air, land, sea, and space) have an executive agent or service whose primary mission is to control that domain. A service or agency acting as the supported commander—if one is ever codified--in the cyberspace domain has a worldwide area of responsibility that extends from the telemetry of satellites in geosynchronous orbit, to simplest Morse code transmission. The operational implications (such as drawing geographical versus functional areas of responsibility) of accepting the broad definition could be the topic of another thesis. However, one could infer that a JFC conducting electronic jamming or naval forces communicating via satellite would be operating in another command's area of operations. This could interfere with a JFC's ability to act and shape his geographically defined operating environment, if such actions impacted an aspect of the electromagnetic spectrum---from zero to infinity Hz.

Contrarily, and perhaps to the benefit of JFCs engaging in two major theater wars and the global war on terrorism, the DepSecDef definition is more conservative and builds upon the accepted definitions of Computer Network Operations (CNO, see glossary). Accepting this less transformational definition does not require a re-thinking of worldwide command

relationships in the cyberspace domain. The advantage to this more conservative approach is that it allows DOD to incorporate new ideas in a rapidly changing technical arena while building on an already agreed upon definitional framework. DOD should build on current definitions and understanding, modifying them to fit new technologies.

What if cyberspace is accepted as a domain, as described by both the NMS-CO and DepSecDef? This simply means that military operational functions[v] as well as a wide range of other activities such as commerce, diplomacy, crime, etc., occur in cyberspace. The military mission is simply another activity therein. If one accepts this premise, one can logically conclude that traditional missions and military tasks occur in this domain, and many currently accepted joint definitions of those missions and tasks apply. In other words, the DepSecDef definition acknowledges the existence of a new domain, but strongly implies the accepted definition of CNO is sufficient to understand how the military and the JFC should operate within the new domain. Thus, the JFC staff can move out, organize and execute with the understanding that CNA provides another tool to achieve assigned end states. Given the more focused definition of cyberspace, the understanding that is it a domain in which a wide range of activities occur, why does DOD need new terminology (ISA and CSA) as subcategories of CNA?

The term CNA is not too limiting; it is *too broad*---further subcategories are needed to allow JFCs to properly discuss operations. The reason for this is simple; some CNA targets information, while other CNA targets computers which control other systems, often to create physical or kinetic effects. Saying that one wishes to conduct CNA does not lead to an intuitive understanding of required skill sets, technologies, force structure, rules of engagement, or C2 functions. The term is more specific than “cyberspace operation”, but

still lacks precision. A JFC has different planning considerations if he contemplates deleting information on a hard drive, as opposed to hacking into a power grid to shut down electric power---yet both are CNAs. CNA is broadly defined by DOD as "actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers themselves."[vi] By this definition, Mathers correctly points out that CNA includes everything from draining funds from adversary bank accounts to "hacking" websites to accessing adversary networks to open a dam's floodgates.[vii] There is a solution. In his article *What You Should Know About Attacking Computer Networks*, Tim Gibson points out that there are two types of computer networks: information systems and infrastructure-control systems.[viii] He then describes information systems as systems which control no physical assets, such as "databases, reservation system, documents, web pages…"[ix] On the other hand, infrastructure control systems interact with the physical world, and include things such as "system controllers at power, chemical, or water plants, automated air defense fire-control systems, and robots on manufacturing lines."[x] Thus, here are two proposed new categories of CNA:

1. Information System Attack (ISA): A type of computer network attack intended to disrupt, corrupt, deny, degrade, or destroy information residing in, or transiting cyberspace where the data itself is the target. ISA does not involve the use of force. Examples include denial of service attacks, deleting files, altering web pages.

2. Control System Attack (CSA): A type of computer network attack conducted through cyberspace intended to affect other networked objects, including but not limited to supervisory control and data acquisition systems, surveillance, and kinetic weapons. A CSA generally creates destruction and is considered a use of force. Examples include disrupting, damaging, or affecting fire control commands to weapons, military C2, and other capabilities in the physical world.

To summarize: first, from a JFC perspective, the term cyberspace should be defined using the more specific language issued by the DepSecDef. To a JFC trying to conduct operational

art, the NMS-CO definition complicates matters and does not necessarily add clarity in the planning and execution of operations. Second, the term computer network attack is relevant but too broad. This paper proposes creating new subcategories of CNA----ISA and CSA-- in order to better describe the actual mission the JFC wishes to conduct. In short, the DOD should develop specific CNA definitions as opposed to adopting a "cyber-revolutionary" approach.

OPERATIONS IN CYBERSPACE ARE TRADITIONAL MILITARY OPERATIONS

The JFC should understand that CNA provides him "ways" to achieve traditional military "means". In other words, globally networked microprocessors are new but the methods (means) to operational "ends" are not. Lt Col Mathers presents the JFC with CNA "ways" to coerce the enemy prior to Phase II operations. His thesis abstract reads (in part), "Cyberspace is a war fighting domain and can be used by joint force commanders in Phase 0 (Shape) and Phase 1 (Deter) of their operations to prevent escalation to armed conflict." He adds, "…China and Russia have used cyberspace operations to coerce their adversaries and place themselves in a position of strength to deter their future adversaries in space." In his paper, Mathers also describes six examples of "cyberspace operations" to achieve JFC ends.[xi] Arguably, there are no "cyberspace operations", that is, unique operations which do not exist in other domains. Rather, there are "operations in cyberspace", and CNA provides the commander with a tool for performing operational functions for which he is already responsible. This is a fine point, but "words matter."

Mather's specific example: ***CNA "Ways"***	***Doctrinal Term which applies or should apply:*** ***CNA "Means"***	***Type of CNA which should apply***
Drain funds from adversary bank accounts, electronic isolation of Estonia by Russia	Strategic Attack	Information System Attack
Fabricating email, false media / internet information attributed to enemy leadership	Strategic Deception	Information System Attack
Altering / deleting content in adversary websites	Counter PSYOP	Information System Attack
Inserting false targets into fire control system	Command and Control Warfare	Control System Attack
Influencing adversary populations through websites	Psychological Operations	Information System Attack
Accessing networks to open a dam's floodgates	Physical Attack	Control System Attack

Table 1: Categorization of Mathers' Cyber Coercion Examples

For a JFC, there are three things to consider in examining this table. First, CNA offers alternative methods (ways) to accomplish his objectives. Second, the JFC needs to specifically define his CNA means as ISA or CSA; the blanket term "operation in cyberspace" or even "computer network attack" is not specific enough. The "CNA ways" column in the table is intended to illustrate the vastly different types of computer network attack. Third, CNA command relationships will depend on the type of CNA the JFC wishes to conduct. The next section of this paper deals with command relationships for ISA or CSA.

COMMAND RELATIONSHIPS FOR ISA

There are several reasons why USSTRATCOM should have TACON of ISA forces---which are simply any forces conducting information system attack---and should provide support to the JFC. USSTRATCOM is task organized for the ISA mission and has ties to the national intelligence community to allow this rapid transition from intelligence preparation to

ISA. Information system attack is a strategic, trans-regional IO mission, and the Unified Command Plan (UCP) tasks USSTRATCOM with both.

USSTRATCOM is structured to conduct ISA, because of their Joint Functional Component Command (JFCC) structure (see appendix for command wiring diagram[xii]). The Joint Task Force for Global Network Operations (JTF-GNO) defends the DOD portion of cyberspace, while the JFCC-Network Warfare (JFCC-NW) conducts CNA (or, as defined herein, ISA). Furthermore, the Director, National Security Agency (DIRNSA) is dual-hatted as the JFCC-NW commander, and his Title 10 ISA forces reside at Fort Meade, co-located with NSA. USSTRATCOM defines network warfare as, "the employment of computer network operations with the intent of denying adversaries the effective use of their own *computers, information systems, and networks*."[xiii] Although the term "network warfare" is not codified in joint doctrine, the definition is almost identical to this paper's definition of information system attack. In sum, JFCC-NW is a standing CNA (ISA) organization under USSTRATCOM. GCCs do not have equivalent standing commands. However, structure in itself does not mean that USSTRATCOM should have TACON of ISA forces.

The JFCC-NW structure builds ties with the national intelligence community---the most compelling reason USSTRATCOM should have TACON of ISA forces. The name "information system attack" even suggests a close association with intelligence data---closer than in the physical world, because ISA affects only data. Although DIRNSA is dual-hatted as the commander, JFCC-NW, as one senior defense official observed, "NSA is where the mother lode of (computer network exploitation) resides. Those are the folks that have been looking at the capability for the longest time."[xiv] Another author reiterated the point, "the most advanced expertise on operating is held by NSA, the DOD intelligence arm that

monitors foreign phone calls, emails, and other communication."[xv] Granted, intelligence collection is not the same as attack; however, if an organization can obtain access to an adversary's information system, it is a simple matter to alter, deny, degrade or disrupt that information. Technically speaking, information system attack is a keystroke away from computer network exploitation; if one can establish root level access to a computer, one can then exploit or attack. However, ISA is still an attack mission.

A JFC, not an intelligence agency, must be the one to command and control ISA. Note the use of the term "attack" although by definition there is no kinetic impact in the physical world. Information system attack could be construed as a war like act although it does not involve the use of force; therefore a military Title 10 organization should exercise TACON of such forces. To illustrate the war-like nature of ISA, Russia allegedly attempted to electronically isolate the Georgian government from its people, using denial of service attacks to disable many Georgian government websites, "making it difficult to inform citizens of import updates…hindering communication in the country."[xvi] The point of this example is that ISA is an extremely disruptive and provocative act, potentially an act of war. As such, a JFC, under Title 10 authority, should be the ISA "trigger puller", not a member of the intelligence community. Why should USSTRATCOM be that JFC, however?

USSTRATCOM should have TACON of ISA forces for two reasons: the UCP and the strategic nature of ISAs. The UCP tasks USSTRATCOM to plan and execute DOD Information Operations---and CNA is a subcomponent thereof---which cross COCOM AOR boundaries.[xvii] The Internet is certainly trans-regional. Joint doctrine further states that USSTRATCOM conducts CNA in support of other combatant commands, as directed.[xviii] ISA is a strategic attack---USSTRATCOM's mission. The DepSecDef, in defining

cyberspace as a domain, elevates ISA to a realm of *national strategy* and interagency policy. For example, the decision to launch a strategic information system attack to drain funds from adversary bank accounts could have serious consequences in the United States. As the head of the Department of Homeland Security cautioned, "Imagine a sophisticated attack on our financial systems that caused them to be paralyzed…with an open internet, you can't guarantee security."[xix] In this type of ISA, the U.S. State Department would probably become involved. According to the Estonian Prime Minister, computers from 75 nations attacked Estonia, and most of those originated from the United States.[xx] The point is that information systems connected to the Internet can quickly involve law enforcement as well as economic interests at home and abroad. USSTRATCOM is postured by virtue of mission and already established JFCC-NW organization to create a standing ISA joint interagency task force, which would be able to react more quickly than one created in a crisis by another JFC. This evidence leads one to believe that the JFC is best served by having USSTRATCOM, with its inherent strategic attack mission and tie to the national intelligence community (and other interagency partners), support the JFC in conducting ISA. However, assigning ISA forces TACON to JFCC-NW has its risks as well as benefits and the risks must be addressed.

A GCC could be concerned with the lack of TACON of ISA forces. The close ties to national intelligence engendered by dual-hatting the DIRNSA and the JFCC-NW commander potentially means that the intelligence organization is doing computer network exploitation and also formally or informally helping determine which targets USSTRATCOM should attack. Indeed, some authors argue that high payoff internet targets are also "intelligence treasure troves", and the decision to attack systems where national intelligence is collected

"must be made objectively by someone who oversees both the operational and intelligence units involved."[xxi] The GCC would most likely disagree---adamantly. War fighters, not intelligence agencies, make intelligence gain / loss decisions. Dual-hatting one officer (DIRNSA, sitting far removed from the point of attack) as the attacker *and* collector could put him in a position to non-concur with his own recommendation. Several organizations, including the U.S. Air Force, point out that the close ties to the national intelligence community can hinder the JTF war fighter in accomplishing his CNA mission. Dr. Lani Kass, a senior Air Force official and former director of that service's Cyberspace Task Force notes that NSA collects signals intelligence, and performs that job very well, but emphasized that they are not a war-fighting organization. She cautions, "Let's not mistake intelligence collection with military operations."[xxii] Some authors go further, and suggest that if the operational authority (JFCC-NW commander) is also the intelligence collector (DIRNSA) the tendency will be to avoid jeopardizing collection activities.[xxiii] While these are valid concerns, USSTRATCOM is still the military authority and the Title 10 trigger puller for "network warfare" or "information system attack" operations---*not* the intelligence community. Dr. Kass' argument is flawed in that regard. However, there could still be issues with USSTRATCOM exercising central authority and C2 via TACON.

LCDR Michael C. Elliot points out that while the USSTRATCOM C2 model puts CNA and CND under one Combatant command, this structure could sub-optimize support to the JFC by introducing national and USSTRATCOM competing objectives, potentially conflicting with the JFC priorities.[xxiv] He is concerned that this arrangement is doctrinally unsound and could lead to a lack of planning, synchronization and priority; and places CNA is a strategic realm, whereas such decisions are local and operational in nature. Joint doctrine

is not silent on this point either. It states that "USSTRATCOM's specific authority and responsibility to coordinate (CNO as an aspect of information operations) across AOR…boundaries *does not diminish* the imperative for other combatant commanders to coordinate, integrate, execute and employ IO."[xxv] In conducting ISA, there is a more compelling case that JFCs are still responsible to coordinate and integrate ISA, but can and should do so with USSTRATCOM in a supporting role via forces TACON to USSTRATCOM. This is because of the standing task organization of JFCC-NW, the trans-regional nature of the Internet, and the need for close association with national intelligence in the conduct of ISA.

Information system attacks are both trans-regional and likely to be strategic in nature. When conducting such attacks, there are ample opportunities for missteps, especially if a JFC is altering Internet content unilaterally. The Internet is a global commons and attacks require de-confliction with CIA, FBI, DoS, DHS and other agencies. Similarly, conducting ISA to "drain funds from bank accounts" needs national and interagency participation in both the virtual and physical realms to be effective. To be most effective, ISA against financial systems would achieve greater success if conducted as an element of an integrated national strategy which leverages the economic and diplomatic instruments of power. In sum then, USSTRATCOM should maintain TACON of units conducting information system attacks. However, this is not the case for control system attacks which target more than information.

COMMAND RELATIONSHIPS FOR CSA

When conducting control system attack, the JFC closest to the attack should have TACON of the attack forces, regardless of their geographic location. In Mathers' example (Table 1) of accessing networks to open a dam's floodgates, CSA is a means to control a

system, in this case the dam's floodgates. It is less relevant that CSA created the flood as opposed to a 2000 pound bomb---the kinetic effect is the one that matters. The local JFC should have TACON of such forces. Control system attacks are not theoretical capabilities---they exist today.

The United States has the capability to use CNA operationally and tactically in support of kinetic operations, or even as an alternative to physical attack. According to former Secretary of the Air Force Michael Wynne, "EC-130 Compass Call communications jamming and information warfare aircraft…penetrate enemy (fire control) computer systems to take control of them, plant false targets, send misleading messages and even manipulate enemy radar sensors."[xxvi] CNA of the future could "well include soldiers and Marines having backpack-borne CNA weapons to create tactical and operational effects on the battlefield."[xxvii] Lt Col Forrest Hare makes the additional point that in many instances, forces operating in the JFC's battle space will have to conduct CNA, because they require line of sight to "radio networks, closed battlefield C2 networks, or operate in the footprint of enemy satellites."[xxviii] In the CNA examples above---both of CSA---the JFC should have C2 of the forces creating the effects. In the first case, the JFACC would exercise TACON over the EC-130 aircraft and crews and in the second the JFLCC would have TACON of the ground forces and their equipment. Why is this?

There are several reasons why the JFC (either the GCC or his subordinate JFC) should exercise TACON of CSA forces. First, the JFC normally has TACON of joint fires, both lethal and nonlethal, in his JOA. Joint Publication 3-09, *Joint Fire Support* indicates that nonlethal fires include "…information operations…that disable the enemy's C2 systems, and disrupt operations."[xxix] In this sentence, the enemy's C2 systems and operations are the

target, not the information resident in cyberspace. Control system attacks, therefore, can and should be construed as nonlethal joint fires, which the JFC normally directs. The second reason is perhaps more compelling: while information system attacks do not create physical destruction, control system attacks can create physical destruction, and thereby constitute a use of force. Within a JOA, the JTF commander should be the one exercising command over kinetic attack forces. As Dr. Milan Vego points out, unity of command is critical, and a failure to create unity of command is "historically a recipe for disaster."[xxx] If anyone other than the JFC creates lethal effects in the JOA, it could hinder unity of effort, and certainly simplicity. At worst it could endanger mission accomplishment. Simply, the commander should be close to theater, and have TACON of those forces creating effects for him where possible. Could USSTRATCOM still employ kinetic force in another COCOM's AOR or JFC's JOA? Yes, but historically this is not the way the US conducts kinetic attacks. Even CONUS-based bombers on global strike missions against CENTCOM targets CHOP to CENTCOM during their mission. There may be a case, however to centralize execution of CSA with USSTRATCOM, so the next section deals with that command relationship.

As discussed, USSTRATCOM should have C2 of ISA forces because of the close ties to the national intelligence community and the strategic nature of *information* system attack. Could the same case be made for *control* system attack? For example, JFCC-NW could have forces in garrison who, by working closely with NSA, are able to develop access to a control system in a JFC's JOA. The target could be strategic in nature, such as a nuclear power plant in a rogue nation. The SecDef might wish to shut the power plant down or create damage to neutralize it. Even in this case, the GCC would have to plan for consequence management, synchronization all other aspects of the operation (information

operations, consequence management, intelligence collection, coordination with local embassies, etc) and should have TACON over forces conducting the single kinetic event, to best synchronize the attack. While it is possible that JFCC-NW could conduct a CSA against a nuclear power plant in a rogue nation, it is more plausible that local SOF forces would be the ones to conduct such a CSA. And, while geographic proximity does not necessitate TACON or unity of command, the principles of war support the position that the local JFC is best served when commanding forces in his JOA.

SUMMARY AND RECOMMENDATIONS

This paper attempts to demonstrate that war fighters need a common lexicon and a common set of "cyber terminology". Rather than broadening the definition of cyberspace in a manner that could impact command relationships across the world, the DoD should accept the more focused definition of cyberspace promulgated by Deputy Secretary of Defense England. Joint force commanders need to be able to precisely and succinctly give planning guidance, request authorities, C2 structures, and the like. While some wish to define the horizons of cyberspace as boundless and without borders, the unfocused NMS-CO definition does not assist the JFC in this regard.

However, the definition of CNA is still too broad and encompasses many missions a JFC might wish to accomplish in the cyberspace domain. The CNA categories of information system attack and control system attack apply to all of the operations Mathers described in his thesis. By categorizing Mathers' proposed operations into doctrinally defined operational functions, mission types and terms, and further categorizing them as ISA or CSA, joint force

commanders have a tool to more readily define effects and command relationships. The reason for the two subcategories is fundamental; ISA affects information, CSA affects the physical world. While they are both CNA, the operational considerations and implications are different.

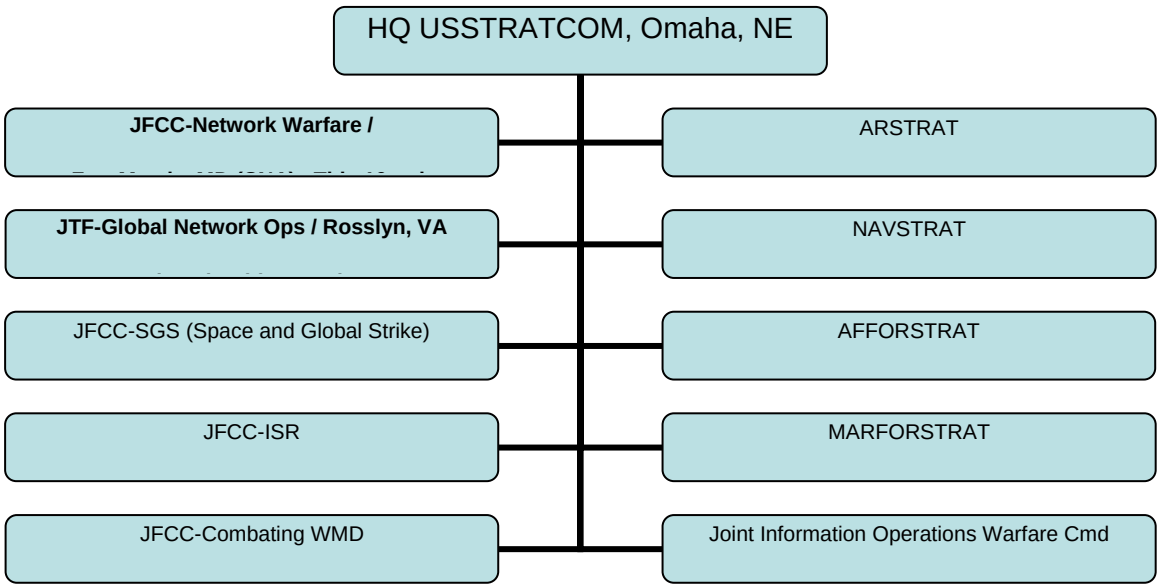
USSTRATCOM should have TACON of forces conducting ISA. That command has a strategic mission reflective of the trans-regional nature of the cyberspace domain, as well as close ties to the national intelligence community. How could an organization attacking an information system be effective otherwise? When attacking control systems, however, physical effects drive everything. The GCC and subordinate JFC must have TACON of the forces, in keeping with time-tested unity of command principles.

Words mean things: in the military, they define effects, help articulate objectives, and factor into operational decisions like command relationships, organizational diagrams and areas of responsibility. To add the requisite structure to the rapidly emerging and changing cyberspace domain----the newest domain---DOD should take the following steps. First, the Department should adopt the more precise definition of cyberspace suggested by DepSecDef. Second, the joint IO / CNA community should consider refining as necessary and adopting the ISA and CSA terminology in order to allow war fighters to better articulate CNA ways and means. Finally, those communities should consider adopting the command relationships for ISA and CSA as a means of attacking targets and creating effects in this new, rapidly changing domain.

NOTES

[i] Buxbaum, Peter A., "Virtual Blue Yonder." *Defense Technology International*, 1 December 2007, 2, ProQuest (accessed 10 September 2008).
[ii] Chairman, U.S. Joint Chiefs of Staff, *National Military Strategy for Cyberspace Operations* (U), (Washington, DC: CJCS, September 2006), (Secret) Information extracted is unclassified, 3, http://www.dod.mil/pubs/foi/ojcs/07-F-2105doc1.pdf (accessed 22 October 2008).
[iii] Hare, Forrest B., "Five Myths of Cyberspace and Cyberpower." *Signal Magazine*, June 2007, 2, http://www.afcea.org/signal/articles/anmviewer.asp?a=1333&print=yes (accessed 18 October 2008).
[iv] Dilley, Chelsea, "Air Force Cyber Command Factsheet." *Center for Defense Information*, 7 August 2008, http://www.cdi.org/friendlyversion/printversion.cfm?documentID= 4357 (accessed
18 October 2008).
[v] Vego, Milan N., Dr., *Operational Warfare*. U.S. Naval War College, Newport, RI, VIII-3.
[vi] U.S. Office of the Chairman of the Joint Chiefs of Staff. Information Operations. Joint Publication (JP) 3-13. Washington, DC: CJCS, 13 February 2006, GL-5.
[vii] Mathers, Russell F., "Cyberspace Coercion In Phase 0/1: How to Deter Armed Conflict," (research paper, Newport RI: U.S. Naval War College, Joint Military Operations Department, 2006), 8-12.
[viii] Gibson, Tim, "What You Should Know About Attacking Computer Networks." *Proceedings*, January 2003, 1, ProQuest (accessed 8 September 2008).
[ix] Ibid., 1.
[x] Ibid., 1.
[xi] Mathers, Russell F., "Cyberspace Coercion In Phase 0/1: How to Deter Armed Conflict," (research paper, Newport RI: U.S. Naval War College, Joint Military Operations Department, 2006), 8-12.
[xii] Tegnelia, Dr. Jim. "Countering the Proliferation of Weapons of Mass Destruction." Briefing. Precision Strike Technology Symposium, 20 October 2005.
[xiii] Alexander, Keith B., "Warfighting in Cyberspace." *Joint Forces Quarterly*, no. 46 (3rd Quarter 2007), 61.
[xiv] Barnes, Julian E., "Hacking Could Become Weapon in U.S. Arsenal." *Los Angeles Times*, 8 September 2008, 2, http://articles.latimes.com/2008/sep/08/nation/na cyber8 (accessed 11 September 2008).
[xv] Ibid., 2.
[xvi] Hart, Kim, "Longtime Battle Lines Are Recast In Russia and Georgia." The Washington Post. 14 August 2008, 1, ProQuest (accessed 10 September 2008).
[xvii] Horowicz, Mark, "Designating Information Operations as the Joint Force's Main Effort-What Do We Really Mean?" *IO Sphere*, Spring 2006, 15.

[xviii] U.S. Office of the Chairman of the Joint Chiefs of Staff. *Information Operations*. Joint Publication (JP) 3-13. Washington, DC: CJCS, 13 February 2006. IV-1.
[xix] Allard, Tom, "In Cyberspace They Can't Hear You Scream; The Essay." *Sydney Morning Herald*, 19 April 2008, 2, ProQuest (accessed 10 September 2008).
[xx] Derene, Glenn, "The Coming Digital War." *Popular Mechanics*, September 2008, ProQuest (accessed 4 September 2008).
[xxi] Gibson, Tim, "What You Should Know About Attacking Computer Networks." *Proceedings*, January 2003, 4, ProQuest (accessed 8 September 2008).
[xxii] Barnes, Julian E., "Hacking Could Become Weapon in U.S. Arsenal." *Los Angeles Times*, 8 September 2008, 3, http://articles.latimes.com/2008/sep/08/nation/na cyber8 (accessed 11 September 2008).
[xxiii] Hare, Forrest B., "Five Myths of Cyberspace and Cyberpower." *Signal Magazine*, June 2007, http://www.afcea.org/signal/articles/anmviewer.asp?a=1333&print=yes (accessed 18 October 2008).
[xxiv] Elliott, Michael C., "Operational Command and Control Of Joint Task Force Cyberspace Operations." (research paper, Newport, RI: U.S. Naval War College, Joint Military Operations Department, 2008), 24.
[xxv] U.S. Office of the Chairman of the Joint Chiefs of Staff. Information Operations. Joint Publication (JP) 3-13. Washington, DC: CJCS, 13 February 2006, IV-2.
[xxvi] Fulgham, David A., "Infowar To Invade Air Defense Networks." Aviation Week and Space Technology, 4 September 2002, 3, EBSCOhost (accessed 8 September 2008).
[xxvii] Barnes, Julian E., "Hacking Could Become Weapon in U.S. Arsenal." *Los Angeles Times*, 8 September 2008, 3, http://articles.latimes.com/2008/sep/08/nation/na cyber8 (accessed 11 September 2008).
[xxviii] Hare, Forrest B., "Five Myths of Cyberspace and Cyberpower." *Signal Magazine*, June 2007, 2, http://www.afcea.org/signal/articles/anmviewer.asp?a=1333&print=yes (accessed 18 October 2008).
[xxix] U.S. Office of the Chairman of the Joint Chiefs of Staff. Joint Fire Support. Joint Publication (JP) 3-09. Washington, DC: CJCS, 13 November 2006, III-21.
[xxx] Vego, Milan N., Dr., *Operational Warfare*. U.S. Naval War College, Newport, RI, VII-13.



USSTRATCOM's Component Structure

GLOSSARY

Computer: An electronic machine that receives, processes and presents data. A computer can be programmed to perform complicated tasks, like solving complex mathematical equations or controlling a flight simulator (http://www.spaceday.org/ index.php/Glossary-of-Aeronautics-Terms.html. Not defined in Joint Doctrine.

Computer Network Attack (CNA): Actions take through the use of computer networks to disrupt, deny, degrade or destroy information resident in computers and computer networks, or the computers themselves. JP 3-13.

Computer Network Exploitation (CNE): Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. JP 3-13.

Computer Network Operations (CNO): Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations. JP 3-13.

Cyberspace: A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers (http://www.dod.mil/pubs/foi/ojcs/07-F-2105doc1.pdf)

Cyberspace Operations: Not defined by DOD.

Network Warfare (NW): The employment of computer network operations with the intent of denying adversaries the effective use of their own computers, information systems, and networks. Not defined in Joint Doctrine. Alexander, Keith B., "Warfighting in Cyberspace.

BIBLIOGRAPHY

Alexander, Keith B., "Warfighting in Cyberspace." *Joint Forces Quarterly*, no. 46 (3rd Quarter 2007): 58-61.

Allard, Tom, "In Cyberspace They Can't Hear You Scream; The Essay." *Sydney Morning Herald*, 19 April 2008, ProQuest (accessed 10 September 2008)

Barnes, Julian E., "Hacking Could Become Weapon in U.S. Arsenal." *Los Angeles Times*, 8 September 2008, http://articles.latimes.com/2008/sep/08/nation/na cyber8 (accessed 11 September 2008).

Buxbaum, Peter A., "Virtual Blue Yonder." *Defense Technology International*, 1 December 2007, ProQuest (accessed 10 September 2008).

Chairman, U.S. Joint Chiefs of Staff, *National Military Strategy for Cyberspace Operations* (U), (Washington, DC: CJCS, September 2006), (Secret) Information extracted is unclassified, http://www.dod.mil/pubs/foi/ojcs/07-F-2105doc1.pdf (accessed 22 October 2008).

Derene, Glenn, "The Coming Digital War." *Popular Mechanics*, September 2008, ProQuest (accessed 4 September 2008)

Dilley, Chelsea, "Air Force Cyber Command Factsheet." *Center for Defense Information*, 7 August 2008, http://www.cdi.org/friendlyversion/printversion.cfm?documentID= 4357 (accessed 18 October 2008).

Elliott, Michael C., "Operational Command and Control Of Joint Task Force Cyberspace Operations." (research paper, Newport, RI: U.S. Naval War College, Joint Military Operations Department, 2008).

Fulgham, David A., "Infowar To Invade Air Defense Networks." Aviation Week and Space Technology, 4 September 2002, EBSCOhost (accessed 8 September 2008).

Gibson, Tim, "What You Should Know About Attacking Computer Networks." *Proceedings*, January 2003, ProQuest (accessed 8 September 2008).

Hare, Forrest B., "Five Myths of Cyberspace and Cyberpower." *Signal Magazine*, June 2007, http://www.afcea.org/signal/articles/anmviewer.asp?a=1333&print=yes (accessed 18 October 2008).

Hart, Kim, "Longtime Battle Lines Are Recast In Russia and Georgia." The Washington Post. 14 August 2008, ProQuest (accessed 10 September 2008).

Horowicz, Mark, "Designating Information Operations as the Joint Force's Main Effort-What Do We Really Mean?" IO Sphere, Spring 2006, 14-16.

Mathers, Russell F., "Cyberspace Coercion In Phase 0/1: How to Deter Armed Conflict," (research paper, Newport RI: U.S. Naval War College, Joint Military Operations Department, 2006)

U.S. Office of the Chairman of the Joint Chiefs of Staff. Joint Fire Support. Joint Publication (JP) 3-09. Washington, DC: CJCS, 13 November 2006.

U.S. Office of the Chairman of the Joint Chiefs of Staff. Information Operations. Joint Publication (JP) 3-13. Washington, DC: CJCS, 13 February 2006.

Vego, Milan N., Dr., *Operational Warfare*. U.S. Naval War College, Newport, RI: