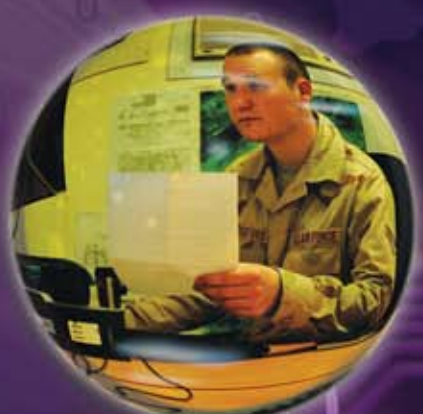
Spring 2010

IO SPHERE

The Professional Journal of Joint Information Operations

IN THIS ISSUE

Cyberspace



Joint Information Operations Warfare Center

IO SPHERE

FEATURE ITEMS and ARTICLES

Credit and thanks for our cover design go to our graphics editor Mr. Vincent Childress of the US Air Force ISR Agency.

Printed by the Air Force Intelligence, Surveillance & Reconnaissance Agency Print Plant, San Antonio, Texas-Mr. Rosalio Martinez, Director.

About the Covers: Front cover is a collection of photos of US service members using computers and of cyberspace operations centers. Back cover is a collection of phots from the activation of US Cyber Command. All photos are examples of "Cyberspace."

Staff

Mr. Mark H. Johnson
Director, Joint Information Operations Warfare Center

Mr. Charles Chenoweth
Executive Editor and Editorial Board President

Mr. Henry (Keith) Howerton
Editor and Layout Design
Webhead Group Incorporated

Mr. Vincent Childress
Graphics Editor and Layout Design

Cut Along Line

If you're on a .mil network, then ***IO Sphere*** *is available to you on the Joint Staff's* **JDEIS** *electronic publishing site.*

Go to https://jdeis.js.mil, and look under "Supplemental Info," then "CJCS," then click on "JIOWC IO Sphere"

Footnote references for all **academic** articles are published with the article. Additional references are found at the *IO Sphere* Home Page at: https://www/jiowc.osis.gov/Publications/IOSphere/index.cfm. Click on the "updates" link under the Spring 2010 issue.

Note: This works from dot gov domains only.

Group Photo at the Activation of US Cyber Command.

From Left to Right: General David Petraeus, Admiral Michael Mullen, General Keith Alexander, Secretary of Defense Robert Gates, and General Kevin Chilton. Source: defenseimagery.mil

IO SPHERE

QUARTERLY SUBMISSION DEADLINES: 31 MARCH, 30 JUNE, 30 SEPTEMBER, 31 DECEMBER

IO Sphere welcomes submissions of articles regarding full-spectrum IO, including its core, supporting and related capabilities. *IO Sphere* also welcomes book reviews and editorial commentary on IO and defense related topics.

SUBMISSION GUIDELINES

TEXT - Microsoft Word or Adobe Acrobat format

CHARTS/GRAPHS - TIFF, GIF or JPG format (if not 300 DPI please provide scannable hard copy)

PHOTOGRAPHS - TIFF, GIF or JPG (if not 300 DPI please provide scannable hard copy)

FORMAT/LENGTH - 700 - 4,000 words, double spaced

Please place graphs/photographs/charts on separate pages or as file attachments.

See the ***IO Sphere*** website from your .mil or .gov domain: https://www.jiowc.osis.gov or via Intelink at https://www.intelink.gov/wiki/IO_Sphere

Send Letters to the Editor, Articles & *Editorials* to:

iosphere@jiowc.osis.gov
Joint Information Operations Warfare Center - IO Sphere
2 Hall Blvd, Suite 217
San Antonio, TX 78243-7074
Phone: (210) 210-977-3680
FAX: (210) 977-4654 DSN: 969

CALL FOR ARTICLES

IO Sphere is currently seeking submissions on Military Information Support Operations, IO Training and Education, IO Support to Public Diplomacy, Public Affairs, and Electronic Warfare.

Views from the Top - Comments From the JIOWC Director

Welcome to the Spring 2010 issue of IO Sphere Journal. I sincerely hope that everyone in our worldwide Information Operations community is engaged in the defense of freedom and having a great 2010 as a start of a new decade.

This issue of IO Sphere is titled: "Cyberspace." Cyberspace is a critical domain to warfighting and the defense of the nation. At US Strategic Command (USSTRATCOM) cyberspace is one of the critical mission areas. USSTRATCOM, under the leadership of General Kevin P. Chilton, placed emphasis on the importance of cyberspace as the newest domain of warfighting. The command continues to lead the US Department of Defense in the identification of cyberspace as a specific area of emphasis. At USSTRATCOM cyberspace is as important as land, air, space, and sea power.

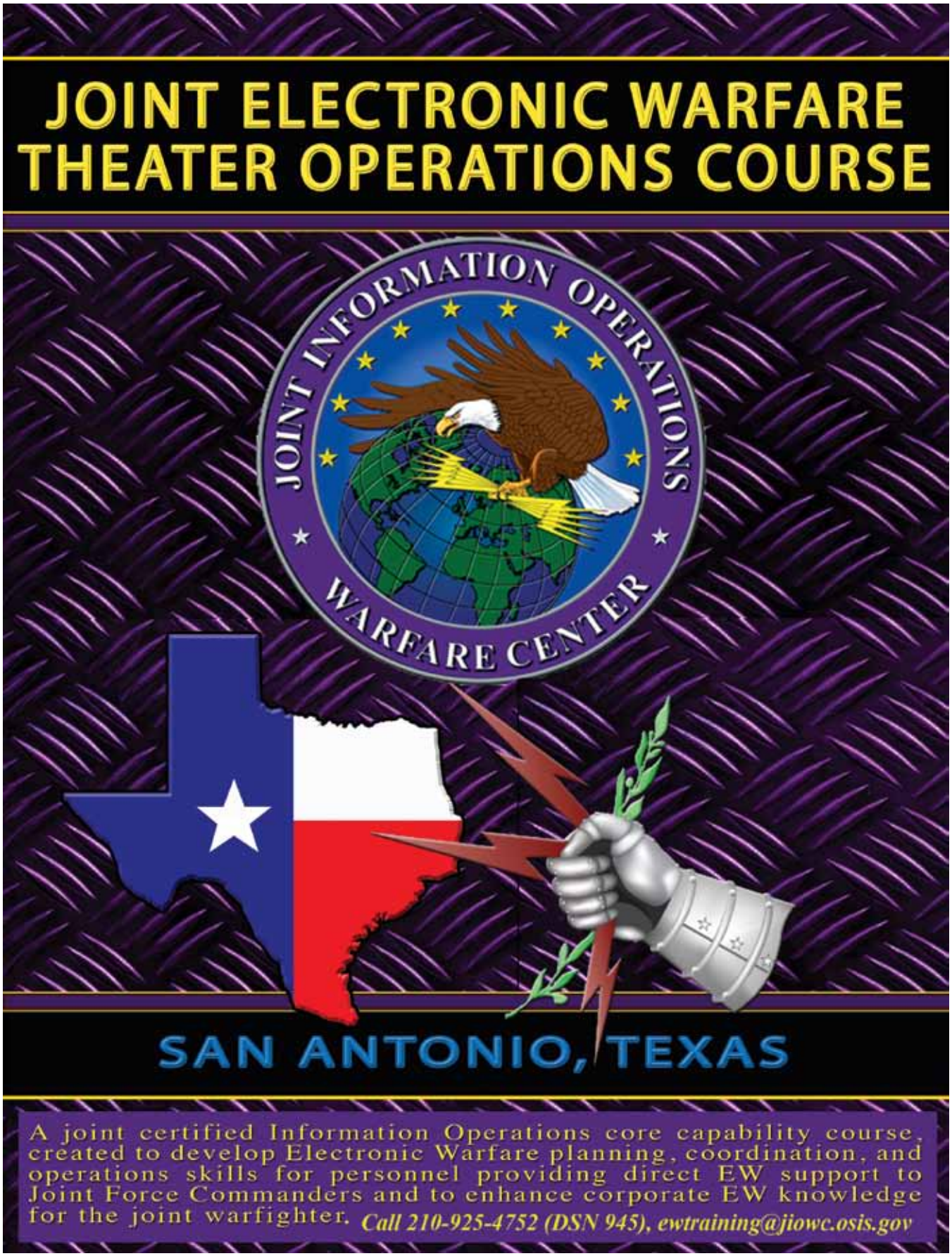
Illustrating the importance of cyberspace, US Strategic Command recently hosted the second annual "Cyberspace Symposium" in Omaha Nebraska. The symposium is an annual gathering of many of the most important policy and decision makers from government, industry, and defense. The focus is to discuss issues and share solutions for successful operations in cyberspace, as well as, successful computing and management of information. The Armed Forces Communications Electronics Association International is a co-sponsor of the annual event and provides the critical connection of the US Department of Defense with the professional organization most focused on cyberspace and the rapid changes and challenges associated with it.

In addition to the Cyberspace Symposium, this past spring saw the formation of the US Cyber Command as a sub-unified command under USSTRATCOM. The newly formed command, under the leadership of a General Keith Alexander, is responsible for the domain of cyberspace and is a reflection of the nation's commitment to successfully defending critical information and the ability to maneuver within a domain of ever-increasing complexity.

All of these events are critically important to the IO professional and IO Sphere and the Joint Information Operations Warfare Center recognizes this importance. It is entirely likely that in the 21st century many issues of conflict, peace, and international competition will occur in the domain of cyberspace. The importance of cyberspace can no longer be underestimated. The ability to successfully use and defend the domain of cyberspace is critical to all other elements of warfighting. The domain of cyberspace is, in many ways, the largest and most complex domain of warfighting in history. US Deputy Secretary of Defense William J. Lynn III recently stated in a press conference that; *"cyberspace and the internet does not respect or reflect national sovereignty and a large portion of it is privately owned."* The secretary's comments highlight the complexity and difficulties of operations in cyberspace. As IO professionals, we all must rise to that challenge and be a key part of the emerging doctrine and procedures for the successful use and defense of the cyberspace domain. It is critical that IO community focus effort, expertise, and resources to these emerging challenges of cyberspace. This effort will be one of the lasting legacies of our profession as IO warriors.

Mark H. Johnson, SES
Director, JIOWC
Department of Defense

Mr. Mark H. Johnson, a member of the Senior Executive Service, is the Director of the Joint Information Operations Warfare Center, Lackland Air Force Base,Texas. Subordinate to the US Strategic Command, the Joint Information Operations Warfare Center is the lead component for Information Operations and Strategic Communication in support of US national security objectives. The Command's 420 personnel support the development of global effects and provide IO/SC planning in support of USSTRATCOM mission areas of strategic deterrence, space, and cyberspace operations. Mr. Johnson served in the US Army from May 1979 to June 2008, achieving the rank of Colonel. Prior to his active duty retirement, Mr. Johnson was the Deputy Commander, Joint Information Operations Warfare Center. He is a master parachutist.


JOINT ELECTRONIC WARFARE
THEATER OPERATIONS COURSE
JOINT INFORMATION OPERATIONS
WARFARE CENTER
SAN ANTONIO, TEXAS
A joint certified Information Operations core capability course, created to develop Electronic Warfare planning, coordination, and operations skills for personnel providing direct EW support to Joint Force Commanders and to enhance corporate EW knowledge for the joint warfighter. Call 210-925-4752 (DSN 945), ewtraining@jiowc.osis.gov

Deputy Secretary of Defense William J. Lynn III on Cyberspace

The US Deputy Secretary of Defense Remarks at the USSTRATCOM and Armed Forces Communications and Electronics Association's 2010 Cyberspace Symposium

Editor's Note: The second annual USSTRATCOM and Armed Forces Electronics Association International (AFCEA) cyberspace symposium was held in Omaha Nebraska from 26-27 May 2010. Below is the text of Secretary Lynn's remarks. These remarks are largely unedited.

Thank you General Chilton. I appreciate the kind introduction. I am pleased to be with you today at Stratcom. I would like to thank General Chilton for hosting this important symposium and for all of his work on cyber security. I would also like to welcome our international colleagues and industry partners with us here today. I have been working closely on cyber security this past year. The whole issue is something of a good news/bad news predicament. Which reminds me of a story I know.

It's a story of two gentlemen who started off together in high school playing baseball. They were baseball fanatics. They went on to play baseball together at the same college. And they continued their passion over the years by watching games together every weekend. By the time they got well into their eighties, it became pretty clear that one of them was going to pass on fairly soon. Therefore, they made a little pact. Whoever died first would come back to tell the other the answer to their most important question: would there be baseball in heaven? Soon thereafter, one of them did pass on. While the other was sleeping a few nights later, an apparition appeared. Sure enough, it was his friend. "Terrific!," One friend said to the other. "You've held to the deal! You're back. Tell me, is there baseball in heaven?" His friend replied, "Well, there is good news and bad news. What do you want first?" "Oh, good news, I guess." So his friend goes on to say, "There is baseball in heaven. It's terrific. It's all outdoor fields and natural grass. You're playing with some of the best players ever: Joe DiMaggio, Ted Williams. It's just what you would have hoped for in heaven." The friend still on earth asked, "How can there

DEPSECDEF William J. Lynn III Keynote Speech at the 2010 Cyberspace Symposium
Source: USSTRATCOM, Photo by Dan Rohan

be bad news in that?" His friend says, "Well, you're pitching tomorrow."

And that's the story with cyber security as well. Without question, we are the world's leading producer and consumer of information technology. It powers our economy. It enables almost everything our military does. Command and control of our forces, intelligence gathering, logistical support of our troops—cyber gives us significant advantages over any adversary. But cyber also poses a threat. Our very reliance on cyber furnishes an obvious route for adversaries to attack us. Cyber is therefore a source of potential vulnerability.

So today, I would like to talk about how DOD is addressing cyber security—how we see the environment, what we see as the threats, and what our strategy is to combat those threats. I will also discuss the importance of U.S. Cyber Command, which we formally established last Friday. Finally, I want to address the importance of partnering closely with industry and the need for the Department to develop a better process for IT acquisition.

Let me start with the basics. DOD has a large IT footprint. We operate more than 15,000 networks within the dot mil domain. We have seven million computing devices. Ninety thousand people are directly involved in the operation of our information technology. We rely not only on our own networks, but also on many commercial and government networks outside the dot mil domain. The fact is that our department depends on the overall IT infrastructure of our nation. The threat to our computer networks is substantial. They are scanned millions of time a day. They are probed thousands of times a day. And we have not always been successful in stopping intrusions. In fact, over the past several years we have experienced damaging penetrations.

Cyber is an especially asymmetric technology. The low cost of computing devices means that our adversaries do not have to build expensive weapons systems to pose a serious threat. They do not need fleets of ships or aircraft to conduct damaging attacks on our society. Knowing this, many militaries are developing offensive cyber capabilities, and more than 100 foreign intelligence organizations are trying to break into U.S. systems. Some governments already have the capacity to disrupt elements of the U.S. information infrastructure. Cyber is also an attractive weapon to our adversaries because it is hard to identify the origin of an attack and even more difficult to deter one.

A keystroke travels twice around the world in 300 milliseconds. But the forensics necessary to identify an attacker may take months. Without establishing the identity of the attacker in near real time, our paradigm of deterrence breaks down. Missiles come with a return address. Cyber attacks, for the most part, do not. For these reasons established models of deterrence do not wholly apply to cyber. We need a deterrent structure that fuses offensive, defensive, and intelligence operations to meet current and future threats.

In our analysis, we see four overlapping cyber threats. The first is to our military networks themselves. This threat was recognized fairly early, and we have made a concerted effort over the last five years to construct substantial defenses.

DEPSECDEF Lynn, General Kevin P. Chilton, and Lieutenant General Larry D. James
Source: defenseimagery.mil

We are not invulnerable at this point. But the level of protection is higher than you will find on any other IT systems. With the establishment of Cyber Command, we are continuing to increase that protection through the use of more active defenses, which I will discuss in a few moments. The second threat is to the nation's critical infrastructure. Computer-induced failures of our power grids, transportation system, or financial sector could lead to physical damage and economic disruption on a massive scale. The Clinton administration identified this threat in the late '90s. The Bush administration made it a part of their cyber initiative.

But we have not yet arrived at the point at which these networks are as protected as they need to be. I believe there are steps we can take, and I will outline one possible approach later. The third and in many ways least discussed threat is to our intellectual property. Earlier this year key parts of Google's source code were ex-filtrated in a sophisticated operation that also targeted dozens of other companies. The defense industry has similarly been targeted. Designs for key weapons systems have been stolen.

The threat to intellectual property is less dramatic than a cyber attack on our infrastructure. But it may over the long term be the most significant cyber threat our nation faces. The risk of tampering in our supply chain is the fourth and final threat. Rogue code, including so-called "logic bombs," can be inserted into software as it is being developed, allowing outside actors to manipulate systems from afar.

Hardware is also at risk. Remotely operated "kill-switches" and hidden backdoors can be written into the chips and physical buses used in military hardware. The risk of compromise in the manufacturing process is very real, and in many respects is the threat we least understand. Tampering is difficult to detect, and even harder to prevent. To give you an example of how pervasive the cyber threat is, not even our presidential candidates were spared.

In the 2008 campaign, both Barack Obama and John McCain had their computer systems compromised. Emails, travel plans, and policy documents were all compromised. The intrusion was eventually detected and repelled, but not before sensitive information was taken. For all these reasons, President Obama has appointed Howard Schmidt as his Cyber Coordinator and has called cyber, "one of the most serious economic and national security challenges that we face as a nation." To respond to the array of cyber threats that confront us, the Pentagon is taking action on several fronts.

As a doctrinal matter, the Defense Department has formally recognized cyberspace for what it is—a new domain of warfare. Like land, sea, air, and space, cyberspace is a domain that we must operate effectively within. Cyberspace is the only domain that is man made and largely privately owned, but it is nevertheless just as critical to our military effectiveness as the others are. To secure our digital infrastructure, the Department has established three lines of defense. Our first line of cyber defense is ordinary hygiene—keeping systems and software up to date. The internet is teeming with so many viruses and bonnets that an unprotected computer can be infected within minutes of being placed online. To remain secure, any network that has contact with the internet must constantly refresh malware signatures and install security patches. With three million users, keeping our computers up to date is a constant challenge, but one that we are starting to meet. Automated systems now ensure firewalls and anti-virus software are properly configured on each of our computers. We estimate that effective hygiene will block about half of attempted intrusions.

Perimeter security forms our next line of defense. To monitor traffic flowing into and out of our networks, we narrowed the number of ports at which our systems accesses the commercial internet. We also deployed host-based security services and intrusion detection systems on our servers and routers. These sensors are linked to network mapping and visualization software that help identify breaches. We believe perimeter defenses block another 30-40% of attempted intrusions. Taken together, proper hygiene and perimeter security furnish a level of protection approaching 90%. But sophisticated adversaries

2010 Cyberspace Symposium Entry Sign

Source: IO Sphere Staff Photographer

are able to surmount even these defenses, leaving our networks at risk. In cyber, offense is dominant. A fortress mentality will not work. We cannot retreat behind a Maginot line of firewalls. In this way cyber is much like maneuver warfare, in which speed and counterattack matter most. If we stand still for a minute, our adversaries will overtake us.

Given the dominance of offense, our defenses need to be dynamic. We need to respond to attacks at network speed, as they happen or even before they arrive. The core of our effort in this regard is at the National Security Agency. The NSA has developed systems that give us the kind of active defenses we need. These active defenses, which use foreign intelligence to help anticipate threats, prevent the last 10 or 20 percent of sophisticated intrusions. Moreover, intrusions will not always be caught at the boundary. Some of them will inevitably evade detection. To find intruders once they are inside, we have to be able to hunt on our own networks. Cyber is also an area in which the U.S. cannot go it alone. There is a strong logic to collective cyber defenses. Alliances are powerful tools. I have traveled to Australia and the U.K., and will soon be going to Canada. We are seeking to develop a system of shared warning and shared technology. Collective cyber defenses are similar to air and missile defense in that the more attack signatures that you see, the better your defenses will be.

The concept of collective defense is a key part of our strategy. Facing these foundational challenges, we made a decision to establish a military command for cyber operations. Until recently, the military's cyber effort was run by a loose confederation of joint task forces spread too far and too wide, both geographically and institutionally, to be fully effective. Secretary Gates recognized that the scale of the cyber enterprise had outgrown the military's existing structures. Last June, he ordered their consolidation into a single four-star command, U.S. Cyber Command. Cyber Command, a sub-unified command, is a part of the U.S. Strategic Command. Cyber Command will perform three core missions. It will lead the day-to-day defense of dot mil networks. It will support military and counterterrorism missions. And under the leadership of the Department of Homeland Security, it will assist civil authorities and industry partners. We achieved initial operations capability at Cyber Command last Friday. General Keith Alexander, head of the National Security Agency, has been appointed its commander. The key part of Cyber Command is its linking of intelligence, offense, and defense under one roof. In cyber, the capability to repel attackers is closely tied to the ability to identify threats and anticipate intrusions. You will not be effective in the cyber world if you segregate these three functions.

We also need a command to lead the planning, training, and equipping of our forces. In the military, we exercise our

US DEPSECDEF William J. Lynn III
Source: defenseimagery.mil

capabilities on target ranges and in a variety of simulations. We do not yet have that capability in the cyber world. Therefore, DARPA, which helped build the internet decades ago, is developed a national cyber training range—in effect a model of the internet. Once operational, the training range will allow us to test tactics before we field them. A single chain of command runs from the head of Cyber Command to individual units around the world. Service commands, including the Army's Network Enterprise Technology Command, the Navy's 10th Fleet Cyber Command, and the 24th Air Force, will ensure cyber is a regular part of training and equipping the force. With Cyber Command, the progress we are now making is significant. But we will not be successful unless we continue to augment our capabilities and our personnel.

So today, I would like to describe our next steps in cyber. I see three major challenges ahead: strengthening our human capital over the long term, rethinking IT acquisition, and providing security for those parts of the commercial internet DOD depends upon. Our effectiveness in IT is to a great degree predicated on our ability to train sufficient numbers of qualified personnel. In the last two years, we have increased the number of trained cyber professionals and deepened the level of their training. This includes a formal certification program for information assurance and training our network administrators. But even as we strengthen our cadre of cyber professionals, we must recognize that the long-term trend in human capital is against us.

Over the next twenty years there is little doubt that China or India will train more computer scientists than we will. We will not be able to keep up. Demographics work against us. If our cyber advantage is predicated solely upon amassing trained cyber professionals, we will lose. Therefore, we need to confront cyber in the same way we confront other quantitatively dominant competitors. We do not always compete on numbers. We compete on technology and information dominance. The same will be true in cyber. We will need automated systems, sensors, and artificial intelligence to multiply the value of the trained cyber professionals we have.

Beyond human capital, improving the acquisition of information technology is a pressing concern. The Department has a traditional way of acquiring technology. It is generally focused on developing airplanes, tanks, and ships. In this very ordered process we decide what the mission is, identify requirements to meet that mission, and analyze alternatives to meet those requirements. Only then, do we develop a program and budget for it. Eight or nine years later, we actually have something. Now this may seem like a long time, but this nation has the best technology any military has ever seen. So the system actually works pretty well. To date, our acquisition of IT largely follows this model. On average, it takes the Department 81 months from when an IT program is first funded to when it becomes operational. But if we take into the account the continued growth of computing power, as suggested by Moore's law, this

2010 Cyberspace Symposium Defense Vendor Display Area

Source: IO Sphere Staff Photographer

means that systems are being delivered four to five generations behind the state of the art. By comparison, the iPhone was developed in 24 months. That is less time than it would take us to prepare and defend a budget and receive Congressional approval for it. Steve Jobs gets an iPhone. We get a budget. It's not an acceptable trade.

Therefore, we have established a new task force to improve our approach to IT acquisition. The Task Force reports directly to me. I have directed it study how we can refashion IT acquisition around four principles. First, heeding Secretary Gates' call to make our department more agile, speed must be our overarching priority. We need to match the acquisition process to the technology development cycle. In IT, this means 12 to 36 months cycles, not 7 or 8 years. Second, we must acknowledge that incremental development, testing, and whenever possible, fielding of new capabilities provides better outcomes in IT than trying to deploy large complex systems in one "big bang." Third, to achieve speedy, incremental improvements, we need to carefully examine how to establish the requirements that govern acquisition. Systems must always be tailored to serve the needs of end users, but departing from standard architectures in IT imposes great costs. To achieve speed, we must be willing to sacrifice or defer some customization. Making use of established standards, and open modular platforms, is of paramount importance. Fourth, the department's IT needs range from modernizing nuclear command and control systems to updating word processing software on our office computers.

We must recognize that different IT applications demand different levels of oversight and enterprise integration. We are working to outline a series of acquisition paths that apply high levels of institutional due diligence where it is needed and strip away excess requirements where it is not. The problem we are trying to solve is not an easy one. The Defense Department has unique IT needs that limit our ability to replicate the dynamism of private industry. Our systems must work across business, war-fighting, and intelligence applications. We cannot usually go without the functionality of existing systems as they are being updated or replaced. In addition, for us it is not merely about purchasing new technology. The planning, programming, and Congressionally-mandated budgeting process must all be in alignment.

Despite these significant obstacles, I believe we can make dramatic improvements in IT acquisition. Our focus is on identifying who is being innovative, how to make better use of existing authorities, and where to try pilot projects. Our intent is to target things we can change now, while laying the foundation for longer term reforms that may require Congress to legislate new authorities.

Finally, the best-laid defenses on military networks will matter little unless our civilian critical infrastructure is also protected. Critical infrastructure will certainly be targeted in a military conflict. The Department of Homeland Security appropriately has the lead to protect the dot gov and dot com domains. The Defense Department plays an important supporting role in this mission, and has direct responsibility for securing defense industry networks. Years of concerted investments on the military side have placed critical cyber capabilities within the Defense Department and National Security Agency. We are already using our technical capabilities to support DHS in developing the Einstein 2 and 3 programs to protect government networks. We need to think imaginatively about how this technology can also help secure a space on the internet for critical government and commercial applications. For the dot com world, could we create a secure architecture for that lets private parties opt-in to the protections afforded by active defenses? In this way, protection would be voluntary. Operators of critical infrastructure could opt-in to a government-sponsored security regime. Individual users who do not want to enroll could stay in the "wild West" of the unprotected internet. This type of secure dot com approach could build on the collaboration between DOD and the defense industry. It could offer an important gateway to ensure our nation's critical infrastructure is protected from cyber attacks. As you can see, the front line of national security has been redefined. Although the challenges we face in cyber seem daunting, it is useful to remember that we are at the beginning of a new technological age. So let me leave you with this simple observation. We just marked the 20th anniversary of the World Wide Web. In comparison, we have just passed the 100th anniversary of military aviation. The Wright Brothers brought their military flyer to the national capital for its first demonstration flight 100 years ago last June. It was the first time the Army Signal Corps had purchased an airplane. We are now 100 years into military aviation, whereas with cyber we only have twenty years of collective experience. Essentially, in the cyber world, it's 1929. We are still in the era of dirigibles and biplanes. We are at the dawn of a new epoch, with decades of innovations in safety, performance, and reliability to come. We have a lot of work to do to make the cyber domain safe, so its revolutionary innovations can be used without fear of endangering our national and economic security. But with the advent of Cyber Command and the other steps DOD is taking, we are well on our way. Thank you very much.

Old vs New: Legal Considerations Of Cyber Targeting

by

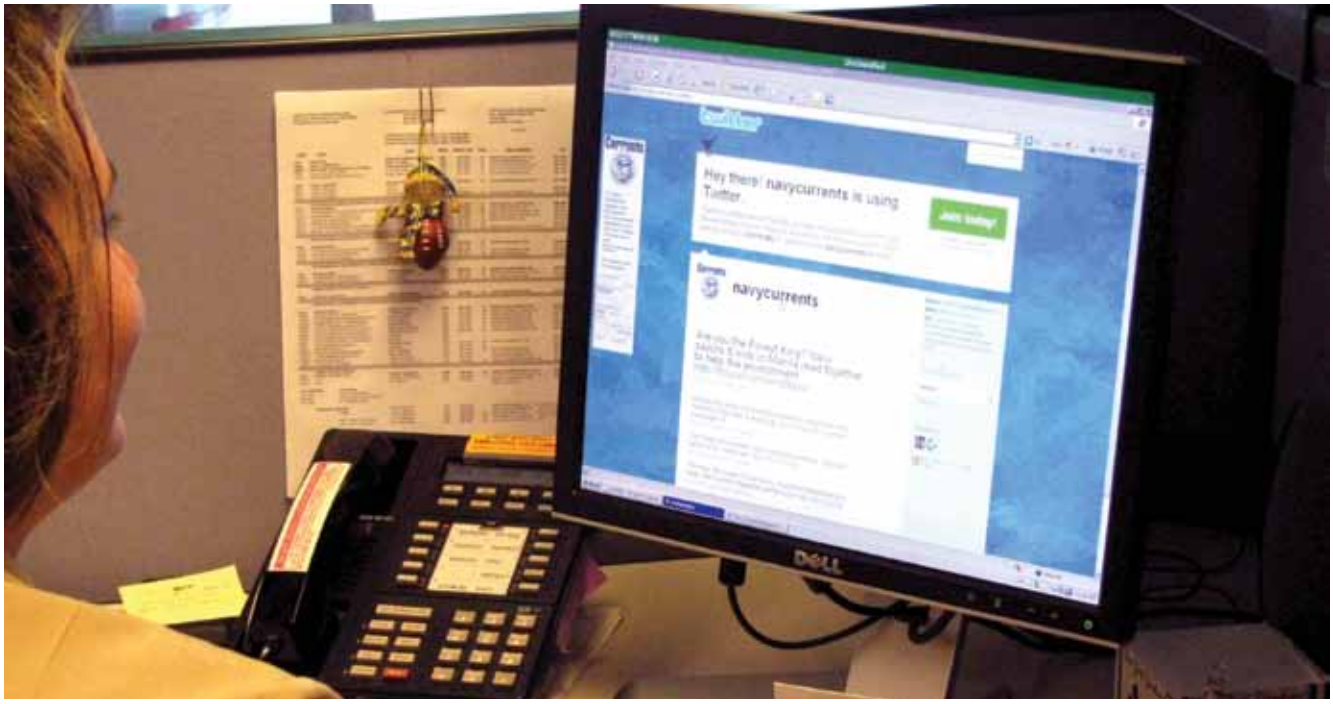
Mr. Dondi West

Editor's Note: Mr. West's views on cyber targeting and the legal ramifications of such operations are important to this current and relevant topic. Even DEPSECDEF Lynn in his comments at the 2010 Cyberspace Symposium spoke if the unique legal challenges of cyberspace and cyberspace operations. Mr. West's views are very important to this issue of IO Sphere Journal.

Executive Summary

Regulating the conduct of individuals, nations, and other entities during war has a long history. One of the earliest known instances of regulating the conduct of war can be found in the Old Testament in Deuteronomy 20:19 limits the amount of collateral and environmental damage: "When thou shalt besiege a city... in making war against it to take it, thou shalt not destroy the trees thereof..." Another example occurs in the early 7th century, when the first Caliph, Abu Bakr laid down the following rules concerning warfare while instructing his Muslim army: "Stop, O people, that I may give you ten rules for your guidance in the battlefield. You must not mutilate dead bodies. Neither kill a child, nor a woman, nor an aged man. Bring no harm to the trees, nor burn them with fire, especially those which are fruitful..."[1] In the above historical examples, even trees appear to be off limits and would not qualify as lawful military targets under those rules.[2]

Obviously, the rules and conventions of warfare have changed since the days of the Old Testament and Abu Bakr. In today's information age, combatant commanders are faced with targeting decisions that would have appeared to be out of a science-fiction movie just twenty years ago. We are living in a net-centric world, participating as a part of a continuously evolving, complex community of people, devices, information, and services interconnected by communication networks that provide superior information needed to empower decision makers. The net-centric nature of our society has also altered our battle space. The 2006 National Military Strategy for Cyberspace Operations states that "as a warfighting domain… cyberspace favors the offense." As such, offensive capabilities in cyberspace offer both the US and our adversaries an opportunity to gain and maintain the initiative.



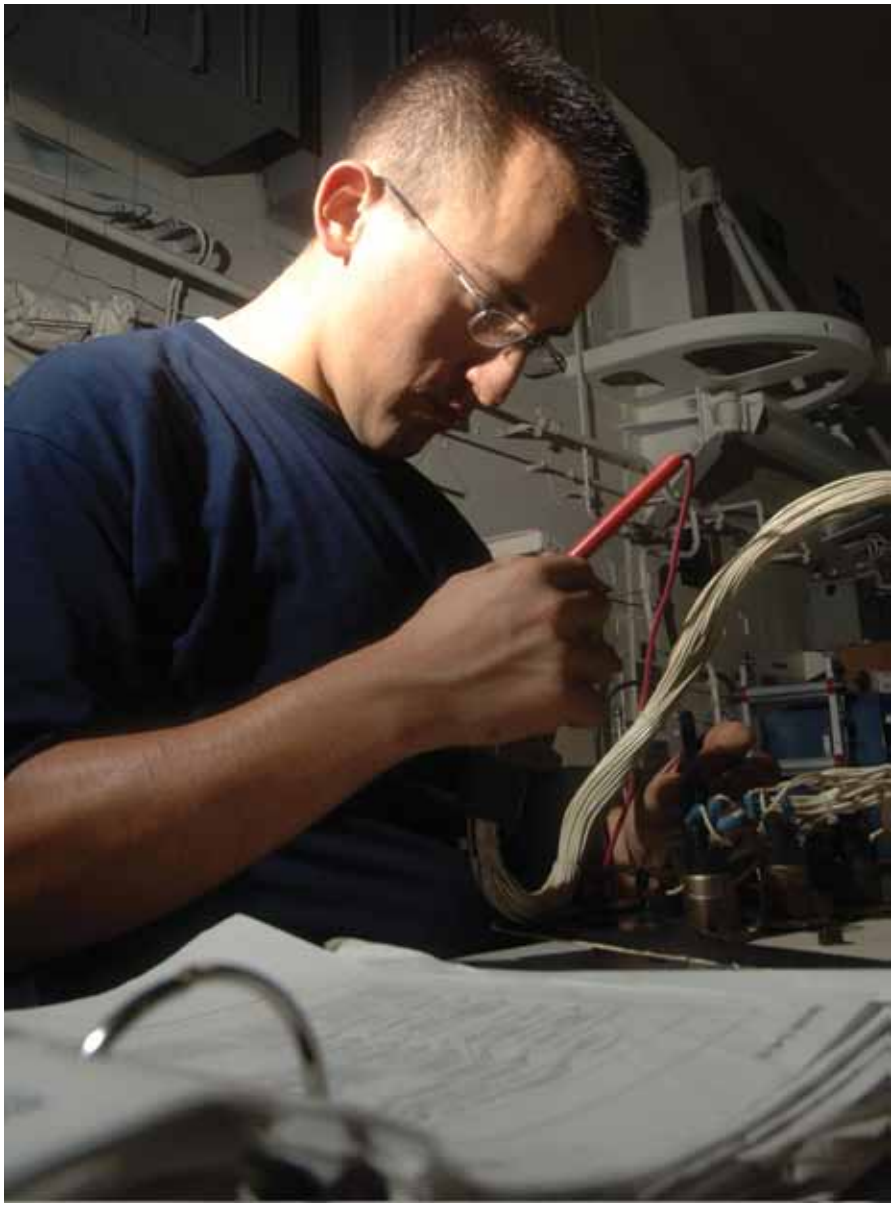
US Navy Staff Judge Advocate Officer Sharing Legal Information on Twitter with Sailors

Source: defenseimagery.mil

Although the rate of technological development would appear to wreak havoc on the legal frameworks related to military targeting, the principles of distinction, military necessity, and proportionality appear to be withstanding the test of time.[3] While some legal scholars are advocating for a new international treatise for Cyber Warfare, others argue that the rules related to traditional-kinetic warfare are adequate.[4] This paper is intended to introduce the laws that govern traditional military and Cyber Targeting. In addition, this paper seeks to highlight two opposing schools of thought in developing legal frameworks related to Cyber Warfare.

Defining Computer Network Operations

According to Joint Publication 3-13, the full-spectrum of Computer Network Operations (CNO) encompasses three domains: computer network attack (CNA), computer network exploitation (CNE), and computer network defense (CND). Within the military domain, CNO is considered one of five core capabilities under Information Operations (IO). The other capabilities include PSYOPS, military deception (MILDEC), operations security (OPSEC), and electronic warfare (EW). The Joint Publication also defines each of the three domains of CNO.



US Navy Technician Working on a Navigation Computer System

Source: defenseimagery.mil

CNA includes actions taken via computer networks to disrupt, deny, degrade, or destroy the information within enemy computers and computer networks. CNE includes enabling actions and intelligence collection via computer networks that exploit data gathered from target or enemy information systems or networks. CND includes actions taken via computer networks to protect, monitor, analyze, detect, and respond to network attacks, intrusions, disruptions, or other unauthorized actions that would compromise or cripple defense information systems and networks. This paper is mainly concerned with the legal implications of targeting while conducting CNA ("Cyber Warfare").

Defining Lawful Military (Cyber) Targets

Once two nations are in armed conflict with each other, the law of war applies.[5] The Department of Defense (DOD) mandates the law of war to apply in all operations including military operations other than war (emphasis added).[6] Thus, combatant commanders must adhere to the law of war during Cyber operations.

"The law [of war] requires that only objectives of military importance be attacked..." Lawful military targets are "combatants and those objects, which, by their nature, location, purpose, or use, effectively contribute to the enemy's war-fighting or war-sustaining capability and whose total or partial destruction, capture, or neutralization would constitute a definite military advantage to the attacker under the circumstances at the time of the attack."[7] "Targets of the enemy that indirectly but effectively support and sustain the enemy's war-fighting capability may also be attacked."[8] A combatant commander must consider three factors when deciding if a target can

be attacked: (1) Distinction, (2) Balancing Military Necessity with Humanity, and (3) Proportionality.[9]

Distinction

Two concepts emerge under the principle of distinction: (1) that there be a formal distinction between combatants and noncombatants;[10] and (2) the duty to conduct warfare in a manner that minimizes harm to civilians and other noncombatants. Because this paper is primarily concerned with targeting, an emphasis is placed on the latter concept of distinction. However, as a note, lawful combatants include the uniformed regular armed forces of a state, who have the sole right to participate in armed attacks or hostilities against an enemy.[11]

A combatant commander is required to distinguish between military and civilian objects where the central idea of distinction is to only engage valid military targets. Protocol Additional to the Geneva Conventions covers distinction in this respect.[12] The general rule for distinction is embodied in Article 48, which states that "[i]n order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives." Article 50 defines who is a civilian and what is a civilian population. Article 51 describes the protection that should be given to civilian populations. Article 52 regulates the targeting of civilian objects. Article 57 outlines specific steps that a commander must take in order to verify that and object is not civilian in nature.

Drawing the line of distinction is not as simple as it may appear to be. Complicating the matter for commanders, civilian objects can temporarily become valid military objectives based on location, purpose, or use.[13] Major Eric Talbot Jensen, a Professor in The International and Operational Law Department at The U.S. Army's Judge Advocate General School explained the concept of dual use objects using an infamous bridge example: "*A bridge that normally carries civilian traffic and would be considered a civilian object would become a military objective based on its location if it became the means for the enemy's armed forces to move to the battle. While still serving as a primary means for civilian transport over the river, the bridge is now a military object, as it is the primary means for the military to cross that same river. Objects like this are known as dual-use objects; objects that simultaneously serve civilian and military objectives. These dual-use objects present a unique challenge for commanders.*"[14]

It is important to note that even when engaging a dual-use object found to be a military objective, the commander, when possible, must make an effort to limit his attack to the portions of the dual-use object that is military in nature. Furthermore, once the dual-use object ceases to support military objectives, it must be looked upon as being civilian in nature.[15]

Within the concept of cyber targeting, one can imagine distinction coming into play when attacking an enemy's computer network. Because of the inter-connective nature of the internet, that network would likely be dual use, due to the internet likely being serviced by a civilian internet service provider, while supporting the enemy's military objective of communicating. As discussed above, a combatant commander would need to take reasonable steps in order to limit his attack to the portion of the network used by the enemy. If a computer virus is designed to propagate randomly through networks on which essential civilian functions reside, such as banking, medical care or electrical power, then the principle of distinction would likely be violated.

Balancing Military Necessity with Humanity

Military necessity is very similar to distinction. Under military necessity, an attack on a particular target must further a

US Navy Sailors at their Stations in a Cyber Defense Center

Source: defenseimagery.mil

legitimate military objective or confer a definite military advantage.[16] Although the principle of military necessity appears to be a liberal one, it is not unchecked. It must be balanced against the principle of humanity.[17] That is, an attack should not cause unnecessary suffering or superfluous injury in order to accomplish a military purpose.[18]

Military necessity must be balanced with humanity in the cyber context and can be based on the fictitious attack on an enemy's computer system that controls its power supply. Although disabling the power supply might be a legitimate military objective, the commander must weigh this objective against humanitarian gains and losses such as extensive power loss, or power loss to a civilian hospital or other critical civilian objects. Using the principle of humanity, targets that might be deemed critical civilian infrastructures, are protected under established valid military objectives. The decision to attack critical civilian infrastructures, which may be a dual-use target, must be weighed against the principle of humanity prior to any engagement decisions.

Proportionality

A simple way to remember the principle of proportionality is by recalling the popular phrase that 'the ends must justify the means.' In other words, the incidental harm caused to civilians or civilian property must be proportional and not excessive in relation to the concrete and direct military advantage anticipated by an attack on a military objective.[19] Taking the above requirement to balance military necessity and humanity into consideration, proportionality would be the tool by which they are balanced. The combatant commander ordering the attack is responsible for making the proportionality judgment. A corollary of the principle of proportionality is that the attacker has a responsibility to take reasonable steps to find out what collateral damage a contemplated attack may cause.[20]

Applying proportionality in the context of a power supply scenario, one can see that proportionality is the calculus applied to determine whether the benefits from achieving the military objectives outweigh its negative collateral effects such as extensive power loss to the civilian population.

US Air Force Communications Specialist Servicing Communications Computers
Source: defenseimagery.mil

Calls for an International Treatise for Cyber Warfare?

As noted supra in Section 3 Parts A-C, cyber targeting and warfare is governed by the same laws that are applied to traditional kinetic warfare. The same body of law that governs a commander dropping a bomb on an enemy compound also governs a commander choosing to attack an enemy's computer network. Legal scholars have criticized the law of war as outdated as it relates to cyber warfare, and therefore call for the creation of an International Treatise for Cyber Warfare. Still, other legal scholars contend that the law of war compliments the ability for commanders to employ cyber capabilities.

Davis Brown suggests that applying the current law of war to cyber and information warfare "erroneously assumes that warfare by computer is not significantly different from warfare with kinetic weapons such as bombs and bullets." Brown goes on to caution

against assuming, that conventional law of war "will resolve all of the new issues raised by the use of malicious code, denial-of-service attacks, and control of vital systems when used against the enemy." To support the above contention, Brown points out two paradigms that have emerged due to cyber and information warfare. First, that there is a shift in favored weaponry from kinetic weapons towards information weapons. Second, that there is a growing dependency on civilians and civilian objects when conducting warfare. Based on those two paradigms, Brown concludes that "[t]he square peg of conventional [law of war] does not fit neatly into the round hole of [cyber and] information warfare," and he therefore proposes an "International Convention to Regulate the Use of Information Systems in Armed Conflict." Brown goes on to state that this proposed body of law governing Cyber Warfare should be based on the current law of war, including the principles of Part III above, but not so much that the essence of Cyber and Information Warfare is crippled.[21]

On the other hand, Major Eric Jensen contends that the traditional law of war actually compliments a commander's ability to conduct Cyber Warfare. Jensen argues that the law of war accommodates a commander's use of CNA in that the commander only needs to determine "if, in good faith, he believes that the damage to civilian objects, and injury to civilians that is expected from the attack, given the circumstances as known to him at the time . . . is not excessive to the concrete and direct military advantage anticipated." Jensen concludes "the legal standard when considering potential unexpected consequences is no different in CNO from in normal kinetic operations and presents no significant addition to the standard targeting analysis."[22]

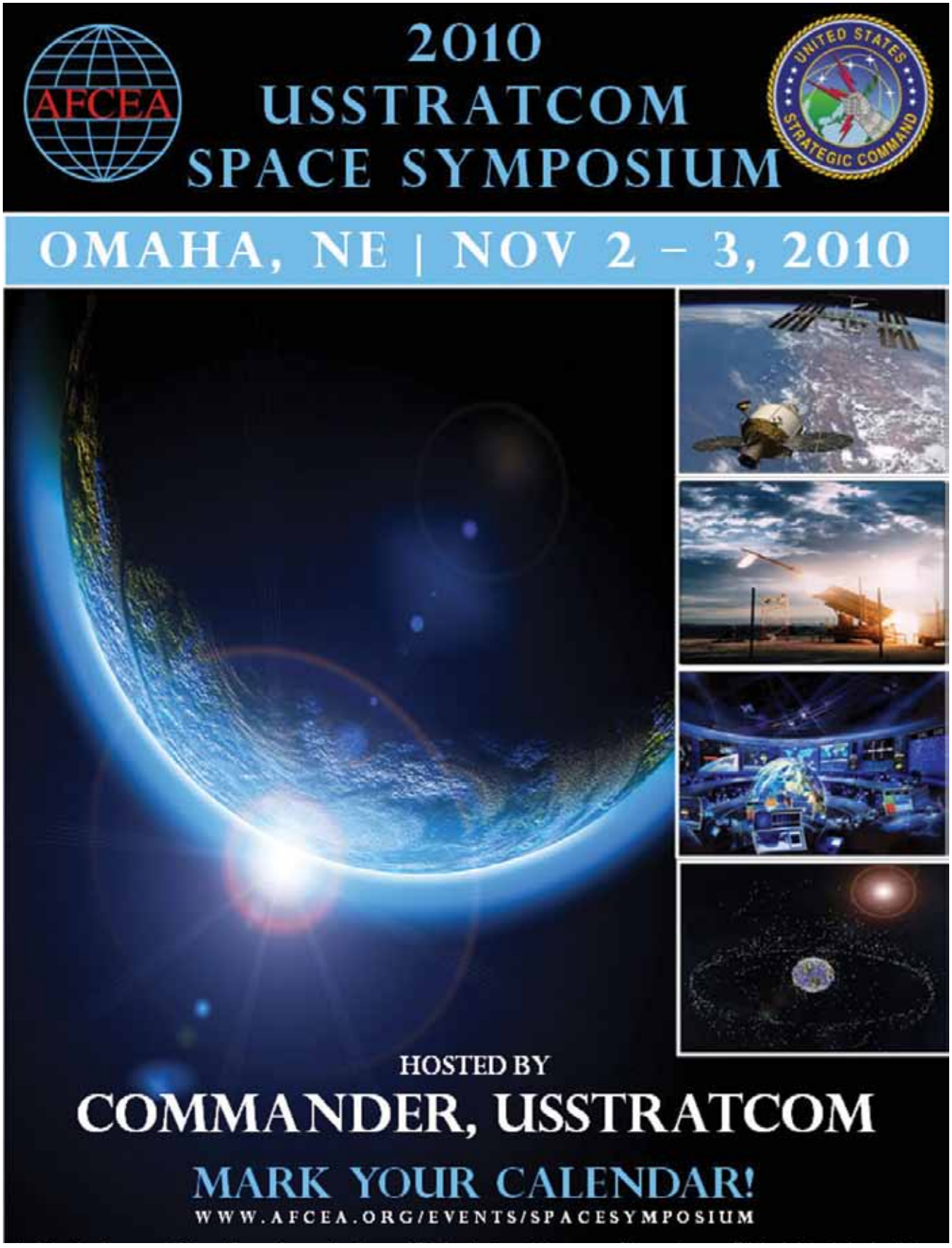
Both of the above schools of thought show that the law related to Cyber Warfare and targeting is a hot topic. It is unknown whether there will one day be an International Treatise for Cyber Warfare, but it is known that the law of war has been able to withstand the test of time.

Conclusion

With the rapid development of technology, it is important to understand the law that governs cyber targeting and warfare. A military commander must consider three factors when deciding if a target can be attacked: (1) Distinction; (2) Balancing Military Necessity with Humanity; and (3) Proportionality. The above framework appears to have withstood the test of time, although some legal scholars are calling for an International Treatise for Cyber Warfare.

Footnotes:

1. Aboul-Enein, H. Yousuf and Zuhur, Sherifa, Islamic Rulings on Warfare, p. 22, Strategic Studies Institute, US Army War College, Diane Publishing Co., Darby PA,
2. See infra Part III.
3. See infra Part III.
4. See infra Part IV.
5. See Condition (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, art. 2 (stating that the law of war comes into play during international armed conflict).
6. See DoDD 5100.77, The Law of War Program.
7. Additional Protocol I to the Geneva Conventions art. 52.
8. Id.
9. See U.S. Dep't of the Navy, NWP 1-14M, Commander's Handbook on the Law of Naval Operations (Jul. 2007).
10. 1949 Geneva Convention (III) Relative to the Treatment of Prisoners of War ("GPW"), art. 4.
11. Id.
12. The full name is Protocol Additional to the Geneva Conventions of 1949, and Relating to the Protection of Victims of International Armed Conflict ("GPI").
13. See GPI, supra note 21, art. 57, para. 2(a)(ii), 1125 U.N.T.S. at 29.
14. Major Eric Jensen, Unexpected Consequences From Knock-On Effects: A Different Standard for Computer Network Operations?, 18 AM. U. INT'L L. REV. 1145, 1156-57 (2003).
15. Id.
16. Protocol 1 to the Geneva Conventions art. 52(2).
17. See Hague Convention on Land Warfare art. 22 (1907) (demonstrating the essential relationship between military necessity and humanity).
18. See GPI art. 35 para. 2.
19. Yoram Dinstein, The Conduct of Hostilities Under the Law of International Conflict 12-23 (2004).
20. Id.
21. Davis Brown, A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict, 47 HARV. INT'L L.J. 179, 179-83 (2006).
22. Jensen supra note 13 at 1146-75.


AFCEA
2010
USSTRATCOM
SPACE SYMPOSIUM
UNITED STATES STRATEGIC COMMAND
OMAHA, NE | NOV 2 – 3, 2010
HOSTED BY
COMMANDER, USSTRATCOM
MARK YOUR CALENDAR!
WWW.AFCEA.ORG/EVENTS/SPACESYMPOSIUM

Challenges to Successful Capability Analysis in Cyberspace

by

Mr. Lee Enemark

Editor's Note: Mr. Enemark's discussion of cyberspace targeting in this article is critical to the emerging doctrine of military operations in cyberspace. It is also a great addition to the legal article by Mr. West. Just as Mr. West used the "Law of Land Warfare" for the basis of his discussion, Mr. Enemark uses currently accepted targeting processes and procedures to frame his discussion of these processes as related to offensive cyberspace operations. This is a very relevant topic of discussion concerning military operations in cyberspace.

Background

This paper will discuss some of the complex challenges in adopting the capability analysis, or "weaponeering," process commonly used for conventional weapons into the cyberspace domain. These valued insights will clarify the capability analysis process for the Joint Functional Component Command for Network Warfare (JFCC-NW) and the CNA community.

Introduction

Capability analysis, or weaponeering, occurs as part of phase three in the Joint Targeting Cycle. During the capabilities analysis phase of joint targeting, the targeter estimates the most likely outcome resulting from employing selected friendly-force capabilities against a specific target to achieve a specific effect. Its purpose is to weigh the relative efficacy of the available forces and systems or processes and agents. Capabilities analysis may also inform the Joint Force Commander's (JFC) choice of Course of Action (COA) and other decision-making processes. Specifically, the targeter focuses on the target's physical, functional, cognitive, and environmental characteristics to determine vulnerabilities that can be leveraged. The Intelligence Community (IC) and federated partners provide target materials, which include estimative analyses essential to assessing how a specific method can affect the target. Any intelligence gaps highlighted during this phase will also refine collection requirements.[1] The product of a capability analysis is typically a weaponeering table, an effects expectancy estimate, and an input into the collateral damage estimate.

The Goal

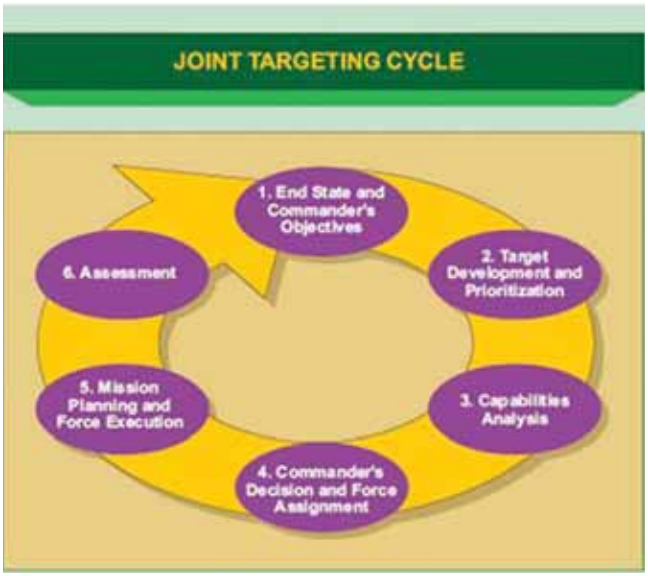
The Computer Network Attack (CNA) capability analysis goal is a user-friendly process that allows targeters to provide the Commander with a clear COA recommendation and an understandable expectation of success for a wide range of CNA weapons and targets. Additionally, the process should fit into the current capability analysis system used by Combatant Commands (COCOM) to be included with other recommendations for conventional weapons and targets that meet Joint Staff requirements. Lastly, the CNA capability analysis process should contribute to CNA weapons acquisition.

The Three Complex Challenges to Capability Analysis

1. There is a lack of historical data to quantify the effectiveness of CNA weapons. Because CNA is so new, there is not a sufficient amount of certified and tested weapons to choose from and little data verifying their reliability. This lack of information makes the existing capability analysis tools ineffective.

2. There is a lack of clear guidance for a rational acquisition process to develop new CNA weapons that all organizations must follow. The military acquisition process is firmly in the hands of the military services to "train and equip" their forces. That is not necessarily bad, but the CNA community has no governing body, such as a program manager or steering group, that drives the procurement of new weapons throughout the CNA community.

3. There is a lack of reliable and easy to use planning tools to support capability analysis and CNA planning. The currently available planning tools do not yet adequately support CNA operations or meet the needs of CNA planners.



The Doctrinal Joint Targeting Cycle
Source: Joint Publication (JP) 3-60 Joint Targeting

Discussion

The process for conventional weapons capability analysis is not applied to CNA weapons. The same rigor and demand for an "approved" conventional weapon system does not seem to apply to computer network operations. A new fighter plane would never be fielded without extensive testing and certification, but that happens fairly regularly with CNA weapons. Although DOD guidance exists that mandates technical assurance, standards for all CNA capabilities[2] and defense acquisition, there are no joint or interagency agreements about what a CNA "weapon" is and what standards must apply for their use in cyberspace.

There is a view that CNA is fundamentally different from the conventional targeting and weapons development processes; that because some aspects of computer networks change very quickly we can't possibly apply the same rules to CNA weapons.

A robust process for CNA capability analysis, weapons acquisition, testing, certification, and assessment has only just begun to gain acceptance in the CNA community. Industry and the Information Operations (IO) Joint Munitions Effectiveness Manual (JMEM) working group is addressing these complex challenges with valued insights for planning tools and processes to support CNA targeting and weapons development.

Although cyberspace is a dynamic environment, there are aspects that remain stable. A core group of weapons must be developed to satisfy the commander's objectives for static infrastructure. Conversely, a flexible, adaptive weapons development process is necessary to address the dynamic elements and emerging technologies (i.e. Twitter, Facebook, Second Life, etc.) in cyberspace.

A core group of available CNA weapons would allow planners to choose from a wide range of planning options and help avoid a unique technical weaponeering solution for each new target. The current computer-based planning tools offer some assistance (e.g. CARRS for technical assurance and C-REA for COA assessments). However, there is a need to become more user friendly and include a much larger database of certified weapons.

Recommendations

1. Establish Joint and inter-agency agreed upon rules and regulations for the development of all CNA weapons, follow the already established acquisition regulations, and enforce those agreements for all CNA weapons developers.

2. Establish program managers for all agencies that produce CNA weapons and follow the guidance of a central steering group in the development and funding of new CNA weapons (as directed in DODIO-3600.3).

3. USSTRATCOM, through JFCC-NW, should provide guidance to the CNA community and central steering group on CNA weapons acquisition and request funding through the defense budget process to support those goals.

4. Support a robust Munitions Effectiveness Assessment (MEA) process to ensure CNA weapons reliability data is updated in existing planning tools and is available for future operations.

5. Continue to work closely within the JMEM process so that CNA targeting is compatible and credible within the existing targeting process.

Footnotes:
1. Joint Pub 3-60, pg. F-1
2. DoDI O-3600.3

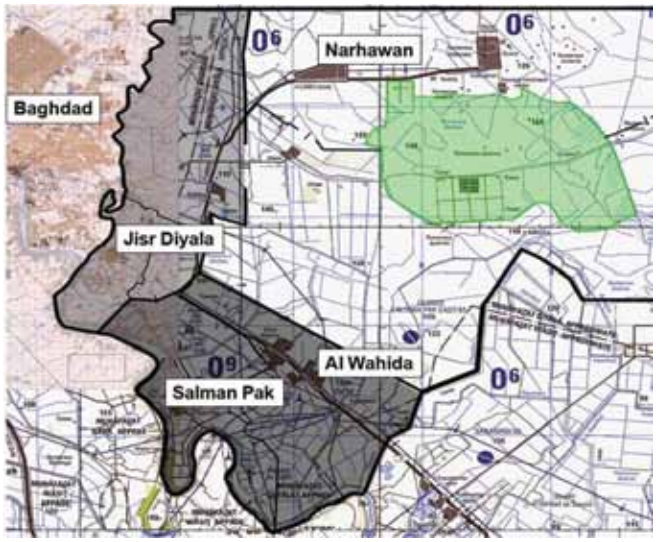
Adapting to the Information Environment in Iraq During the Surge-A Personal View

by

Lieutenant Colonel Nathan Hass

Editor's Note: LTC Hass' observations are relevant for the IO professional and his lessons learned from his experience in Iraq are key to understanding some of the issues in strategic communication related to the current surge in Afghanistan. At the time this article was written the name of Psychological Operations (PSYOP) had not changed. To stay true to the character of this work IO Sphere did not edit or change the name.

"Don't get stuck on specific techniques," my boss, LTC Robert Foley, warned me when I asked for advice and TTPs on how to be a successful Brigade IO officer, "figure out the information environment first because it changes over time and is different from place to place. What works in one area will not necessarily be the best technique in your area." At the time, I was the current operations officer in the G7 Cell with 3rd Infantry Division while it was the headquarters for the Multi-National Division Baghdad in 2005 and LTC Foley was the G7. I wanted his opinion based on working with the various brigades that were operating under him in MND-B. I was slated to be the Information Operations officer for the 3d Heavy Brigade Combat Team, "Sledgehammer" 3d Infantry Division based out of Fort Benning, Georgia. LTC Foley's advice would prove remarkably helpful when the brigade deployed as the third of the "Surge" Brigades in March 2007. Continuous adaptation tied to continuous assessment proved to be the key to conducting IO in our operational environment.



MAP of Mada'in Qada showing proximity to Baghdad and its four major cities.
Source: Author

The Sledgehammer Brigade was responsible for an area roughly contiguous with the borders of the Mada'in Qada which lay to the east and slightly southeast of Baghdad – across the Diyala River and north of the Tigris River. A population estimated at 1.2 million lived in an area roughly the size of Rhode Island. Sectarian strife had exploded since 2005 to the extent that people had been fleeing the area in large numbers. Primarily Shia, the area held pockets of Sunnis primarily along the southern boundary with the Tigris River. One city of 100,000, Jisr Diyala, was so dominated by the Shia extremists it was called "Little Sadr City." Another city, Nahrawan, with a population also around 100,000, was deceptively quiet – and considered a homestead location for many of the Shia extremist leaders. To the south, Salman Pak, a former resort town for Sunni elites during the Saddam era, was the former seat of the Qada government and the epicenter of sectarian strife.

The Brigade mission was to interdict accelerants coming into Baghdad and conduct counterinsurgency operations. My work as the IO officer involved what I called "extending and enhancing" the effects of the Brigade operations – kinetic and non-kinetic – in order to influence the various target audiences by shaping their perceptions. To explain my work, I often used the analogy of marketing and auto manufacturing. Marketers do not merely help auto makers sell their cars after production; they also help the manufacturer to best decide what types of cars to build in the first place. In the Mada'in Qada, the number one product we endeavored to "sell" was legitimacy – legitimacy of the local and national government, legitimacy of the security forces, and legitimacy of our efforts to assist them to make life safer and better for the citizens of the area.

In practice, we accomplished the "front-side" marketing integration through the targeting process. Our commanders and operations officers incorporated it into their decision making during mission analysis and COA development. I had constantly stressed in my OPD's, briefings, and conversations that all operations produced "IO effects" - not just specific "non-kinetic" activity like a television media event, a billboard, or a handbill. I wanted to avoid having leaders think of IO as something added on like "pixie dust" to an operation. Every friendly unit action was a message, or sent a message – even the absence of action sent a message. What we strove to do was to enhance, extend, or reinforce the messages that we wanted our actions to communicate.

Our units incorporated messages into all operations and messages to be used in their engagements that explained the operations. As the BCT IO officer, I helped to synchronize the

messaging, but I quickly discovered that the breadth and variety of our operational environment mandated a loose approach to the message alignment and that the subordinate battalion fire support officers and commanders were very adept at developing messages that were synchronized with the Brigade commander's intent.

For our on-going interactive assessment of the information environment, we sought to discover three things:

1. How information was spread, what "networks" existed, or what habits caused information to spread?

2. What "portals" we could use or create to inject information into the environment?

3. How we could shape the information "networks" or habits to maximize our effects.

How information flowed:

With a strong Bedouin cultural influence, the communities in our part of Iraq were dramatically different from a typical neighborhood in the United States where individuals are relatively "atomized" and information flows primarily from mass-media sources. Most of the people in our area of Iraq lived in the middle of close-knit social network. Frequent conversation within large families, between neighbors and friends within tribal units meant that "word-of-mouth" was a much more powerful venue of information flow than in communities in the United States. The prevalent use of cell-phones reinforced the word-of-mouth channels by speeding them up and extending them geographically. I imagined the word-of-mouth as an information network and various media outlets as "portals" into the network. This meant that a newspaper article read by 5% of the population could easily influence a disproportionate number of people – much greater than the original readers.

The Mada'in Qada had no indigenous media outlets – no newspapers or magazines, and no radio or television stations. Furthermore, reporters from media outlets in Baghdad were afraid to enter the area because of its reputation for sectarian violence. As a result, the Qada government had developed no capacity for engaging the media and despite the word-of-mouth "network" – we found few residents who were aware of the Qada government's efficacy.

Literacy in the area was difficult to determine, but since it was mainly rural and mainly Shia, it was likely lower than the national average for Iraq. However, since primary school education nearly universal and the area possessed a strong literary heritage,…we estimated between 60-70%. We looked at how our opposition and other parties communicated and noted that Al Qaeda handbills were all text, that graffiti used only text – not pictures, and the Sadrist posters and murals used text with images.

The Mada'in Qada area had a tradition pre-dating Saddam Hussein of being a center of culture and literary achievement. The Brigade's Civil Military Officer and I were given the seats of honor at a poetry festival held in the city of al Wahida. The festival attracted the top literary talents of the nation and an audience that participated enthusiastically in the poetry recitation. The event highlighted both the power of the literary tradition as well as the Bedouin emphasis on oral communication.

The consumption of media was similar to that of other areas of Iraq with approximately 80% watching satellite Arabic television, 5-10% listening to radio, and 5-10% reading newspapers. A handful of internet cafes existed, and the internet usage was estimated around 5% by some Iraqis.

Old techniques from OIF III:

The brigade had come to Iraq wanting to repeat some of the successful techniques of the previous tour, but the lack of local media outlets and resistance by the Baghdad media to cover events prevented this from happening initially. Two techniques used successfully in the unit's previous tour were a) having a close relationship with the provincial press officer, and b) access to a successfully operating radio station.

During OIF III, the Sledgehammer Brigade had operated in the Diyala Province and had been partnered with the provincial government. The Diyala provincial government had a press secretary who had organized a press corps of local media outlets. The Brigade enjoyed a close working relationship with the Press Corps that tremendously facilitated achieving rapid information effects on the local population.

The radio station provided the brigade the ability to disseminate messages rapidly and hold radio interviews with local officials. In an indication of how important, the radio station was, the brigade dedicated a mechanized infantry platoon to protect it. However, neither of these techniques was viable in the beginning and we were pressed to adapt and attack the IO problem with a different set of solutions.

Our plan of attack:

We decided we had to attack through every means possible, with the intent that we would mass the effects at the decisive point – the minds of the people in our area. As the IO officer, I was given a mandate "to be the most creative officer in the Brigade" by my boss, Colonel Wayne W. Grigsby Jr. So I adopted an experimental, trial-and-error approach, with nothing off limits. My goal was to try to achieve our effects by pushing on as many methods or "portals" as possible and see which ones would prove to be the most fruitful. In some cases, where there was no "portal" – we sought to create one- changing the shape of the information environment in our area.

Over the course of the fourteen months, we were operating in Iraq, our IO activity fell into five categories of effort:

1. Traditional PSYOP activity – face-to-face, handbills, posters, loudspeaker, leaflets, & billboards.

2. Iraqi and Arabic media engagements – inviting media, primarily satellite television news agencies, to cover a variety of events in our area.

3. IO initiatives – radio station, mural painting, taxi-side ads, city-wide loudspeaker systems.

4. Capacity building – developing the ability of the local government and partnered Iraqi police or Army units to communicate and influence.

5. Rapid response, or "IO counter-fire."

PSYOP Employment:

Our baseline was the PSYOP activity was face to face engagement and loudspeaker operations by the Tactical PSYOP Teams as well as billboards and leaflet drops. We placed our tactical PSYOP teams OPCON under our subordinate battalions and then used the targeting process and our IOWG to provide direction on how to use them. The IOWG we conducted through "Breeze" with the battalion IO officers (all were the multi-hatted battalion Fire Support Officers) – provided a forum for sharing the best Tactics, Techniques, and Procedures for employing the PSYOP assets. One battalion used their Tactical PSYOP Team's loudspeaker to invite more tribal leaders to a Nahia[1] meeting that had been hitherto poorly attended – the next day, over 75 sheiks were present at the meeting. Another battalion used their PSYOP team during an uprising in Jisr Diyala in the spring of 2008 to detect and decisive stop a rumor that coalition forces had been stealing funds allocated for teacher salaries from a school. During a mission to arrest an extremist leader, battalions would have their TPT present with messages ready to explain the arrest to the people in the neighborhood. Battalions also used their TPT loudspeakers for small-scale deception efforts playing tank and helicopter noises. TPTs also conducted non-scientific polling and assessments to gain some feedback on the effects of the various IO efforts. When the battalions briefed their CONOP to the brigade commander and staff 48 hours before the mission, I had another opportunity

Iraqi Local Media News Conference
Source: Author

to provide input on how they used their TPT to enhance the mission. The Tactical PSYOP Teams provided our battalion commanders a significant and responsive capability to inform, influence, and assess in their AORs.

Iraqi / Arabic Media Engagement:

Because of the lack of any media outlets in our AOR and the high number of people who watched satellite television, we put a lot of energy toward attracting the Iraqi television media. Our division G7 provided invaluable assistance here by setting up procedures for requesting Iraqi media through the Iraqi Media Engagement Team (IMET) and providing helicopter transportation and an interpreter and escort for the media.[2] The G7 required a request form five days prior to the event and a "CONOP" three days prior. These two documents helped the G7 shop make the coordination, but they also guided us to plan the event with sufficient detail. Initially, I fought the requirement for the detailed request form because I knew that it would inhibit the battalions from requesting Iraqi media coverage of the events in their area. What I discovered however, was that the request format became almost like a rehearsal and helped to ensure that we had a common picture of the event from the platoon to division level.

The lack of media operating from within our AOR posed enormous challenges logistically, but proved to be a boon in regards to granting us the ability to shape the story we presented to the media. The extremists in our AOR (and Iraq in general) had been so hostile toward the members of the media that they would not cover any events without military security escort. Ironically, that fact tended to reduce the extremists inclination to stage high profile-media targeted events – such as bombings of markets or government buildings. The extremists designed these types of events to achieve effects at several levels. Locally the events affected the people directly affected, but the most important target audiences – throughout the rest of Iraq, the Middle East, and the world; these were reached by drawing media coverage of the event. During my first tour in 2005, we noticed that some media outlets always seemed to be on scene before anyone else and we suspected that these outlets were being alerted by extremists ahead of time ("something is going to happen at noon on Haifa Street"). In our AOR, the extremists were never able to achieve that sort of effects extension through media coverage because they had made it unsafe for the media to travel except under the umbrella of our security. This allowed us to have the first and last word – to shape the story and frame the discussion.

With encouragement from COL Grigsby, we set out to increase the number of media events conducted each month in the Brigade's operational environment. We started off conducting only two events per month in July and August, 2007, but then double the number in September and doubled again in October. We accomplished this through tasking subordinate units via the Target Cycle FRAGO with verbal emphasis provided by the Commander. I strove in the tasking language to strike a balance between providing clear direction through detailed task, conditions, and standards without reducing the subordinate units' flexibility and initiative. A typical direction in the Target Cycle FRAGO was for each battalion conduct no less than two events – to average one per week per battalion. The media events were incredibly complex operations with every echelon from platoon to division working in synchronization to create a successful outcome.

IO Initiatives:

Given my charter to "be the most creative officer on the staff," I set out to try any and all techniques that I had heard of or had seen being used in other places. The urgency of the surge meant that I couldn't work on these in serial fashion to see which would work best. Instead, we worked on all of them almost simultaneously. We sponsored local artists to paint murals. We contracted with local businessmen to place stickers on the ubiquitous taxis in the area. We contracted for the construction of a city-wide public address system. We built a small radio station, the "Voice of Mada'in," to provide a local, rapid response, and interactive method for communicating. When the Sons of Iraq movement developed in our AOR, we developed a newsletter that we distributed through their chain of command. Finally, we developed the plans for a small local newspaper – to be produced by the Qada public relations cell.

Murals:

There was already a precedent for painting murals on the concrete walls that had been erected in Baghdad to protect neighborhoods and marketplaces, so it was not hard to find local artists to contract for the murals. The Chief Executive of the Mada'in Qada helped us with the bidding process by putting out the information from the statement of work and collecting the bids. We asked the artists to provide us with a sketch of their mural concept, but I wrote the statement of work to give them the maximum latitude to exercise their artistic creativity.

A local artist painting a mural in Al Wahida
Source: Author

Local Taxi with Banner
Source: Author

We could have just given them one of our PSYOP products and told them to paint it, but I was convinced that they could – if they understood the intent – produce an image that would resonate more strongly within the local cultural context. We were not disappointed. The feedback we received from people in the area was overwhelmingly positive. We intended the murals to provide positive images that promoted unity and reconciliation, but the artists were bolder than I expected creating several murals with strongly anti-extremist themes.

Later, when the Malaki administration was contending with the Basra uprising in the spring of 2008, someone painted threatening graffiti on the walls outside one of the Qada government building. We noticed that the person painting the graffiti had avoided defacing the murals that were on this wall, so we decided to paint over the graffiti with murals as part of the counter-propaganda effort.

Taxi-side ads:

This idea originated after I read a paper on IO by BG Cardon, our division's DCG/S, who had suggested bus-side ads in a list of communication techniques. When we looked into it, we discovered that there were no local bus companies in our AOR. The Qada Chief Executive suggested taxi's instead. It turned out that taxi's were used extensively in our AOR. Some were marked with the traditional taxi signs on the roof and were used as full-time taxis, but many others were part-time taxi's, had no markings, and appeared to be a means of supplemental income for the driver.

We conducted one run of taxi-side ads, placing them on about 1,500 vehicles.[3] The contractors we worked with had the ability to do the graphic art work and print stickers. As with the murals, I wanted the graphic artists to communicate directly within their culture, so we gave them the latitude in the contract to use their creativity to create messages and images to communicate our themes. The result, we realized when we saw the proofs, were much better quality than we expected.

Taxi-side ads themes were oriented toward building legitimacy of the local government and many of them featured photos or photo montages of projects that the local government had coordinated. We wanted to keep the message very positive to avoid making the taxis into targets for the extremists.

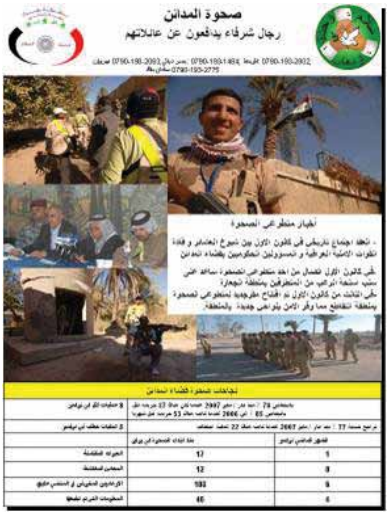
City-wide Public Address System:

I got the idea for the public address system from an article I read about a system a Marine Corps unit had set up in Ramadi. Their system utilized sophisticated equipment and was controlled from the local Joint Security Stations (JSS). They had developed the system because there were no local media outlets, the population had a relatively low literacy rate and few had radios. Our area seemed to have some of these characteristics, so we were eager to try this out. The statement of work for the contractors indicated that they would utilize locally acquired PA system equipment – using equipment similar to what was used in mosques to broadcast the cleric's sermon. We wanted to make sure that the local government would be able to maintain it and replace components if they were damaged.

Sons of Iraq Newsletter:

The movement that was originally known as "the awakening" started in our area in August 2007 and spread north and then east from the area around Jisr Diyala. A critical part of our counter-insurgency effort, the Sons of Iraq not only greatly facilitated our clearing operations; they became the all-important holding force that kept the cleared areas safe after they were opened up. The Brigade Commander directed us to develop a product that would publicize the impact they were having and help build their espirit d 'corps. Additionally, he wanted us to utilize the Sons of Iraq networks and chains of command as the method of distribution since that would ensure placement of the product to tens of thousands of men in our area.

Recognizing the relatively low literacy levels among the Sons of Iraq volunteers, we created a one page product that we published twice per month or once per target cycle that made heavy use of photo-imagery. The top half of the newsletter was all photos- primarily the excellent photos taken by our COMCAM team. The middle contained 3-5 bullet sentences mentioning accomplishments by the various Sons of Iraq elements. At the bottom we created a small "scorecard" which we updated with each edition. The scorecard announced how many road side bombs were recovered and estimated how many lives had been saved as a result. The feedback we received from our battalions was that the Sons of Iraq leaders and rank and file loved the way the newsletter portrayed their efforts and they especially enjoyed seeing photos of themselves making their neighborhoods safer.


صحوة المدائن
رجال شرفاء يدافعون عن عائلاتهم

Sons of Iraq Newsletter
Source: Author

Joint Information Operations Education Programs

Sponsored by the Joint Command, Control and Information Operations School

The Joint Command, Control, and Information Operations (IO) School (JC2IOS) is one of four schools residing within the Joint Forces Staff College. The IO Division within JC2IOS conducts the Department of Defense's only certified course for the education and training of Joint IO planners. The Joint Information Operations Planning Course (JIOPC) is a 4-week DOD-directed prerequisite for personnel assigned to joint IO planning billets and is taught at a classified level. Following orientation to the IO core, supporting and related capabilities in the first week, the students are broken into 6-10 person staff planning groups. The remaining 3 weeks of the course are spent in hands-on practical application using scenario based planning exercises.

JIOPC Graduates:

- **Understand the complexity and construct of the Information Environment (content and flow)**
- **Know Joint IO Theory and Doctrine and understand core, supporting and related IO capabilities and their potential effects in the operating environment**
- **Know and demonstrate individual proficiency in the Joint Operational Planning Process (JOPP) and the completion of IO planning and execution products**
- **Graduate fully prepared to serve as a lead IO planner in a Joint IO or IO-related planning position.**

The IO Division also conducts a 1-week Joint IO Orientation Course (JIOOC). The JIOOC can be taught in residence or conducted by Mobile Training Team (MTT). Past MTT audiences include multiple COCOMs, support to intermediate and advanced service PME, service IO education programs and inter-agency audiences.

The Joint Forces Staff College is the Accredited Institution for IO Education and is part of the National Defense University System. The JIOPC is the Joint Staff certified course for IO Training in U.S. Department of Defense.

For More Information

Web: http://www.jfsc.ndu.edu/schools_programs/jc2ios/io/default.asp

Contact the Registrar: LTC Hugh Mullaly
Phone: (757) 443-6333 DSN 646-6333
Fax: (757) 443-6035, DSN 646-6035
E-Mail: mullalyh@ndu.edu or jc2ios-io@ndu.edu

Voice of Mada'in Radio Station:

Initially, I did not place a high priority on starting a radio station since it appeared to be a very low bang for a high buck given the relatively low numbers of people who we believed would listen to the radio. However, guidance from my commander based on the need to have a rapid response communication tool, overrode my opinion. We made three attempts at creating a radio station before we had success. The operator of a radio station that had been in operation for 4 years on a Coalition Forces' FOB proved to be a wealth of information on how to run a radio station. He also knew people with radio experience who we could hire to work at our station and offered to be a contractor to purchase the radio station equipment and put the station into operation.

We discovered however, once the radio station became operational, that it had potential beyond what we realized as well as problems we had not anticipated. The people in the local government and people on the street seemed to genuinely proud that they had a radio station – it was the first in the Qada. We knew from small scale surveys our PSYOP and CA teams had conducted that there were few radios being used in homes. Most cars we observed had radios, however, and we believed that with marketing, we could increase the listener base. The radio station developed a logo and we ordered thousands of stickers with the logo on it to help spread the word about the station. After the station had been in operation a couple months, our PSYOP teams were receiving feedback that people were familiar with the logo and knew about the station. We also used our TPTs to prompt people directly to listen to the radio station and call in to ask questions during the interactive talk-shows the station conducted with local leaders.

Capacity building:

Simultaneously, another of our goals was to build capacity in the local government to conduct Information Operations – which we re-named Public Relations. This was an effort that required months of engagement and persuasion – notably from our Brigade Deputy Commander – COL Ryan Kuhn. With help from the USAID, we were able to help fund the hire of an individual in January 2008. The individual we hired proved to be intelligent, eager, hard-working, and capable. Previous to hiring Ali, I would join COL Kuhn during his weekly engagement of the Qada Mayor and have a portion of the meeting where I could discuss public relations with the Mayor. With a counterpart on the local government staff, however, I went on combat patrols to the local government building more often and was able to meet with Ali for much longer than I could with the Mayor. Through our ePRT we were able to assist Ali in acquiring equipment – cameras, voice recorder, etc. Before our Brigade redeployed in May 2008, we were able to do all the planning and preparation to expand the PR officer into a PR section of 5-6 people who would fulfill three functions. They would report on events in the Qada to create media products for distribution to Iraqi news outlets, coordinate Iraqi media coverage for events, and publish their own small newspaper.

IO Battle Drills:

From the beginning, we recognized the necessity to act quickly on occasion to affect the information environment. We understood that in the effort to influence the population we faced a competition with other narratives for the conflict and that in this competition time mattered. If an event occurred that could have an adverse impact on the opinion of the population

Voice of Mada' in Radio Station
Source: Author

toward us or toward the Iraqi government and its security forces, we knew we had to act quickly to frame the discourse as much as possible so that our narrative could possibly overcome that promoted by our adversaries. We called our tool for acting quickly "IO CONOPs." For our IO CONOPs, we borrowed from other units and then refined them for our situation as we gained experience.

Three broad categories of incidents demanded quick reaction by the brigade:

1. An action by the enemy – such as an assassination or bombing – designed to create negative effects in the information environment for the Government of Iraq, the Iraqi Security Forces, or Coalition Forces.

2. An action by Coalition Forces or the Iraqi Security Forces – like collateral damage or an escalation of force (EOF) incident or the arrest of a member of the community – that had potential to create negative effects in the information environment

3. Or actions by other parties, not necessarily "enemies" – such as demonstrations – that had potential to create negative effects.

The battle drills provided a template for action by various members of the brigade staff, the brigade commander and for the battalion commanders and staff. Most of the battle drills were reactive, but some were proactive. Our battle drills reflected the necessity of coordination, collaboration, and empowerment of our local community leaders. The drills also proscribed a decision point for determining actions by echelon. The seriousness and scope of the incident generally determined whether the actions would occur at company, battalion, or brigade levels. We ended up with four CONOPs which we incorporated into our brigade tactical standard operation procedure (TACSOP).

IO CONOPs and their functions:

1. "Turnover" – For minimizing negative effects of Coalition Forces (CF) or Iraqi Security Forces (ISF) actions that result in destruction of life, property, or essential services. Frame the story truthfully and explain the purpose of friendly actions in order to disrupt adversary misinformation and propaganda efforts. Facilitate rapid response to deny insurgents ability to gain sympathy from the local populace.

2. "Clear Window" – For exploiting negative SIGACTs: IED detonation, SAF, kidnapping, EOF. Dislocate the adversary from LN support by emphasizing that the atrocities and crimes are committed by the AQI and militias. Emphasize the purpose of ISF and CF actions are to promote security and safety. Get our story out before the insurgents and force the insurgents to react to our messages.

3. "Calm Weather" – For managing civil demonstrations. Influence local leaders and populace to avoid violence. Set conditions for a return to a safe and secure environment.

4. "Good Neighbor" – Consequence management for CM for CF/ISF Raid, Cordon & Search, Counter-fire & Area Denial fire. Prevent local population interference. Clarify CF/ISF intentions and actions. Empower local leaders. Influence local population to support the GOI and ISF. Foster integration and coordination between ISF and GOI.

US Medic Treating Iraqi Civilian Per the IO Battle Drill

Source: Author

A few months after we began operations in the Mada'in Qada an artillery round fell "short" during a terrain denial mission. The round struck a home in a small village along one of our main routes and killed the mother and one child and seriously wounded another child. The battalion involved notified the brigade headquarters immediately and several members of the brigade staff held a quick huddle to determine how we would assist the battalion. The huddle included the Brigade Civil Military officer, the Brigade Public Affairs officer, the Brigade PSYOP planner, and me. A combination of PSYOP and Civil Affairs and the battalion commander went to the scene and addressed the village leaders and the family we were able to engage. We promised a thorough investigation that we would share with them and emphasized that our terrain denial fires were intended to help make things safer for everyone. We also fast-tracked the [need more details about this event] salasia payment to the family and helped repair the damage to the home. We contacted local civic leaders at the Qada and Nahia levels and explained what had happened – empowering them with factual information and allowing them to assist us with the repair of the damage writ large. The fact that we acted quickly, sensitively, and in collaboration with local leadership transformed what might have been a major setback into a closer relationship with the leaders in the community.

Assessment and Effects:

We never forgot the guidance that our division commander, MG Rich Lynch had given us that IO should inform, influence, and assess. In each of the categories of effort we developed measures of performance and measures of effectiveness. The measures of performance were the easiest to track – number of leaflets dropped, number of media events conducted, number of radio interviews. The measures of effectiveness were much more challenging. While we made attempts to conduct a methodical, statistically reliable and detailed survey, most of our measurements of effectiveness came from anecdotal indicators. The measures of effectiveness mattered for prioritizing our efforts along the various lines of attack, but our goal remained to attack along as many avenues as possible to achieve mutually reinforcing effects on our target audiences.

From our targeting process we had developed three over-arching and over-lapping desired effects we sought to create on our decisive target audience – the local population:

1. Support the local government.

2. Support the local Iraqi Security Forces.

3. Withdraw active and passive support from the extremists.

To achieve these effects, we had to shape perceptions about the level of security, about the effectiveness and responsiveness of the local government, and about the prospects of economic and cultural improvement. At the same time, we had to defeat any extremist misinformation, adverse rumors, or propaganda. In marketing terms – we had one primary product to "sell" and that was legitimacy.

Of course, there had to be coherence between what people were experiencing personally and the perception we were attempting to engender. If a message did not match what people were experiencing – the message would be discredited, but if it matched, and if we were able to present multiple, coherent messages through a variety of methods- then the message would be reinforced and the perception shifted. We respected the ability of the target audiences to interpret what they were seeing based on their own mental frameworks. We believed that the message coherence and its focused, repetitive application would be the best method for shaping that mental framework.

To illustrate the difficulty with quantifying effectiveness, I'll use our Iraqi media effort as an example. Our measure of performance was the number of media events we were able to facilitate- which was easy to measure, but the measure of effectiveness involved estimating how many people were reached with the message and how that message had influenced them toward the effects we desired. We knew that people had begun to perceive that there were improvements in security – families had been moving out of the area when we had arrived, we noticed them moving back in increasing numbers into the area starting in December of 2007. Some of the returning people told one of our battalion commanders that they had heard about the improvements on the Iraqi satellite television stations. The chief executive of the local government told us that his friends in Syria and Jordan – themselves former residents of the area – had called him because they had seen his speech at the opening of a key government building opening on Iraqi satellite television. These friends, we were told, were full of questions about how things had improved – that they had immediately recognized the significance of the building opening since it took place on one of the sectarian fault lines. On another occasion, we had an Iraqi journalist from Al Fayha television tell SFC McInnis, the Brigade PSYOP planner, that he especially wanted an interview with our commander because the improvements in Mada'in Qada and the work of the brigade were known throughout southern Iraq.

Staff Funnel:

As soon as we commenced operations in Iraq we were quickly noticed a problem with the modular brigade structure – a problem we called "the staff funnel." The critical addition of the new functions at the brigade level was not accompanied by an increase in capacity at the battalion level, yet the battalion-level was where most of the execution took place. As a result the much smaller battalions' staffs were manned with people who were multi-functional. In our battalions, the Fire Support Officer was the IO officer. These were very hardworking officers were tasked with executing 3 to 5 key functions simultaneously – they were often the battalion Civil Military Officer, Pay Agent, Fire Support Officer, and Public Affairs Officer – along with the traditional FSO function. Given the emphasis in the Hammer Brigade that the brigade staff worked for the subordinate commanders, we sought to help the battalions by doing as much of the staff work as possible at our level.

With the media requests that the brigade had to give our division headquarters, it would have been easiest (for us at Brigade) to simply pass the empty forms down to the battalion IO officer since he had all requisite detail needed. Instead, to reduce the workload below us, at brigade we generated 80% drafts of the media requests and media event CONOPs based on verbal notifications from the subordinate units. These 80% drafts were then sent back to the units for refinement and completion. We discovered that it was not that difficult to develop a 70 to 80% solution with very little information. Giving a mostly completed planning framework for the subordinate staff gave them something to work off. They were not constrained by our work and could modify it as much as they saw fit.

Happily, our division G7 cell led by LTC DeCarvalho also operated according to a similar staff ethic. They minimized their staff information requests while maximizing their ability to provide us with the resources we needed. As a result, I was freed up to focus the majority of my time and energy on managing the IO planning and execution within the brigade- and importantly ensuring that the battalions received the support they needed to conduct information operations at their level. While there were the inevitable inter-echelon frictions, I have to give credit to the way the hard, selfless work by our Division IO cell made a significant difference on my ability to provide IO support to our subordinate battalions.

IO Working Group (IOWG):

Because our subordinate units were dispersed geographically to their Combat Outposts (COPs), our initial IOWGs were largely ineffective. The battalion LNOs were adequate for their primary purpose of representing the battalion for most missions in the Brigade TOC, but proved unable to provide the interactive representation of the battalions' IO officers that we needed for the IOWG. This situation eventually led me to stop holding working group sessions after a few months since I seemed to get more of the requisite coordination work done via email and phone calls than trying to improve the linkage between LNOs and the battalion IO officers. I didn't want to hold a meeting for the sake of holding a meeting and tie up several staff member needlessly. So, in keeping with my experimental approach, I decided to try not holding an IOWG for a while to see if we could function.

However, after operating without a weekly IOWG for a couple months, the necessity for getting our subordinate IO officers into a forum together began to emerge. Partly this was due to the way one battalion was using their PSYOP team much more effectively than the others. That battalion, a Field Artillery unit, had a warrant officer as their IO officer who had extensive experience conducting information operations in a previous tour. We also needed to update them on their requests for support for various IO actions such as support for

US and Iraqi Key Leader Engagement
Source: Author

Iraqi media events and the production and delivery of PSYOP products. Additionally, I wanted to improve the crosstalk between the battalions and improve our awareness of the information environment across the Brigade's AOR. The key was using Adobe Connect to hold a virtual meeting.[4] That allowed our subordinate units and the various members of the Brigade Staff to participate without physically co-locating at the Brigade headquarters. For the format, I provided each subordinate element a slide format and gave them a suspense each week to send me their updates. The bulk of the meeting became the subordinate units talking about what they had done during the previous week and what they had planned for the next week. They also discussed the events of significance to the information environment in their unit AOR. In addition to the synchronizing of the Brigade support for their planned IO actions, these discussions facilitated my staff supervision of my subordinate unit staff counter-parts by giving me a venue to provide guidance and advice.

Conclusion:

As a brigade Information Operations Officer I found myself facing unique challenges when my brigade deployed to the Mada'in Qada in Iraq. While somewhat helpful in giving me a clearer understanding of how to integrate into the staff organization of the brigade, the training prior to arriving in Iraq did not fully present the unique challenges of conducting information operations in a COIN environment.[5] I had to adapt rapidly upon arrival and learn "on the fly." Since the brigade assumed responsibility for an area in which a US brigade had not operated before, I was limited in what I could use from the partial relief in place that we executed. I found myself remembering the advice of my old boss and realized my first task was to discover the nature of the information environment. That discovery process continued through the entire 14 months we operated in the Mada'in Qada. The process involved more than just various methods of assessment; it was also discovery through trial and error. Furthermore, as a brigade, we also sought to influence the nature of the information environment itself- such as our efforts to expand the radio audience for the radio station. In the end, we had indications that our largely successful. People were moving back to our area whereas they had been moving away when we first arrived- and they directly cited the Iraqi media coverage as a factor in changing their perception. People ignored the extremists' "night letters" giving them to our forces without concern whereas before they merely would have remained silent and uncooperative. These effects were not created solely by Information Operations, but by actions of the brigade, lethal and non-lethal, that IO enhanced and extended.

Footnotes:

1. Nahia was a political unit similar to a "township" that was usually named after a major town or city, but included the area around the city and several smaller villages in that area.

2. Initially in MND-C, Iraqi media was handled by the Public Affairs Office. In the summer of 2007, the division shifted the Iraqi and Arabic media coordination function to the G7. Within the brigade, we divided the function in the same way between the Brigade Public Affairs Officer and me.

3. We were not able to do subsequent runs of the taxi-side ads because the restrictions on CERP expenditures in the 2d quarter of FY 2008. The blind bidding process we employed had not caused us to receive the lowest price per unit and we discovered later that we had the ability to get a much lower prince through more of a negotiating process with the contractors. We also realized that to get the saturation impact we wanted from the taxi-side program, we needed to increase the numbers to around 8,000 placements. That boosted the overall cost to the point where other projects took priority, so we never executed a second iteration of the taxi-side contracts.

4. It was a cadre member from the National Training Center visiting our Brigade who asked me about why we were not holding IOWGs. When I explained the difficulties, he asked if I had tried Adobe Connect, and I had to admit the idea had simply not occurred to me. About the same time, CPT Damond Davis, the FSO from 3-1 CAV who was my staff counterpart for that unit, had begun to clamor for some type of meeting or forum to discuss IO issues and support. I realized then that there was a need for a meeting that would actually help solve problems and save time and effort- and that it was feasible using Adobe Connect.

5. It is difficult, even at a CTC, to present a brigade IO officer with training scenarios that realistically present the full complexity of the information environment. There are not enough people or enough time in the training scenario. While the CTC's have gone to great lengths to replicate the problem set that BCTs encounter- such as hiring scores of Iraqi-Americans to live in the replicated villages, the brevity of the training rotations means that responses by the population are scripted rather than sincere responses to the brigade's Information Operations efforts. Our CTC rotation, however, was valuable for those of us on the Brigade staff for giving us an introduction to how the staff would work together and work with the subordinate units.

IO SPHERE

Deputy Secretary of Defense Lynn and General Chilton Speak to the Media at the Second Annual Cyber Symposium

Omaha, NE—(May 26, 2010) The second annual Cyberspace Symposium co-hosted by the Armed Forces Communications Electronics Association International (AFCEA) and US Strategic Command (USSTRATCOM) provided a forum for the Deputy Secretary of Defense William J. Lynn and USSTRATCOM Commander Kevin P. Chilton to speak with members of the media on the subject of the warfighting domain of cyberspace. Media representatives from several media outlets attended the question and answer forum and IO Sphere was included.

Cyberspace, and the US Defense Department's roll in it, has undergone a tremendous transformation since the inaugural Cyberspace Symposium in 2009. Both Secretary Lynn and General Chilton were reflective on the improvements in the previous year. Deputy Secretary Lynn remarked that "DOD has recognized Cyberspace for what it is as a new domain of warfare."

Highlighting that commitment was the activation of US Cyber Command (USCYBERCOM) in May 2010 with a planned full operational capability in fall of 2010. Cyber Command is a four star level sub-unified command under US Strategic Command. US Army General Keith Alexander is the first commander of Cyber Command.

General Chilton was most impressed with the progress and level of individual training and expertise that DOD and the services emphasized in the past year between the 2009 and 2010 Cyberspace Symposiums. "There has been absolute progress in policy and training across both the joint force and the services. The Secretary of Defense has made the Joint Cyber Course a high priority for DOD. The Air Force has focused the 24th Air Force on Cyber Operations, and the Navy has done the same with the 10th Fleet. Everyone has made Operations Security and the proper use of social media more of a priority," Chilton said. He acknowledged that there is much more to do on both the organizational level and the individual level but the trends are all in the right direction. On the specific subject of the use of social media General Chilton commented that, "Social media is not a bad thing, but it must be understood by the service members, our civilians, and our contractors."

A continuing point of concern that remains is the international legal framework of operations in cyberspace. Secretary Lynn acknowledged that the legal framework is not necessarily more of a challenge but it is very different from the legal framework of other warfighting domains. Secretary Lynn stated, "The internet does not respect sovereignty, and a large part of it is privately owned and not connected with any government. It is not necessarily a greater challenge than the legal framework of other operations but it certainly is a different challenge. Cyber is a dimension that is harder to predict when determining threats and targets."

Both Secretary Lynn and General Chilton look forward to the next Cyber Symposium to provide another year of benchmarks for the developing domain of cyberspace. They acknowledge that all the forces must sustain and increase focus on training and knowledge to maintain momentum in the field and that the roll of Cyber Command will be critical in the future defense of the nation.

Secretary Lynn and General Chilton Speak with Media at Cyber Symposium
Source: defenseimagery.mil

Operational Art and Targeting Strategy for Cyberspace Operations

by

Lt Col Sam Arwood, Lt Col (Ret) Robert F. Mills, and Maj (Ret) Richard A. Raines, PhD

Editor's Note: This article is a shorter version of a longer academic submission on several issues of cyberspace operations. The authors have modified the submission to fit the publishing guidelines of IO Sphere. Cyberspace targeting is a critical issue for cyberspace operations. This submission is thought provoking and perfect for this issue of IO Sphere.

Abstract

There has been much written about cyberspace, the potential of cyber warfare in general, and organizing cyberspace operations capabilities (who's in charge). However, there is little discussion about specific theory, doctrine, and how cyberspace capabilities can be integrated with other traditional military capabilities to influence an adversary, create desired effects, and win wars. The purpose of this paper is to stimulate conversation about operational art in cyberspace. Specifically, we present a planning approach that ties together national strategy, instruments of national power, and a well-known targeting strategy for complex systems. The result is a method of selecting targets that can be traced to higher-level strategies and outcomes.

Introduction

In December, 2005, the US Air Force announced that it would begin organizing, training and equipping a force to fight and win in cyberspace. This was an important step in recognizing that in addition to being an enabling domain for operations in air and space, cyberspace was in itself a warfighting domain in which there are peer competitors who will use and exploit the domain to advance their own interests. Because cyberspace is inherently a joint operating area and used by all service branches, the Army, Navy, and Marine Corps are also developing cyber forces unique to their service needs. The military services organize, train, and equip forces, but combatant commanders actually employ those forces. To provide better command, control and oversight of operations in cyberspace, the Department of Defense (DOD) has created a new sub-unified command, US Cyber Command. USCYBERCOM was activated (initial operating capability) on May 21, 2010 and has the following mission:

USCYBERCOM plans, coordinates, integrates, synchronizes, and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.[1]

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…**Secretary of Defense William J. Perry, October 1994**

The primary focus of USCYBERCOM is on protecting and defending DOD networks, and a major objective will be "pulling together existing cyberspace resources, creating synergy that does not currently exist and synchronizing war-fighting effects to defend the information security environment."[2]

The evolution of cyberspace as a warfighting domain has generated much controversy, excitement, confusion, and perhaps fears. Who's in charge? What resources will be available to support this mission area? What's "in" cyberspace and what's not? Is someone trying to take over our mission area? How do we develop a force to operate in this environment? Much of this consternation came from the newness of the domain and our inability to "get our heads around it." Even defining cyberspace was problematic, but in a May 12, 2008 letter, Deputy Secretary of Defense Gordon England defined cyberspace as "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."[3]

Although we now have a standard definition for cyberspace, we are still lacking in theory about how to fight in the domain, and we need a doctrine for employing cyber power at all levels of warfare. This is not the first time we've struggled with this. There are many parallels between our current understanding of cyberspace and air power back in the 1920s. At that time, the air domain was originally seen as a supporting domain (e.g., reconnaissance and close support to local ground commanders), but early air pioneers such as Billy Mitchell believed air power could do much more than simply provide tactical support to ground forces.

While there are certainly parallels between cyberspace and the early days of air power, we should avoid simply replacing all references to "air and space" with "air, space and cyberspace" (which seems to be happening with many Air Force publications). No doubt, the other services will tend to see cyberspace through their own biases and culture, and this is to be expected. When discussing the evolution of

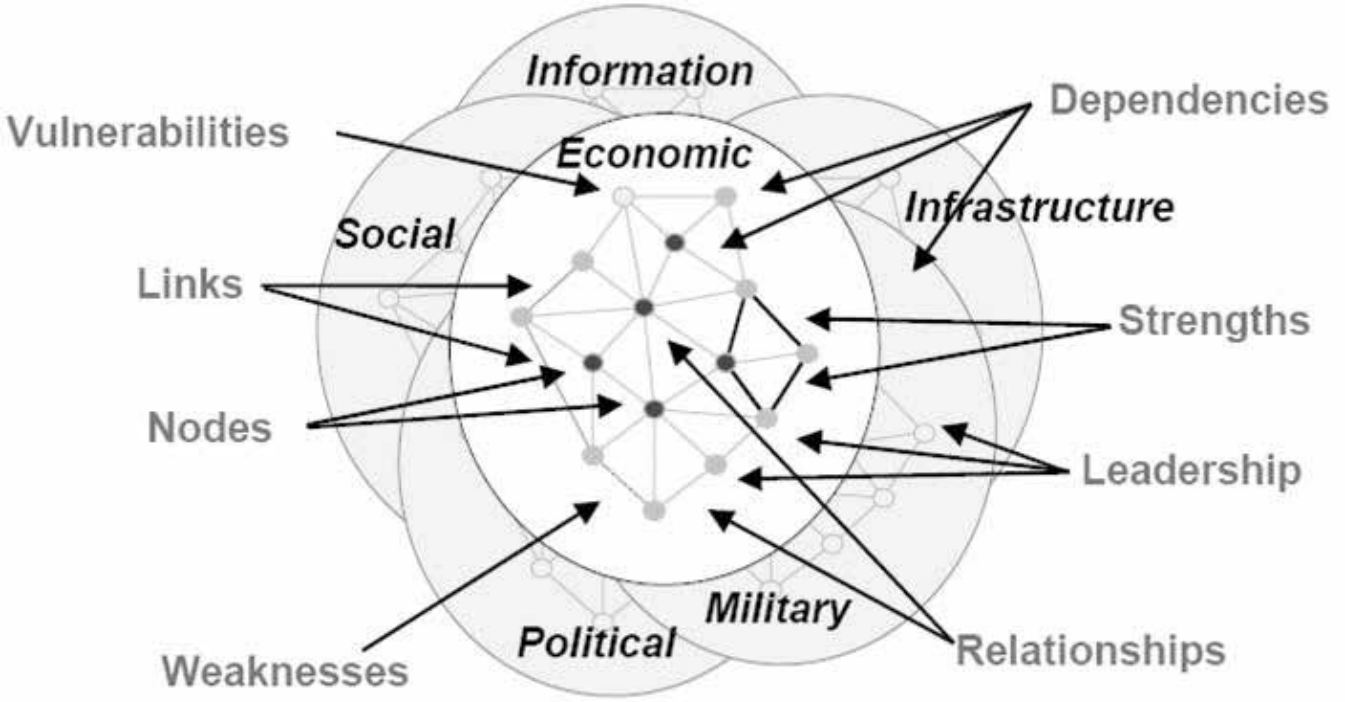


Figure 1. System of Systems Analysis [12]

early command and control doctrine for air power, Kenneth Allard wrote "… these developing perspectives of Land, Sea and Air combat tended to represent syntheses of old doctrines geared to new circumstances."[4] That is, when faced with something new, we tend to just take what we already know and try to make it fit the new situation.

We need to avoid such self-limited thinking. We need to develop people, technologies, processes, and doctrine that will enable us to fully develop and exercise our capabilities in the cyberspace domain, or we risk missing some truly transformational approaches to warfare. We need individuals who understand the possibilities this new environment presents as well as Mitchell and his fellow air pioneers understood the true potential of air power. They saw air power as much more than a ground support activity; likewise, cyberspace is much more than an enabler of operations in air, land, sea, and space.

With air power, we established capabilities, developed theory and strategy, and wrote doctrine based on lessons learned—and then we organized into a separate service. In some ways, we seem to be doing things in reverse order with cyberspace. We have established organizational constructs (e.g., USCYBERCOM, 24th Air Force, and Fleet Cyber Command) but as yet we have little in terms of cyberspace operations theory and doctrine.[5] We have an abundance of theory regarding employment of power in the land, sea, air and space domains, but what do we know about employing power and operational art in cyberspace? The purpose of this paper is to stimulate conversation about operational art in cyberspace. Specifically, we develop a planning approach that links our national strategy, effects-based planning, and a variant of a well-known targeting strategy used by the Air Force.

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.
John F. Kennedy[6]

Strategy and Instruments of Power

Strategy development integrates ends, ways, and means. It is the combination of actions and behavior (ways), using available resources and capabilities (means) to achieve some desired objective (ends). At the strategic level, the means include the instruments of national power (INP)—diplomatic, informational, military, and economic, also known simply as the "DIME." When planning operations at the operational level of warfare, military planners must have a thorough understanding of the national strategic objectives. Planners must also understand that military efforts may be used as the main effort, or they may be subordinate to nonmilitary efforts. Finally, planners must understand how military actions support and integrate with the application of the other INPs.

As the global environment has become more complex, the DIME construct has evolved. DIMEFIL (or MIDLIFE) is an extension of DIME to include financial systems, intelligence, and law

enforcement. These additional INPs are a direct result of the increasingly joint, combined, and interagency nature of modern operations. DIMEFIL traces its roots to the United States' strategy for fighting terrorism, which says the nation will employ military capabilities in conjunction with diplomatic, financial, intelligence and law enforcement activities "to protect the Homeland and extend our defenses, disrupt terrorist operations, and deprive our enemies of what they need to operate and survive."[7] Although counterterrorism was a focus for the evolution of DIMEFIL, the framework can apply to all operations involving interagency coordination, which includes cyberspace.

Implications of Cyberspace

There should be little argument that our increasing dependence on information technology has blurred the lines between the information instrument of national power and the others. In today's information age, it is difficult to wield diplomatic, military, economic, or any other kind of power without a solid information infrastructure. This is not to say it is more important than military or economic power, but information is certainly the glue that holds everything together. As noted by US Secretary of State Condoleezza Rice, "It is a paradox of our times: the very technology that makes our economy so dynamic and our military forces so dominating – also makes us more vulnerable."[8] Consider the nation of Estonia, whose national security was severely threatened by a series of coordinated cyber attacks that nearly crippled the country. During the height of the attacks, citizens lost access to basic government services, online banking, newspapers, and many other sources of information. The Estonian defense minister called the attack a national security situation that "can effectively be compared to when your ports are shut to the sea."[9]

Defensive issues aside, cyberspace presents a wealth of potential targets when building a campaign plan. The challenge is deciding how to select targets to achieve the desired effects.

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, 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.

The heart of strategic air power theory was the idea that wars could be won by striking at the heart of the enemy rather than having to grind through a protracted terrain conflict. The ability to compress time and distance by flying over the battlefield made air power unique. Cyberspace and cyber power have the potential to be as transformational as air power was. Cyberspace may even be more challenging because it is a domain in which we already have peer competitors, it is tailor-made for asymmetric warfare, attacks can be launched from anywhere in the world, and attack attribution can be extremely difficult.

As we develop a theory of cyber power, we must consider cross-domain effects. Operations through cyberspace may affect the land, sea, air, and space environments. Conversely, there are things we can do in the other domains to create effects in cyberspace. There is not a clear boundary around cyberspace, nor is it just a virtual place—many potential targets, such as network routers, servers, transmitters, radars and optical sensors, will exist in the physical and cyberspace domains. Consider a cellular phone tower that is known to be part of a C2 system for terrorists or criminal actors. We can deny the adversary's use of cyberspace by hacking into the cell phone system and shutting it down, whereas a kinetic option might include a precision air strike. Conversely, cyberspace can be used to deliver hard, real destruction in the physical environment, as Department of Homeland Security experiments involving electrical power

	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

Figure 2. Warden's Five Rings Model [16]

generation and distribution have demonstrated.[10]

Targeting Methodologies

What we are most interested in is bridging the gap between strategy (employment of ways and means to achieve a desired objective), centers of gravity (COGs), critical nodes and links, and finally targets against which our INPs can be applied. The targeting process is well known and somewhat independent of the domain (air, land, sea, space, or cyberspace). Targeting is about determining an adversary's vulnerabilities and/or COGs and bringing power against those points to create the desired effects.

PMESII

General Peter Pace, former Chairman, Joint Chiefs of Staff, explained the importance of this linking INPs and targeting in his 2006 Memorandum on Joint Professional Military Education:[11]

The PMESII model mentioned above uses complex systems theory to analyze the operational environment in terms of interconnected nodes and links (Figure 1). PMESII is rooted in System of Systems Analysis (SoSA) theory, which attempts to identify, analyze, and relate the goals and objectives, organization, dependencies and inter-dependencies, external influences, strengths, vulnerabilities, and other aspects of the various systems. The objective is to determine the significance of each PMESII system to the adversary in order to assess systemic vulnerabilities and how they can be exploited or influenced to create effects.

Warden's Five Rings

Air Force Colonel John Warden developed a model for air campaign planning to address what he saw as gaps in the Air Force's ability to think at the operational and strategic levels of warfare. His "Five Rings" model provided the basis for success in the Gulf War and is further developed in his articles "The Enemy as a System"[13] and "Air Theory for the Twenty-first Century."[14] What made Warden's model (Figure 2) so useful is that it provides a simple way to break complex systems down into subsystems that are more tractable. These subsystems have COGs that can be held at risk in order to influence a larger system.

Figure 3. Seven Rings Model

At the strategic level, these subsystems can be viewed as target groupings that affect national power and will. Warden's concept implied that, for example, fielded forces may not have to be directly engaged if the adversary could be convinced to surrender by attacking other rings, such as leadership or system essentials. Debates continue with respect to how the rings should be viewed, and whether the approach should be from the outermost rings in, or the innermost rings out.[15] These debates are useful for determining how best to use the process, which will ultimately add to its effectiveness as a concept for developing a campaign plan that is tailored for a particular situation.

There are similarities between Warden's rings and the PMESII framework. Both models include similar factors (military, infrastructure) albeit with different levels of abstraction. The PMESII model allows for more complex analysis, because nodes and links can be studied within and between the PMESII subsystems. Warden's model, on the other hand, is commonly used within the Air Force for targeting and operational planning. For simplicity, we will continue with Warden's rings, recognizing that the concepts presented could be applied using a more rigorous PMESII analysis.

With the addition of cyberspace to our warfighting domains, we need to expand our thinking beyond what Warden discussed. Warden included lines of communication under leadership, which would include traditional communications systems (e.g., telephone or radio), and any attack against that capability would be worthwhile under Warden's model—classic command and control warfare. His rings concept predated the idea of a cyberspace domain, but he did recognize the importance of information in future warfare: "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."[17] The storage, movement, control, and flow of information are the items of interest as we look at warfare in cyberspace.

Another gap in Warden's original rings concept is the absence of financial and economic institutions as a class of targets. A nation is limited in its ability to wield power if its economy is weak or its citizens are unable to buy goods and services, to include food. When dealing with such a nation, a preferred strategy might be to limit an adversary's means to barter before we eliminate or damage their organic essentials, especially considering the post-conflict rebuilding process. If the population loses its ability to engage in fair trade, or access to its monetary resources, how long can the nation resist, militarily or otherwise? The point here is that stock markets, commodity markets, currency mints,

treasuries, and banks are potential targets when attempting to affect an adversary's will to fight, regardless of the means of the attack.

The concept of "attack" does not necessarily imply military action. As discussed earlier, DIMEFIL was developed to account for the application of other instruments of power in combating terrorism. We use a form of "attack" against financial organizations that control funds for terrorist organizations by confiscating funds or freezing accounts. This applies pressure against the adversary's financial and economic COGs, and these types of target sets should be accounted for in the rings concept. Warden's rings model is therefore applicable across all of the instruments of power.

We therefore offer an extended version of Warden's model that includes two new rings, as shown in Figure 3. The information systems ring would include electronic and traditional systems such as data storage and processing facilities, communications nodes, communications support systems, and government and public records. Financial organizations would include financial markets, market regulatory organizations, and facilities that control the collection, storage, or production of currency. One might argue that information systems and financial systems are already included in Warden's model (infrastructure or system essentials), but we believe these additional rings help segment the target sets to highlight the potential contributions that cyberspace operations may bring to the fight when considering all the instruments of national power. The placement of the new rings is somewhat arbitrary, but we believe it is more important to recognize that these subsystems are present and should be factored into the targeting process.

Putting It All Together

DIMEFIL represents the instruments of power and how they can be used as part of a strategy to achieve objectives. Warden's model was developed to provide insight into how a complex system (nation-state, drug cartel, terrorist group) would be attacked via its centers of gravity, with emphasis on defeating the organization. DIMEFIL and Warden's model are thus the means and ways portions of the strategy equation, respectively. In this section, we develop an operational level planning approach that links objectives (ends) to the seven rings and DIMEFIL. At the strategic level, a nation will employ its INPs against appropriate COGs to achieve desired effects. The means and targets are not limited to military capabilities. INPs are not used in isolation and are in fact most effective when employed in a coordinated manner. Interagency (i.e., whole of government) coordination is a necessity. In executing this coordination, national and military strategy must be at the heart of the effort, as is articulated in our national strategy for combating terrorism:

> ***The paradigm for combating terrorism now involves the application of all elements of our national power and influence. Not only do we employ military power, we use diplomatic, financial, intelligence, and law enforcement activities to protect the Homeland and extend our defenses, disrupt terrorist operations, and deprive our enemies of what they need to operate and survive.***[18]

There are many connections between the INPs and the seven rings (Figure 4). Each INP represents a capability (means) that a nation has with which it attempts to influence others. From a targeting standpoint, each INP is also a system of systems, with each subsystem represented by a ring in the targeting model. For example, the military instrument of power has fielded forces (soldiers), leadership (chain of command), population (combat support), system essentials (supplies, fuel,

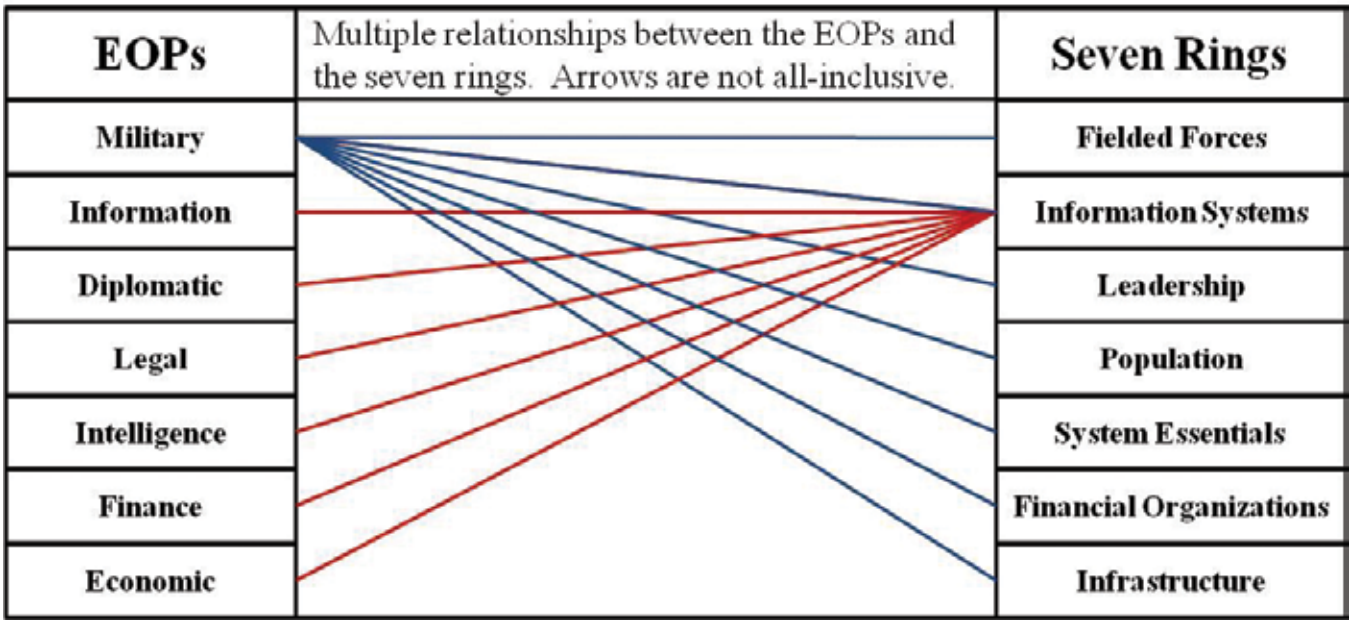


Figure 4. Mapping INPs to the Seven Rings

ammunition), and infrastructure (bases and garrisons). To represent the various connections between INPs and target rings, we develop a combat power matrix (CPM) shown in Figure 5. The CPM is a support tool for targeting and enables the use of all INPs in a coordinated manner.

The CPM can be used for both offensive and defensive planning purposes. From a defensive perspective, it helps identify which branch of the government should take the lead and help determine and mitigate internal risks and defeat an adversary's strategy. System of systems analysis would be used to determine appropriate centers of gravity for each targeting ring in order to assess and document weaknesses, vulnerabilities, and single points of failure. A risk or vulnerability accepted by one is shared by all because of cyberspace's pervasive nature. Furthermore, adversaries do not have to attack us in accordance with how we organize. For example, if the military has hardened networks, a determined adversary may choose to attack us elsewhere and still achieve their desired objective.

From an offensive perspective, the CPM identifies targets as well as which area of the federal government with which the military should interact to validate its assumptions about the effects this target choice may have. Targets would also be validated, perhaps using a "gain/loss" analysis while relying on subject matter experts from other agencies. Clearly, the law of armed conflict must be considered.[19] The Allied strategic bombing campaign in World War II included attacks designed to degrade Germany's industrial and economic capacity to wage war. Such damage may be seen as acceptable in a protracted conflict, but in a short or limited conflict, identifying a military advantage from attacking such targets might prove difficult. "Stock exchanges, banking systems, universities, and similar civilian infrastructures may not be attacked simply because a belligerent has the ability to do so…targeting analysis must be conducted for computer network attacks just as it traditionally has been conducted for attacks using traditional weapons."[20]

As an example of how the CPM can be used, consider the military INP (the third row in the CPM). Leadership functions would include commanders, headquarters units, national security advisors, and of course the commander-in-chief. System essentials would include information (pervasive), fuel, oil, electricity, ammunition, and other consumables necessary for the military to be effective. Financial organizations and systems would include budgeting, programming, accounting, finance, and contract management. Information systems include command and control; intelligence, surveillance and reconnaissance (ISR) systems, and information technology infrastructure.

Seven Targeting Rings

Instruments of National Power	Leadership	Information Systems	Finance	System Essentials	Infrastructure	Population	Fielded Forces
Diplomacy	President or Prime Minister, Ambassadors, Diplomatic Liaisons, State Level Diplomats, Secretary of International Affairs, Attachés	Passports, Green Cards, Work Permits, Visas, Foreign Visitor Systems & Data, 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, Combatant Commanders
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 & Backups, 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 (Comm'l & Govt), IP Tier1 & 2 Facilities, Trunk Lines, Microwave, Satellite, Telephone Libraries, TV & Radio Stations, Newspapers & 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
Military	Military Commanders, National Level Military Headquarters, National Leaders, National Security Advisors, Combatant Commanders, CEOs of Military-Industrial Base Corporations, Terrorist Organization Leadership, Military Support Corporations	Command & 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 Roll, Finance and Accounting Orgs, 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	Command & Control Facilities, Air Fields, Ports, Railroads, Armories, Depots, Highways, Roads, Radio & SATCOM Facilities/Antennas, Telephone Systems, Power Generation & Distribution, 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
Economic	Commerce 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
Finance	Treasury Department Secretary, Federal Reserve Chairman & Board, Chief of National Banking Structure, Mint Chairman	Account 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 Couriers	Accounting & Finance Officers, Contracting Officers, Currency Couriers
Intelligence	National Intelligence Agencies (Military & Civilian), Intelligence Advisors to National Leadership	ISR Systems/Platforms, Intelligence Networks, Mapping Databases & Systems, Targeting Systems, Tasking Systems	Budgeting & Finance, Intelligence Disbursement Records, Contract Records	Information, Electricity, Food, Water	Radio & SATCOM Facilities/Antennas, Intelligence Production Facilities	Private Intelligence Corporation Staff (Satellite Imagery & Data Miners), General Population	Intelligence Officers, Counter Intelligence Officers, HUMINT Officers, Analysts, ELINT Personnel & Resources, ISR Platforms & Operators
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, Criminal/Court Records & Databases, Firearms Registration, Drivers License, Birth Certificates/Records	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, Penal Institutions, 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

Figure 5. Combat Power Matrix

Infrastructure elements would include air fields, military posts, depots, and the defense industrial base. Population would include reserve forces, draft age population, contractors, and civilian employees. Finally, the fielded forces would include uniformed military forces and their equipment (aircraft, fighting vehicles, and ships for example).

Conclusion

In this paper, we have attempted to fill in what we see as a void in current cyber power discussions. Specifically, we have focused on the strategic and operational levels of war, hoping to add clarity and fodder for further discussions on how cyberpower can be employed to achieve national military and strategic objectives. Our approach combines the use of the DIMEFIL instruments of national power and a targeting model based on Warden's Five Rings. The result is a combat power matrix model that we believe will help military planners better link capabilities (means) and targets (ways) to achieve the desired effects (ends). The matrix is useful for both defensive and offensive purposes and facilitates coordination and planning at the interagency level. The approach could easily be adapted to suit alternative targeting philosophies, such as the PMESII method used in effects based planning.

Footnotes:

1. US Cyber Command Fact Sheet, May 25, 2010, http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf.

2. Ibid.

3. Deputy Secretary England's definition was released to ensure Department of Defense activities were more consistent with National and Homeland Security Presidential Directives (NSPD-54/HSPD-23) which seem to be more focused on interconnectedness of systems rather than the physical medium (electronics and electromagnetic spectrum). The new definition does not explicitly mention the electromagnetic spectrum, but the increasing use of wireless communication systems would still seem to fit within the definition of an "interdependent network." Joint Publication 1-02, DOD Dictionary of Military Terms, uses the same definition as in the DEPSECDEF memo.

4. Kenneth Allard. Command, Control, and the Common Defense (Washington DC: National Defense University Press, 1996), page 93.

5. Joint Publication 3-13, Information Operations, defines information operations (IO) as the "integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own." EW and CNO are clearly related to the cyberspace domain, but this does not mean cyberspace operations should be treated as a subset of IO. IO can be performed in all domains of warfare, and significant portions of IO are indeed performed in and through cyberspace. However, the objective of IO is to influence an adversary's decision making processes, whereas cyberspace operations are focused on controlling the cyberspace domain. These are related but different concepts.

6. John F. Kennedy, Remarks at Annapolis to the Graduating Class of the US Naval Academy, June 7, 1961, http://www.jfklink.com/speeches/jfk/publicpapers/1961/jfk232_61.html.

7. National Strategy for Combating Terrorism (NSCT), September 2006, http://www.whitehouse.gov/nsc/nsct/2006.

8. National Security Advisor Condoleezza Rice, quoted in USA Today, 6 February 2002, http://www.usatoday.com/tech/news/2001-03-23-rice-cyberterrorism.htm.

9. Johnny Ryan, "'iWar': A new threat, its convenience – and our increasing vulnerability", NATO Review, Winter 2007, http://www.nato.int/docu/review/2007/issue4/english/analysis2.html.

10. Jeanne Meserve, "Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid," CNN.com, 26 September 2007, http://www.cnn.com/2007/US/09/26/power.at.risk/index.html.

11. General Peter Pace, 2006 Joint Professional Military Education (JPME) Special Areas of Emphasis (SAEs), http://131.84.1.34/doctrine/education/sae_2006.pdf.

12. Joint Publication 5-0, Joint Operation Planning, 26 Dec 2006, http://www.dtic.mil/doctrine/jel/new_pubs/jp5_0.pdf.

13. Col John A. Warden III, "The Enemy as a System," Air power Journal 9, no. 2 (Spring 1995), http://www.air power.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/warden.htm.

14. Col John A. Warden III, "Air Theory for the Twenty-first Century," in Battlefield of the Future, http://www.air power.maxwell.af.mil/airchronicles/battle/chp4.html.

15. Major Russell J. Smith, "Developing an Air Campaign Strategy," Chronicles Online Journal, 23 Nov 1999, http://www.air power.maxwell.af.mil/airchronicles/cc/smith.html.

16. Warden, "Air Theory for the Twenty-first Century."

17. Ibid.

18. National Strategy for Combating Terrorism.

19. The law of armed conflict includes the following principles: distinction between combatants and noncombatants; military necessity; proportionality; superfluous injury; indiscriminate weapons; perfidy; and neutrality.

20. Department of Defense Office of General Counsel report, "An Assessment of International Legal Issues in Information Operations", May 1999, http://www.au.af.mil/au/awc/awcgate/DOD-io-legal/DOD-io-legal.pdf.

Cyberspace Target Systems Analysis

by

Mr. James D. Jones

Introduction

Although knowledge of cyberspace and other such computer terminology is prevalent today, over familiarity, without comprehension, negatively impacts targeting and intelligence processes and products, specifically "Cyberspace" Target Systems Analysis (TSA). There are three factors worth recognizing to appreciate the misnomer of a "Cyberspace" TSA. First, understanding of what a functional target system is and its purpose. Establishing a functional target system enables you to correlate its criticality to TSA. Second, from a military perspective, a targeter needs to understand domains and how military operations are conducted within such domains. Third, the authoritative definition of cyberspace definitively illustrates the inaccuracy of conducting a "Cyberspace" TSA.

To accurately conduct, what is erroneously-named, "Cyberspace" TSA there are two challenges that should be resolved. First, locating where the Information Environment resides within the four domains and how cyberspace aligns with it. Second, to the extent possible, identifying, defining, and categorizing all components that could make up a functional target system that operates in the cyberspace global domain.

Once these challenges are resolved, a TSA can be conducted on, what could be notionally called, the Information Technology Infrastructures (ITI) target system. This categorization will transform this elusive problem set into a tangible target system that targeters can analyze to produce nodal system analysis studies that provide the baseline for target selections that create desired effects that achieve the commander's objectives.

Risks to Incorporating Computer Terminology to Targeting

Although usage of the term "Cyberspace" is commonplace in today's vernacular, over familiarity with it can lead to inaccurate application in military circles in general, and in the military targeting and intelligence community specifically. In the desire to rapidly incorporate the lexicon of cyberspace, the internet, and other such "computer lingo" into established targeting and intelligence processes and products there is a risk of haphazardly applying the terminology. This risk comes from not understanding the actual definitions of these terms or if the Department of Defense (DOD) has equivalent definitions. Without this understanding, combining these terms will likely confuse or obscure current targeting and intelligence processes. For example, stating that you are developing a "Cyber-Joint Intelligence Preparation of the Operational Environment (JIPOE), making a "Cyber-Electronic Target folder, or even creating a "Cyberspace- TSA," creates nuances that affects how, or if, you can develop these products. Prior to TSA production, much less a "Cyberspace-TSA, an analyst or targeter must first understand the definition of a target system.

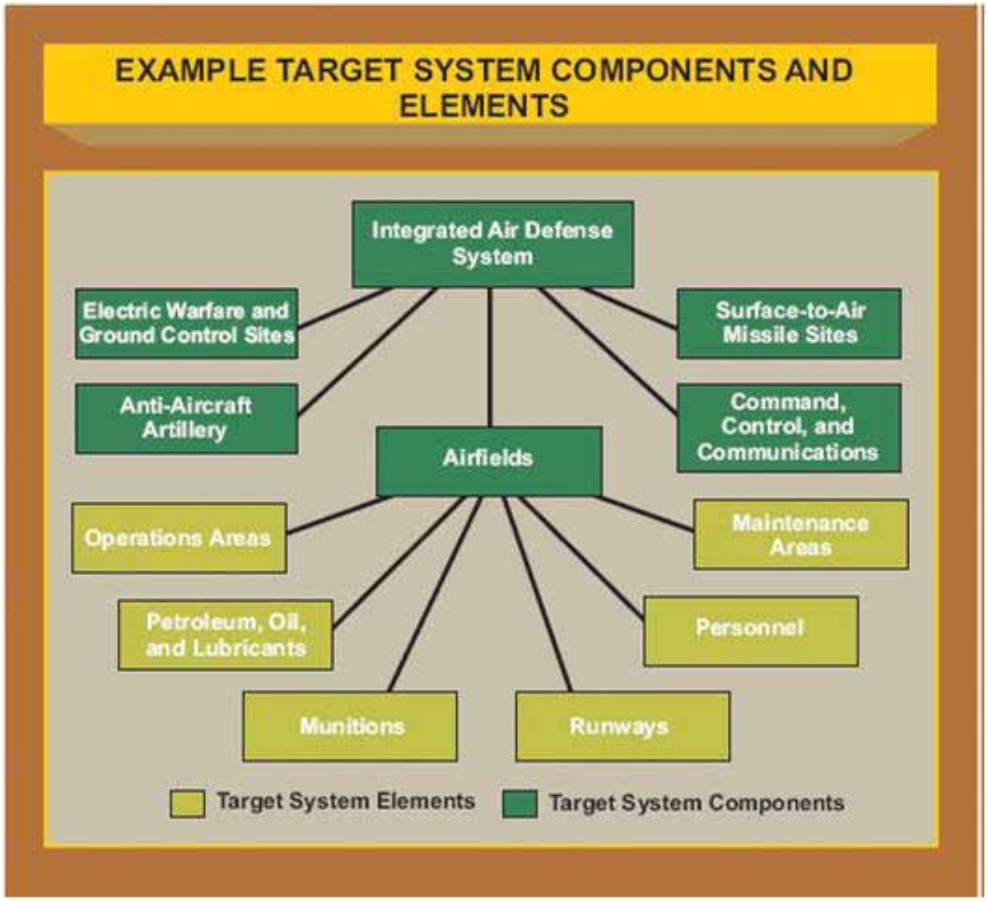


Figure 1. JP 3-60 Joint Targeting

What is A Target System?

Joint Publication 3-60, Joint Targeting defines a target system as, "All the targets situated in a particular geographic area and functionally related…A group of targets that are so related that their destruction will produce some particular effect desired by the attacker."[1] The figure below depicts an example Integrated Air Defense Forces target system from the 14 functional target systems.

The purpose of the 14 functional target systems is to help create specific target sets used to develop targeting courses of actions (COA) and monitoring a commander's objectives through Battle Damage Assessment (BDA). Understanding what a target system is and its purpose gives an accurate foundation to build on when conducting the two primary steps to TSA, target system identification and target system component identification. This highlights the challenges about completing a so-called "Cyberspace-TSA," identifying a "cyberspace" functional target system and its "cyberspace" target system components. A natural follow on question to these challenges is where does the "cyberspace" target system activity take place?

Where should a "Cyberspace" functional target system operate?

Military action, forces, and capabilities operate or function in different domains. The term domain is not listed in the DOD Dictionary, but Webster's II New Riverside University Dictionary provides one that will serve our purposes. One definition states that it is, "A sphere of activity, interest, or function."[2] Militarily speaking, domains are part of a commander's operational environment and consist of the "air, land, maritime/sea, and space"[3] domains.

Using the air domain as an example and paraphrasing it with Webster's definition results in: "The air domain is the sphere where activities, interests, and functions of aerodynamic actions (friendly and adversarial), relevant to the commander's operational environment, takes place."

As seen in Figure 1, the Integrated Air Defense System (IADS) is a functional target system that operates in the air domain. In addition to knowing the domain, a TSA can be conducted on it because the target system and its' target system components have been identified. This adds another challenge to previously mentioned issues noted as identifying a "cyberspace" functional target system and its "cyberspace" target system components. This challenge asks the question, what domain, in the commander's operational environment; does the "Cyberspace" functional target system operate?

The "Ground Truth" about Cyberspace

On May 12th 2008, the Deputy Secretary of Defense (DEPSECDEF) put out a memo stating the definition of cyberspace for the DOD. The memo states that cyberspace is:

"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." [4]

The memo additionally states that, "this definition will serve as the foundation upon which the Department will further mature this warfighting domain." Figure 2 is a visual depiction of this definition.

This definition authoritatively establishes for the military and other DOD affiliates that cyberspace is a domain. By adapting the aforementioned paraphrase as, "The "cyberspace" domain is the sphere where activities, interests, and functions of Internet Protocol (IP) based communication actions (friendly and adversarial), relevant to the commander's operational environment, takes place."

Just as an airplane must adhere to the laws of aerodynamics to function in the air domain, there are laws of "cyberspace" that all IP-based communication means (internet, computers, cellular & satellite phones, etc…) must adhere to as well.

There are basic components that aircraft must have to operate in the air domain, be it a hang-glider, the Wright Brothers' plane at Kitty Hawk, or the latest fighter aircraft. For example, knowing the basic components of an adversary's fighter aircraft aids in the understanding of how to interdict that aircraft or defend against its' used in the air domain.

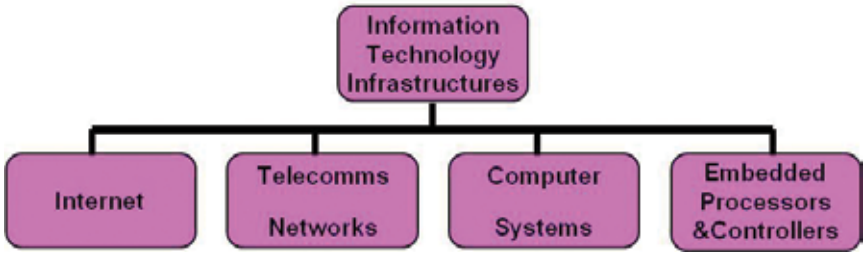


Figure 2. Adapted from Deputy Secretary of Defense Memorandum: "The Definition of Cyberspace" 12 May 2008

Similarly, there are certain basic components that all IP-based communication means must have to operate in the cyberspace domain. Knowing the basic components of these IP-based communication means will also aid efforts to interdict or defend against an adversary's use of these things in the cyberspace domain.

Its' axiomatic to state that a target systems analysis is only conducted on target systems as previously defined, but the point is raised to highlight the inaccuracy of conducting a "Cyberspace" TSA. Just as you would not conduct a TSA on the air, land, sea/maritime, and space domains, the cyberspace domain should be excluded as well. There is a need to identify the target systems that utilize the cyberspace domain and conduct TSA on those systems. Prior to trying to identify these systems and conducting a TSA, there are two more challenges that should be resolved.

Where is the "Information Environment?

The DEPSECDEF memo stated that cyberspace is, "a global domain within the information environment..." The information environment has been defined as, "the aggregate of individuals,

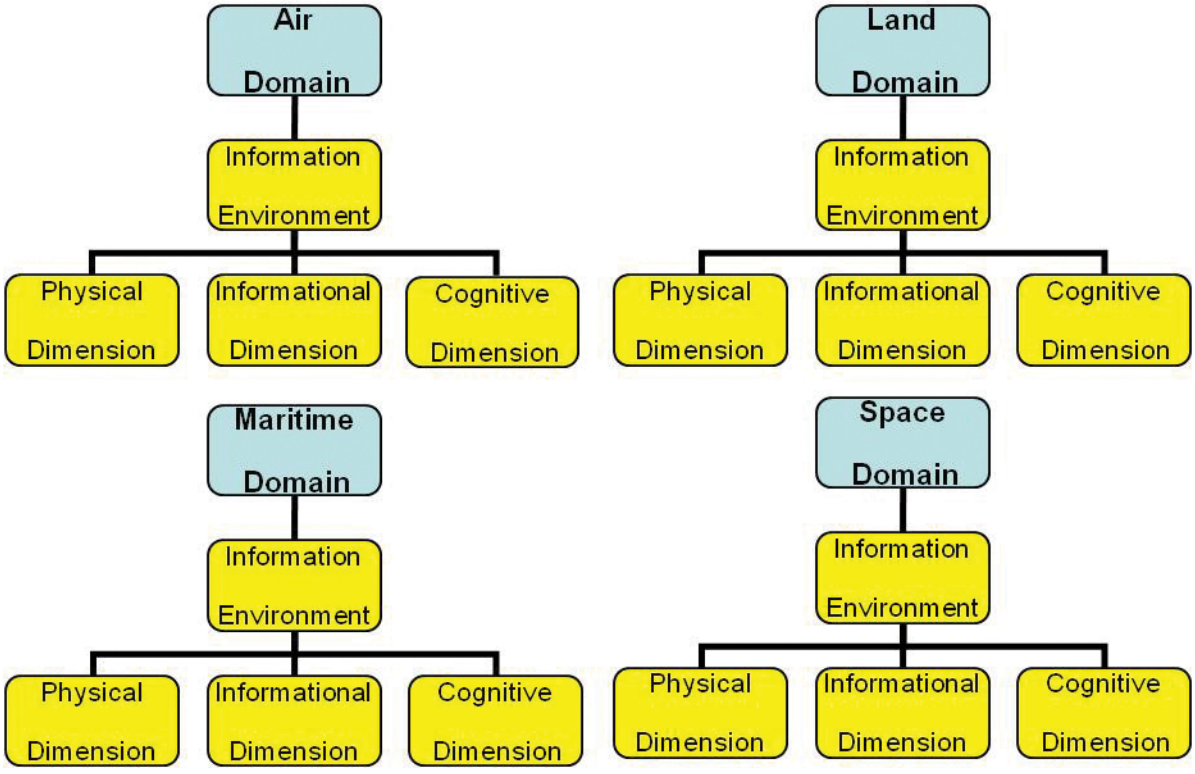


Figure 3. Adapted from JP 3-13: Information Operations, Information Environment "within" the four domains of the Operational Environment.

organizations, and systems that collect, process, disseminate, or act on information."[5] The three dimensions of the information environment are physical, informational, and cognitive. There is conflicting information in Joint Doctrine on where the information environment resides. As the illustration below shows, JP 3-13, Information Operations, states that, "Even though the information environment is distinct, it resides within each of the four domains."[6]

This is in contrast with JP 3-0, Joint Operations (see Figure 4 on the next page), which states that the information environment, "transcends the four physical domains…is a pervasive backdrop to the physical domains of the JFC's operational environment."[7]

The DEPSECDEF's memo has established cyberspace as a global domain and as such provides the grounds for the information environment transcending the five domains as stated in JP 3-0. Figure 5 is a depiction of how the information environment, the cyberspace global domain, and other four domains can be integrated. This representation shows that cyberspace, as a global domain, truly transcends the other four domains and as such, should not be embedded within those domains. Nonetheless, categorizing all IP-based communication means that utilizing the cyberspace domain into target systems is the final obstacle to conducting what is erroneously labeled, "Cyberspace" TSA.

A New Functional Target System?

As previously established, cyberspace is the domain in which all IP-based communication means reside and function on. Those "means" need to be characterized as a target system, as TSA is concerned and crucial at determining the functional relationships in and between target systems.

Just as adversary, aircraft are target; characterize system elements of the Air Forces & Air Fields and Integrated Air Defense Forces functional target system, so too should the adversary's various IP-based communication means as target system elements of an "Internet" functional target system. Having the internet characterized as a target system will greatly aid targeting efforts by scoping the internet and various IP-based means into more manageable target system components and elements more readily analyzed by targeting professionals. Establishing this target system will enhance the accurate selection and prioritization of targets and the matching of an appropriate response to those targets based on the commander's objectives.

The DEPSECDEF memo stated cyberspace is "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."[8]

Although not all inclusive of all IP-based communication means, I recommend using the memo as a prototype for creating an "Information Technology Infrastructures" (ITI) target system with its' respective target system components and elements. Figure 6 below gives an example of how a target system like this could be categorized. The biggest challenge in creating this target system will be the identification of all the target system components that fit under the ITI umbrella and standardizing

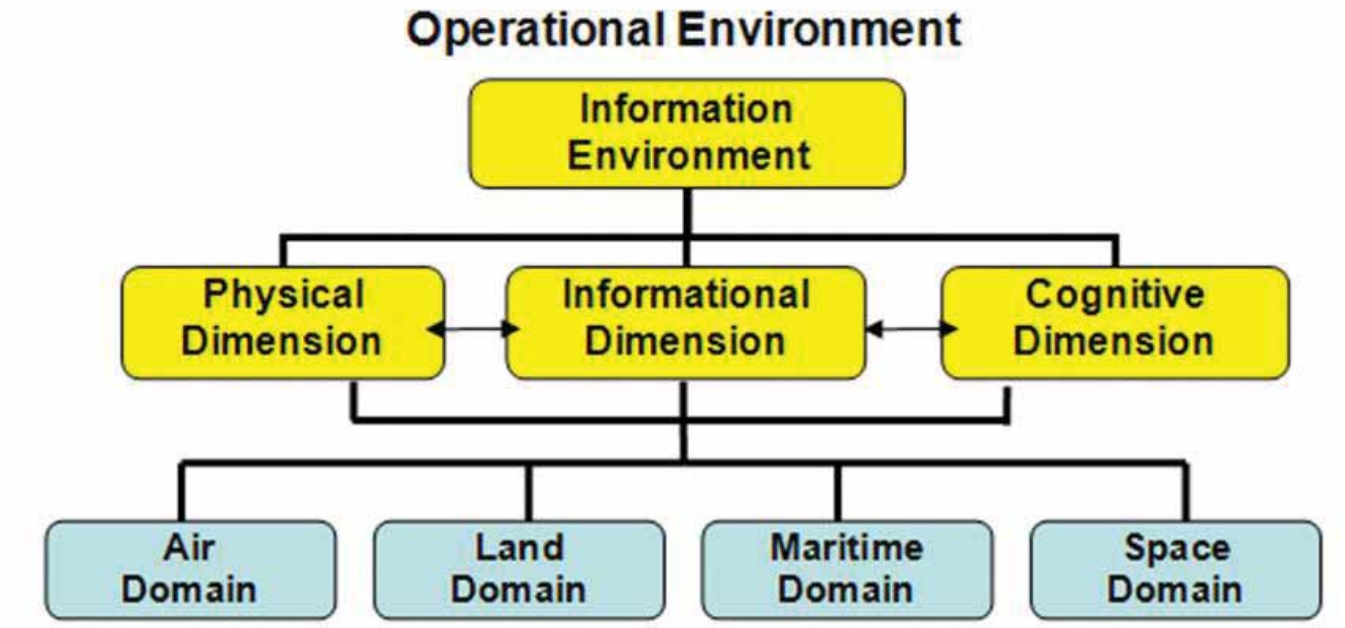


Figure 4. Adapted from JP 3-0: Joint Operations, Information Environment "transcending" and as a "backdrop" to the four domains.

the taxonomy associated with the target system components and elements, a whole other effort beyond this paper. Once this target system is complete, a TSA would be more manageable and would provide nodal analysis studies that could be used as a baseline for target selections that create the desired effects to achieve the commander's objectives.

Conclusion

This article examined how over familiarity of computer terminology without comprehension negatively affects targeting and intelligence processes and products to include the inaccurately named "Cyberspace" Target Systems Analysis (TSA). The three factors to be understood to appreciate the misnomer of a "Cyberspace" TSA are:

1. The definition of what a functional target system is, its' purpose and how it relates to TSA.

2. Clarifying domains and their use for military operations.

3. Understanding the DEPSECDEF's cyberspace memorandum, that cyberspace is a global domain and how conducting a "Cyberspace" TSA is a fallacy.

Finally, the article addressed, with respect to the four domains, where the Information Environment actually resides and how cyberspace aligns with it. Additionally, it stated the importance of categorizing all components and elements of a functional target system that would operate in the cyberspace global domain. Finally, a recommendation was made to use the DEPSECDEF's memo as a prototype for creating an "Information Technology Infrastructures" (ITI) target system with its' respective target system components and elements. It would be this target system that a TSA could be conducted on and the result would be target selections that create the desired effects to achieve the commander's objectives.

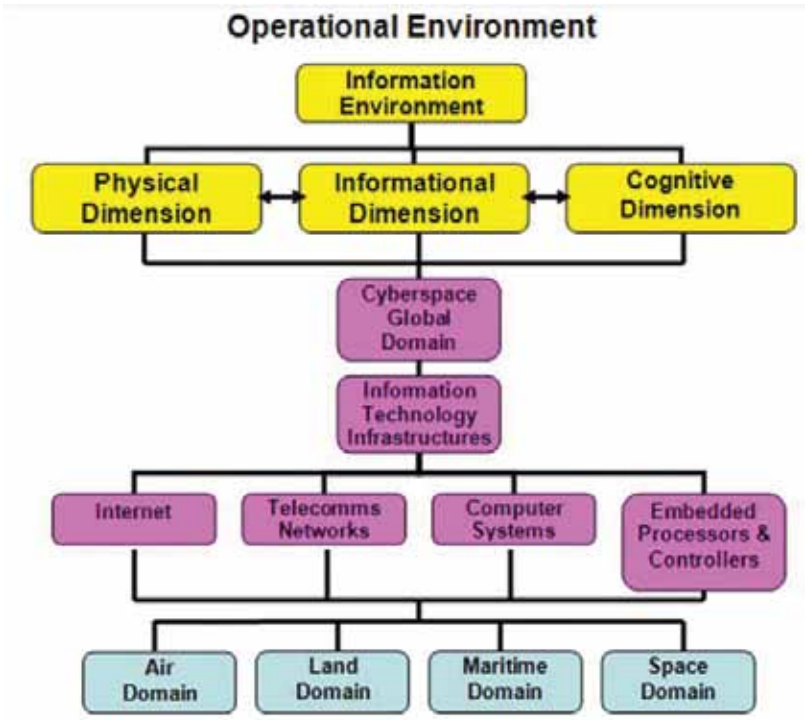


Figure 5: Author's rendition: Merger of Information Environment, Cyberspace Global Domain, and Air, Land, Maritime, & Space

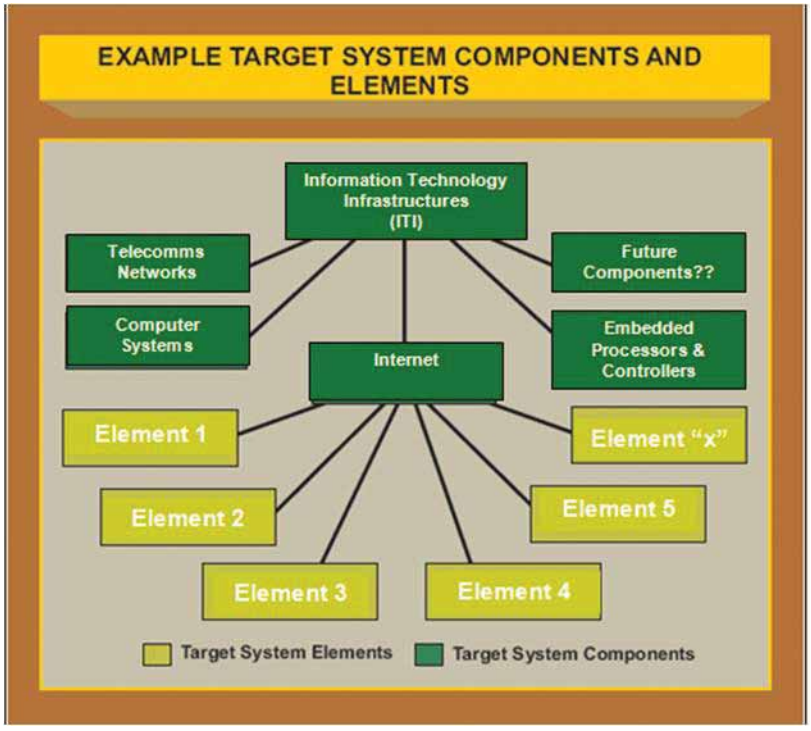


Figure 6. Author's rendition of a proposed ITI functional target system

Footnotes:

1. Joint Publication 3-60, Joint Targeting, 13 April 2007, pg GL-14. Accessed online 11 March 2009.

2. Webster's II New Riverside University Dictionary, definition #2, p. 396.

3. JP 3-0, Joint Operations, 13 Feb 2008, p. II-21 and JP 3-13, Information Operations, 13 Feb 2006, p. I-1.

4. Accessed online 11 March 2009. <www.afei.org/documents/NewCyberspaceDefinition.pdf>.

5. JP 3-13, p. I-1.

6. JP 3-13, p. I-1.

7. JP 3-0, pp. II-21 to II-22.

8. Accessed online 11 March 2009. <www.afei.org/documents/NewCyberspaceDefinition.pdf>

OPSEC and CNO - A United Front in the Republic of Korea

by

Colonel Wes Martin

As two of the core functions of Information Operations in United States Forces Korea (USFK), Computer Network Operations and Operations Security (OPSEC) are steadily developing an even closer and mutually supportive bond. In the spring of 2009, when Information Assurance/ Computer Network Operations (CNO) oversight was completely revamped, the relationship was cemented even further. The value of OPSEC in the network defense fight earned itself permanent panel status in the Flag Level Oversight Committee Charter, signed by USFK Chief of Staff Lieutenant General Joseph Fil. This in turn firmly provided the very element many OPSEC professionals recognize is lacking. That element is senior involvement and support.

The real strength of this oversight program is in the daily interface between OPSEC and two other supporting panels; Intelligence Collection and Computer Emergency Response Cell. Each panel is a forward liaison element to the staff they represent: OPSEC to J-3, Intelligence Collection to J-2, and Computer Response to J-6. The reach-back capability of each of these panels spans their entire organizations. The information gained by the Intelligence Collection Panel is readily shared with those with a need to know; and the Computer Response Panel is able to detect vulnerabilities, trends, and harden system and network defenses. With the critical information and analysis of threats being established and continually updated by the mutually supporting panel process, USFK OPSEC Program Manager Dan Wilkinson is able to primarily focus his and the OPSEC Panel's efforts on analyzing vulnerabilities, assessing risk, and implementing countermeasures.

As part of standard OPSEC doctrine, three of Dan's principle tools in analyzing vulnerabilities and assessing risk are reviews, surveys, and assessments. When he recently received an inquiry on how to ensure Personally Identifiable Information on a commander's information sheet, he realized a review was the appropriate tool. The specific information would be a contact list and data sheet concerning, and to be shared among, all colonels and generals assigned to USFK organizations. As in all reviews, he did not provide a spontaneous answer to a telephonic inquiry. Time was taken to review required information, who had a need to know, who else could gain access to the information, the protection currently being provided, how protection could be increased, and the involvement of other organizations in support. By the end of the day, the requester had a solid way ahead. He also had achieved one-stop shopping and a desire to return with further questions and guidance should a need arise. One question deserves one consolidated answer, not referrals to other organizations for supporting bits and pieces that in execution may conflict with each other.

The more intensive and demanding the OPSEC survey is the better it serves as a tool for evaluation. When a series of incidents resulted in potential loss of information, and time and resources dedicated to addressing the mistakes, a survey was used to separately analyze each incident and roll them up for common denominators. When the survey was initiated, foregone conclusions about the final result could not be allowed. This is always the best way to inhibit effective analysis and prevent an understanding of the true causes of the situation. In this survey, the same two factors kept reappearing despite multiple people being involved in each incident: lack of individual attention to detail and additional people accepting what others had done without double-checking. Although training played a secondary role, focused training and awareness are used to overcome the two primary problems. Likewise, an

USFK OPSEC and CNO Working Group

Source: Author

additional set of technical solutions are now being examined as part of additional countermeasures. As in the case of all countermeasures, continual engagement and fine-tuning of solutions are always necessary.

In addition to OPSEC reviews and surveys, USFK takes full advantage of OPSEC and multidiscipline vulnerability assessments. These assessments leverage outside agencies to deploy to Korea to thoroughly analyze command operations and processes to identify vulnerabilities and recommend additional OPSEC measures. The Joint OPSEC Support Center (JOSC) has provided outstanding assessment support to USFK in the past and continues to plan future visits to assist in strengthening OPSEC, Information Assurance, and Force Protection in the Korean Theater of Operations. Recently, the Army's Test and Evaluation Center (ATEC) and 1st Information Operations Command have joined forces with JOSC to provide more robust OPSEC and IA assessments in Korea during major exercises.

Long proven as the most effective OPSEC measure is a strong cadre of trained OPSEC professionals. In 2009 USFK OPSEC initially set out to conduct an OPSEC officers' course once per quarter. Because military assignments to Korea are typically one year in duration, it was felt this would stay ahead of the rotations ensuring appointed OPSEC officers received this important and required training. Again, working with Joint Information Operations Warfare Command, a significant modification was made to the command-training schedule. A mobile training team from the JOSC would come to Korea three times a year and provide two courses on each trip. To ensure all commands are able to have qualified OPSEC professionals, these classes are rotated throughout the U.S. installations in Korea. Doubts about the ambitiousness of this plan were soon eliminated as every class was filled to expectations and several walk-ons had to be assigned to the next class. The most recent four classes graduated over 150 OPSEC-certified professionals. The six courses already approved and scheduled for 2010 are highly anticipated and are projected to be just as full. For the Army students, there is an additional incentive: completion of the DOD OPSEC Officer Course results in their being awarded a Project Development Skill Identifier (PDSI), which becomes a permanent part of their records. On future assignments, it encourages them to stay involved in OPSEC and allows future commanders a means to identify who in the command already is OPSEC qualified.

Focusing on the need for awareness in Computer Network Defense, Information Assurance, and Korea-unique OPSEC issues, USFK has added its own training to these OPSEC courses. A two-hour presentation is imbedded specifically addressing the current regional counterintelligence and cyber threats. Also hitting close to home, the USFK OPSEC Program Manager delivers a presentation covering the distinctive aspects of managing OPSEC programs in Korea and shares actual results from recent vulnerability assessments conducted in Korea. These eye-opening presentations effectively motivate students and better equip them to tackle their new responsibilities. The result of this forward thinking initiative is now leading the way in courses being taught by both JOSC and Interagency OPSEC Support Staff.

The first step in achieving a success is to create a vision of what the future can be by turning opportunities in objectives. The Republic of Korea is the world's most successful democracy and free-enterprise society on the Asian mainland. Its military is working very diligently to assume lead responsibility for its defense against North Korean aggression. Soon the United States will be in a supporting role. Recognizing the importance of OPSEC, the Republic's Information Operations staff and their American counterparts thoroughly network with each other. Each day they literally work side by side. In routine operations and joint seminars, the concepts and applications of OPSEC are readily exchanged. The Americans have the stronger awareness of OPSEC procedures and methodology, their Korean allies a better understanding of the environment and the threat coming from the north. Just as the United States and the Republic of Korea have become partners in the fight for democracy on the Peninsula the same is true of OPSEC and Computer Network Operations. Like fellow combat warriors, these two Information Operations core functions firmly cover down on each other's flank and provide mutually supporting fields of fire. Meeting today's threat is part of their mission, moving forward to meet tomorrow's challenges is the remainder. The U.S. Forces Korea OPSEC and Computer Network Operations programs meet both challenges backed by command support and international involvement.

Instructors at the USFK and ROK Combined OPSEC Seminar

Source: Author

IO SPHERE
CALL OF ARTICLES

Become a Contributor

IO Sphere welcomes your articles, papers, and commentaries regarding all aspects of full-spectrum Information Operations, including core, supporting and related capabilities, as well as intelligence integration. Articles or book reviews should be 600-3000 words, preferably with an operational, training, or similar focus as related to IO. See submission guidelines or go to the JIOWC public site at https://www.jiowc.osis.gov.

Published Quarterly

Submission Deadlines

- **31 March-Spring Issue**
- **30 June-Summer Issue**
- **30 September-Fall Issue**
- **30 December-Winter Issue**

TO SUBSCRIBE: If you or your organization would like a free subscription to ***IO Sphere***, write to the editor at iosphere@jiowc.osis.gov. Please include your name, organization, office or division, official mailing address with 9-digit zip code and number of copies requested. For more information, contact the ***IO Sphere*** editor at (210) 977-3680 or DSN 969-3680.

Submission Guidelines

Please submit your contribution in Microsoft Word format, version 6.0 or higher, double-spaced in 12-point, Times New Roman font. Place graphs, photographs, and/or charts in separate attachments, not in the body of the paper. Insert a note describing object placement in the body of the paper. Example, "Place attachment one here." All charts/graphs/photographs should be at least 300 DPI resolution and in TIFF or JPEG format. Also, you may submit a high quality hard copy of graphics for scanning.

Find additional submission details on the ***IO Sphere*** homepage at https://www.jiowc.osis.gov or contact the editor.

Email all unclassified submissions to iosphere@jiowc.osis.gov. Point of contact is the *IO Sphere* Editor, Mr. Henry K. Howerton at 210.977.3680 or DSN 969.3680. IO Sphere is published at the unclassified level only. Finally, all items should be security screened, and released by author's parent command/agency/organization/company prior to submission. Please include a letter or email documenting these actions.

Currently Seeking Submissions on the Subject Topics of Electronic Warfare, Public Affairs, Strategic Communications, Military Information Support Operations, IO Education and Training, and IO Support to Public Diplomacy.

IO SPHERE: SUBSCRIPTION REQUEST FORM

Command/Organization: _____

Group/Dept./Division Name: _____

Attention Line: _____

Number & Street Address or Box: _____

City, State/Province: _____

ZIP +4 or Postal Code _____

POC: _____ Phone #: _____

E-mail: _____

FOLD UP HERE

How many people there involved in IO? _____ No. Copies desired: _____

How did you get this journal? _____

_____

Which article(s) did you find most useful? _____

_____

Which article(s) did you find least useful? _____

_____

_____

What would you like to see in future editions? _____

_____

_____

Other comments: _____

_____

_____

FAX TO: (210) 977-4654 (DSN 969) Email: iosphere@jiowc.osis.gov

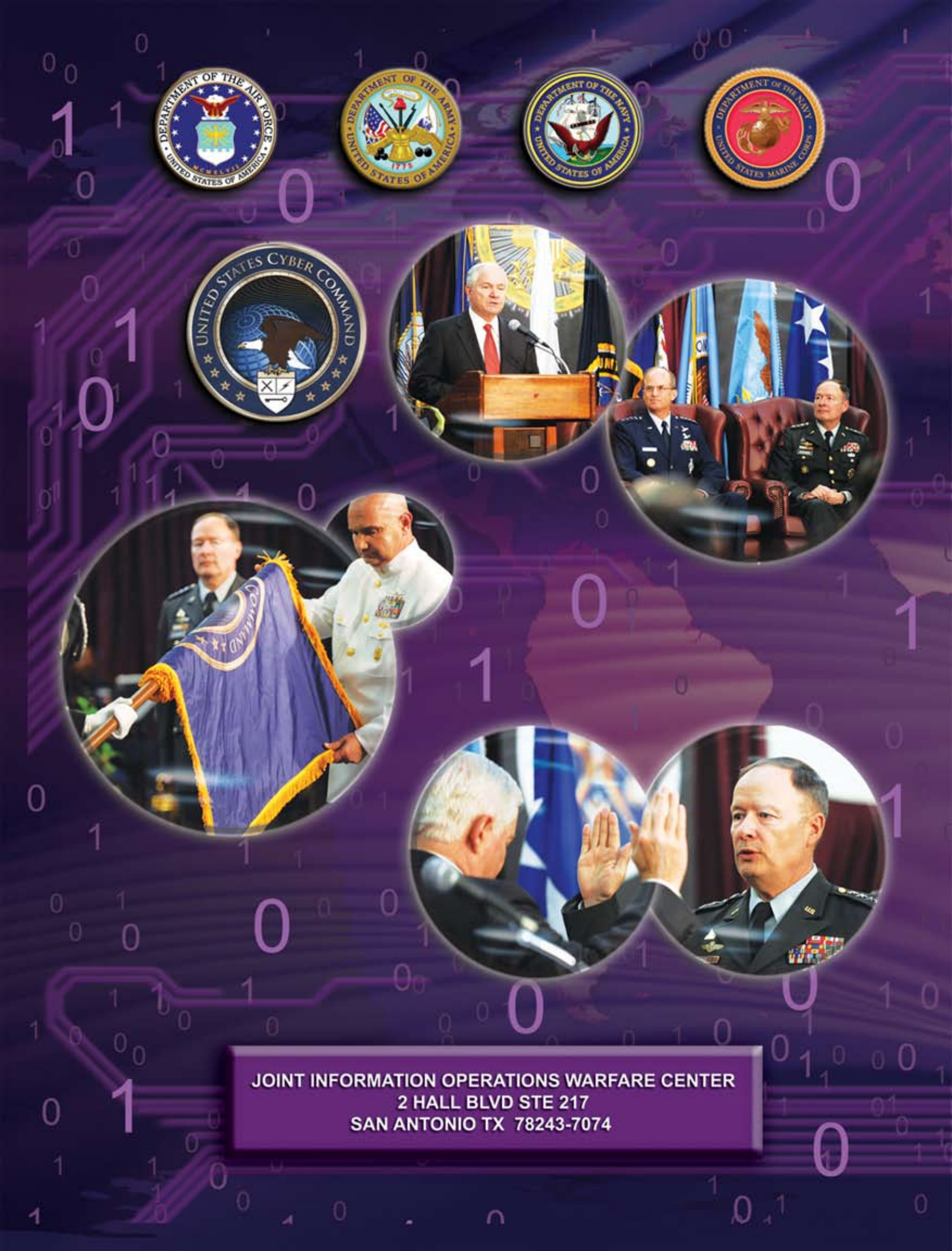
FOLD BACK HERE

Spring 2010

OFFICIAL BUSINESS

PLACE POSTAGE HERE

JOINT INFORMATION OPERATIONS WARFARE CENTER
ATTN: IO SPHERE EDITOR / J35 Outreach Division
2 HALL BLVD STE 217
SAN ANTONIO TX 78243-7074



JOINT INFORMATION OPERATIONS WARFARE CENTER
2 HALL BLVD STE 217
SAN ANTONIO TX 78243-7074