REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)* 14 Feb 2005	**2. REPORT TYPE** FINAL	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE
Improving Information Warfare Targeting: An IW Fires System.

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

LCDR Derek J. Leney, USN

Paper Advisor (if Any): N/A

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

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

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

8. PERFORMING ORGANIZATION REPORT NUMBER

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

10. SPONSOR/MONITOR'S ACRONYM(S)

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

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

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

14. ABSTRACT

Information Operations (IO) has grown in importance during recent conflicts. Yet some aspects of IO coordination and integration have fallen short of expectations. This has led to a desire by many in the IO community to better manage Information Warfare "fires," using the Joint Targeting Cycle as a rational process for their execution. However, current doctrine and joint organizations do not adequately provide for control of these fires. This paper addresses the conceptual challenges of Information Warfare targeting, including the differences between attacking "will" and "capability." Recent lessons learned highlight additional IO problems within the Joint Targeting Cycle. An IW Fires System is proposed to address these shortcomings, providing a formalized and connected organization for IW targeting and fire support.

15. SUBJECT TERMS
Information Operations, Information Warfare, Non-kinetic fires

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Chairman, JMO Dept
a. REPORT UNCLASSIFIED	**b. ABSTRACT** UNCLASSIFIED	**c. THIS PAGE** UNCLASSIFIED		28	**19b. TELEPHONE NUMBER** *(include area code)* 401-841-3556

NAVAL WAR COLLEGE
Newport, RI

Improving Information Warfare Targeting: An IW Fires System

By

Derek J. Leney
LCDR USN

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

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

Signature: _________________________

14 February 2005

Abstract

Information Operations (IO) has grown in importance during recent conflicts. Yet some aspects of IO coordination and integration have fallen short of expectations. This has led to a desire by many in the IO community to better manage Information Warfare "fires," using the Joint Targeting Cycle as a rational process for their execution. However, current doctrine and joint organizations do not adequately provide for control of these fires. This paper addresses the conceptual challenges of Information Warfare targeting, including the differences between attacking "will" and "capability." Recent lessons learned highlight additional IO problems within the Joint Targeting Cycle. An IW Fires System is proposed to address these shortcomings, providing a formalized and connected organization for IW targeting and fire support.

List of Illustrations

Introduction

> "The doctrinal void hampered planning and the education of combined-arms officers and senior formation commanders in the planning and conduct of IO. The resulting IO effort was often disjointed and not well integrated with maneuver, fires, and other combat activities.
>
> *On Point, the United States Army in Operation Iraqi Freedom*.[1]

The role of Information Operations (IO) has grown in importance in recent conflicts, including its fundamental role in Operation Iraqi Freedom (OIF). Of course, information advantage has always been a part of warfare and is intuitively necessary for successful military operations. Thus the current joint IO definition, "actions taken to affect information and information systems while defending one's own," is straightforward.[2] But as information technology has exploded, the scale of military activity aimed at the information environment has also increased. At the "leading edge" of IO theory, some believe that information attacks on human perception will "eventually provide the capability to subdue human will with a minimum use of physical force."[3]

Perhaps this will be eventually be the case. However, the cautionary tone of the Army's OIF lessons learned report reflects a more "down to earth" problem with IO. Despite some specific successes, translating information operations theory into an executable military operation has proven difficult. The Army's OIF report further stated that, "because IO as a domain is so broad and cuts across so many other domains, it is conceivable that the ability to develop a coherent IO campaign as the concept is presently conceived is illusory."[4] This is in contrast with the Army's assessment of air power in Iraqi Freedom: "flexible, responsive, and central to decisive joint operations."[5]

So the short-term imperative with IO is to achieve the same level of responsiveness and integration that has been achieved with air power. Fortunately, many in the IO community have begun to better rationalize IO employment, advocating the use of the Joint Targeting Cycle for information attacks. However, unique challenges exist when applying a targeting cycle in the information environment, especially for non-kinetic IO "weapons." Doctrinal and organizational improvements can resolve some of this friction, especially if focused on the targeting of an adversary's "will" to resist and the capability to control that resistance. A functionally designed Information Warfare Fires System would provide responsive and focused information targeting to the joint force commander.

Information Warfare and Targeting

Joint doctrine defines "Information Warfare" (IW) as IO conducted against an adversary in times of crisis or conflict.[6] This is a useful distinction. The current IO Cell, resident within the Combatant Commander or Joint Task Force (JTF) J-3, might be adequate to control peacetime offensive and defensive IO. Thus the "IW" term is used here deliberately to focus on targeting during more complex situations. IW in this sense also applies to targets throughout an adversary's information environment. This current definition goes beyond the historical role of IW in targeting military command and control (C2).

Joint doctrine also identifies several capabilities that make up an IW strategy: Operations Security (OPSEC), military deception (MILDEC), Psychological Operations (PSYOP), Electronic Warfare (EW), physical attack/destruction, and Special Information Operations (SIO). The Department of Defense's *Information Operations Roadmap*, signed in 2003, refines this definition with five "core" capabilities: EW, PSYOP, OPSEC, MILDEC, and Computer Network Operations (CNO).[7] These capabilities are the “fires” of information warfare.

There are several related capabilities, including Public and Civil Affairs, which also support an IW strategy. These efforts must be synchronized with offensive and defensive IO, which is part of the reason that the information strategy must be coordinated at the JFC level. Notably, the DoD *IO Roadmap* now defines physical attack as a supporting capability for IO, which makes sense from a targeting perspective. The Joint IO Cell is a source of physical attack nominations – an important function**.**[8] But physical attacks can be managed through existing joint targeting and fire support systems already in place. The focus here is on the control of *non-kinetic* IW capabilities - primarily EW, PSYOP, and CNO.[i]

Compared to other elements of joint warfare, current IO doctrine contains less guidance on “how” IW should be employed. Both IO Cell and Joint Operations Center (JOC) IO procedures are left to the J-3 or IO Officer to define.[9] However, service and joint IO centers have sought to reduce ambiguities in IW planning. For example, the Joint Information Operations Center (JIOC) has implemented the Joint Information Operations Planning Process (JIOPP). This process outlines some specific steps needed to translate overall campaign objectives into specific IW tasks.[10]

The Joint Forces Staff College (JFSC) further advocates using the Joint Targeting Cycle as the basis for IO planning and execution.[11] This desire was also advanced by EW planners following operations in Iraq and Afghanistan.[12] Figure (1) shows this process, which is embedded in both targeting and joint fire support doctrine. In fact, joint fire support doctrine includes a brief mention of non-kinetic IW capabilities as options alongside kinetic

[i] The specific capabilities of EW, PSYOP, and CNO are largely classified, but would not change the organizational construct of an IW Fires System.

weapons.[13] But traditional fire support organizations usually lack comprehensive IW expertise, and a consistent theme in lessons learned is that the Joint IO Cell lacks the visibility and authority to control IW Fires.

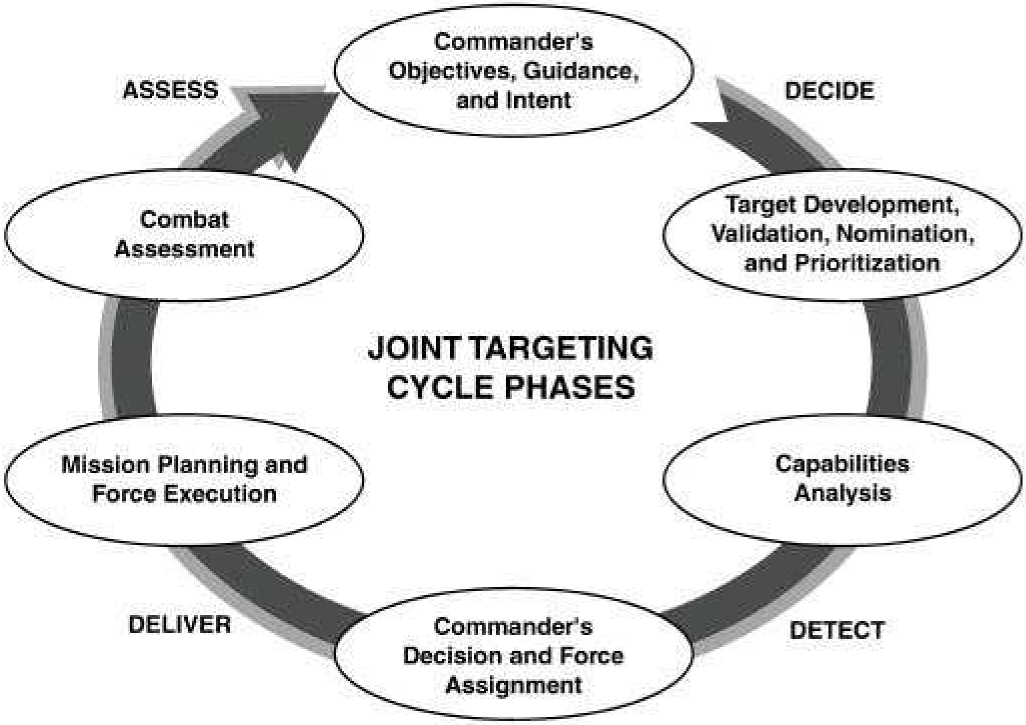

Commander's Objectives, Guidance, and Intent
DECIDE
Target Development, Validation, Nomination, and Prioritization
Capabilities Analysis
DETECT
Commander's Decision and Force Assignment
DELIVER
Mission Planning and Force Execution
Combat Assessment
ASSESS
JOINT TARGETING CYCLE PHASES

Figure 1. Joint Targeting Cycle[14]

Of course, an IW strategy may include actions taken by all elements of a joint force (particularly in deception and OPSEC). Nevertheless, non-kinetic IW attacks are largely performed by specialized EW, PSYOP, and CNO forces.[ii] Doctrinally, these units are not under the command of the Joint IO cell. An exception is the Joint Psychological Operations

[ii] Many forces have defensive non-kinetic capabilities which are sometimes used as part of an overall IO strategy, or possess IW systems along with conventional weapons. But most IW is still performed by legacy EW and PSYOP units. The term CNO "forces" is used here to describe several military and civilian organizations that actually perform CNO as a core competence.

Task Force (JPOTF), which may exercise coordinating authority over all JFC PSYOP forces.[15]

According to members of the Exercise Millennium Challenge 2002 IO Cell, "information operations achieved component-level status with respect to responsibility but lacked the resources and authority to be genuinely effective." Planners from that exercise recommended the establishment of a Joint IO Task Force: a "centralized commander to coordinate activities on the JTF level."[16] For the purposes of this discussion, however, the internal make-up of the Joint IO Cell is less important than providing a controlling mechanism for IW forces.

IW Effects: A Conceptual Framework for IW Targeting

One foundation for a rational IW Fires System is a common understanding of information effects, which are the ultimate results of an IW attack. IW as a concept grew out of Command and Control Warfare (C2W) – which focused specifically on military C2. As IO doctrine has evolved, however, the information target set has grown to include a wider set of information systems, human perception, and behavior. As noted in a 2002 USMC *Concept for Information Operations*, current IO concepts treat IO as a new "domain" of warfare altogether.[17] An emerging Army view divides this domain into physical, information, and cognitive environments. While IW tasks are directed at "first and second order" effects on information systems or their internal functions, their "third order" effects act on cognitive perception, attitudes, and understanding.[18]

U.K. IO doctrine offers a somewhat clearer view. In the British outlook, a simpler distinction is made between operations designed to target "will" and those that target C2 "capability." Influence activities attack a decision-maker's will to fight, while counter-command activities attack C2 infrastructure.[19] The "will vs. capability" split is carried further in a recently proposed "evolving view of IO effects" by JIOC's Michael Miller. As shown in Figure (2), specific IW effects can be grouped into those that influence "will" (*influence attacks*) and those that reduce command and control "capability" (*counter-command attacks*).

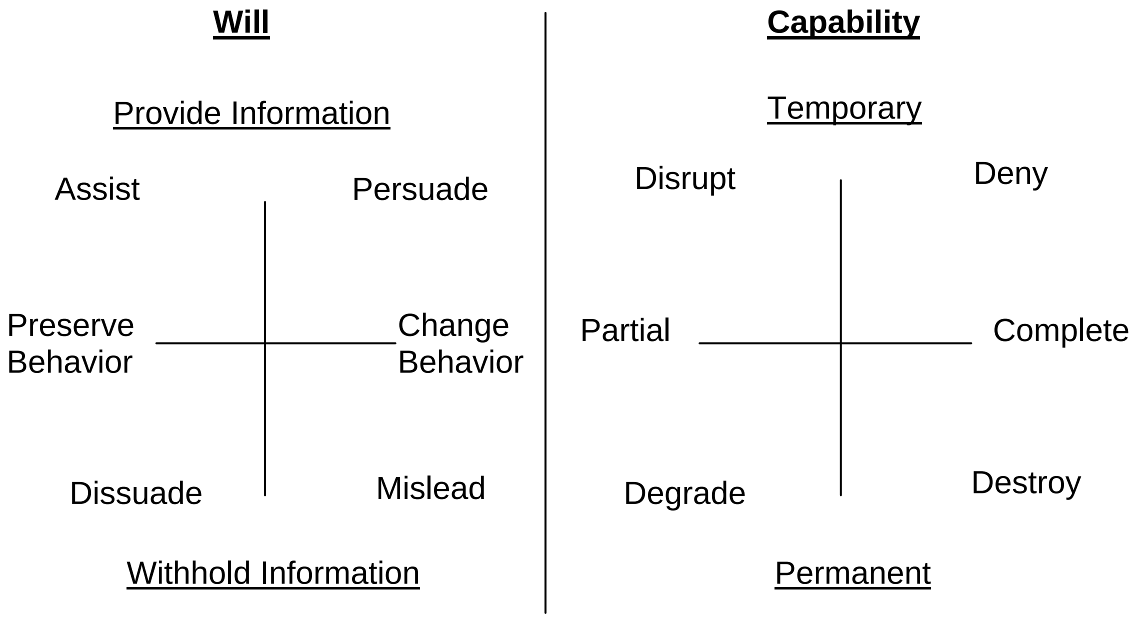


Figure 2. IO Effects [20]

Categorizing the IO effects set has direct implications for IW targeting. Attacking "will" usually requires intimate knowledge of the enemy in order to enable accurate assessment. Targeting "capability" may be more assessable, but prone to target development and force management problems. And in both cases, current doctrine fails to provide adequate systems for IW mission execution.

Influence Attacks: Targeting "Will"

One of the critical challenges of executing an IW targeting cycle is a lack of assessment, and this is most acute in influence attacks. Operation Allied Force in Kosovo showed some of this friction. There were some IW successes in degrading the Serbian air defense system, but effects on the Serbian regime or its ground forces remained suspect.

This is important, as the Serbian air defense system was not the ultimate target of NATO operations. From a broad perspective, the entire NATO campaign was an influence attack aimed at Milosevich himself. Yet as a RAND study noted after the war, "allied planners erred badly at the very outset of the campaign by failing to appreciate Kosovo's profound historical and cultural significance to the Serbs." This led to the "flawed assumption that Milosevich would capitulate to NATO demands without the need for an aggressive or protracted engagement**."**[21] Another RAND Corporation report noted that, "we may never know for sure what mix of pressures and inducements ultimately led Milosevich to admit defeat."[22]

Meanwhile, PSYOP directed at fielded Serbian units was ineffective at dissuading them from conducting ethnic cleansing, at least until the end of a 78-day bombing campaign. For example, PSYOP broadcasts and leaflet drops were employed in mountainous terrain, diluting message delivery. Also, the PSYOP message never matched the reality on the ground. While both PSYOP and Public Affairs claimed high numbers of Serbian vehicles destroyed, these claims were known to be false by Serbian forces on the ground.[23]

What Allied Force illustrates is that targeting an adversary's "will" is difficult at any level of war. At the tactical level, even if the PSYOP message was correct (and this is open to debate) the delivery method (equating to force assignment and execution from the Joint Targeting Cycle) was ineffective. And at the operational/strategic level, only intimate knowledge of the enemy would have allowed NATO to adjust influence targets and PSYOP fires. While Allied Force was successful in the end, even today the linkage between influence targets and Milosevich's behavior remains unclear.

Operation Iraqi Freedom (OIF) involved a more sophisticated attempt to target enemy "will." CENTCOM used innovative methods to target specific sectors of the regime: certain Iraqi commanders in the field, senior military leaders, and "regime" individuals such as WMD scientists.[24] Mobile phone text messaging and e-mails were reportedly sent to key decision-makers, taking advantage of the access only afforded to Baath party leadership.[25]

There is other evidence that the pre-war plan placed heavy emphasis on influence attacks. MGEN Gene Renuart, the CENTCOM J-3, claimed that the success of IO was critical to the overall plan because "it was clear that we were going to have to have an ability to at least neutralize large chunks of Iraqi forces."[26] There were some specific successes in this regard. For example, Iraqis told U.S. personnel that they had deliberately faked oil field sabotage because of PSYOP broadcasts.[27] Similarly, the Iraqi Air Force stayed out of the war even though it had some capability remaining, a cognitive decision. Finally, the U.S. used strategic deception to successfully enable operational surprise at the start of major combat operations.[28]

In other areas, however, influencing Iraqi "will" proved harder to assess. As one NATO PSYOPs officer has argued, the "shock and awe" campaign was itself psychological, with the hope that this overwhelming show of force would cause regime collapse.[29] But "shock and awe" and non-kinetic influence attacks still did not result in capitulation at the strategic level. At the tactical level, the Army OIF lessons learned report claims that the

PSYOP effort was less successful at encouraging Iraqi units to surrender than had been expected.[30]

These examples from Allied Force and Iraqi Freedom are highlighted here because they expose the inherent challenges of applying a rational targeting cycle to the behavioral domain. Joint doctrine notes that measures of effectiveness (MOE's) are a prerequisite to the performance of combat assessment.[31] Yet these measures remain elusive when targeting adversary "will." Fleet Information Warfare Center (FIWC) intelligence officers recently wrote that "the information warrior's ability to assess effectiveness of an IO is limited." When MOE's *are* available, they are likely the result of human intelligence (HUMINT) or, in some limited cases, signals intelligence (SIGINT).[32]

So knowing what an adversary thinks is a difficult task, even in the case of two regimes that had been subject to years of confrontation and study by U.S. (and allied) intelligence. This does not mean, however, that the Joint Targeting Cycle is an invalid model for targeting "will." In some cases, intelligence may become available that can allow direct influence assessment. In other cases, an enemy reaction may be observable, regardless of "why" it happened. Either scenario could result in an "adjust fire" situation for influence attacks.

But what *is* likely is that assessment problems will result in the influence targeting cycle being out of synch with kinetic targeting processes. As the JFSC writes, "the IO cell must be aware that not all IO will fit neatly into the ATO [Air Tasking Order] timeline."[33] If the results of non-kinetic influence attacks are not immediately forthcoming, commanders may be tempted to use traditional means to remove adversary combat capabilities. So an IW

Fires System must maximize the chances for influence assessment, which will require a focused and specialized effort.

Mission planning and execution can also be improved in the influence targeting cycle. In OIF, for example, PSYOP was not responsive to Army maneuver units. Current U.S. policy states that "in order to maximize PSYOP support and ensure timeliness of application, PSYOP must be centrally controlled by the combatant commander or JFC and executed at the most appropriate levels." [34] But Army observers claim that after the first 48 hours of combat, "centralized themes and messages sometimes proved irrelevant to local populations and situations." Leaflet production at the JPOTF level did not provide the text necessary for the situations V Corps faced.[35] So where influence targeting *can* be responsive, it should be. An IW Fires System should therefore have more effective execution links between the JPOTF and "customer" units.

Counter-Command Attacks: Targeting C2 "Capability"

While assessment will still be difficult in counter-command IW attacks, target development and force assignment may present more immediate challenges. For example, technical research will likely allow planners a good forecast of IW effectiveness against certain adversary systems. This has historically been true for EW weapons but might also be known for CNO. So even if effects cannot be *observed* after the fact, counter-command IW effects may well be accurately *predicted*. EW attacks normally focus on the "capability" side of the effects scale. While usually temporary, these effects are nevertheless possible to integrate with other combat operations.

Even adversaries that lack a highly developed C2 infrastructure have proven vulnerable when IW expertise was present at the appropriate level of the joint force.

Unfortunately, this has normally been an ad-hoc arrangement. During Operation Enduring Freedom, the Taliban and Al Qaeda did not offer much in the way of an information systems target set. But EA-6B and EC-130H crews quickly realized that they could disrupt tactical communications as well as operational-level coordination between various terrorist and Taliban cells. These capabilities were integrated into SOF missions fairly early in the Afghanistan operation.[36]

Yet over time it appears that the corporate memory for non-kinetic fires was lost, or at least not exported from SOF planning organizations to the JTF headquarters. By the summer of 2002, Army forces were "unaware that EA-6B's were available to support them," despite the fact that EA-6B's were flying missions over Afghanistan every day. The Army also had IW assets on the ground that, if integrated with airborne EW, could have increased the effectiveness of non-kinetic fires. This was not done because of a lack of integrated knowledge and planning.[37] The situation was improved with aggressive education by EA-6B and EC-130H crews. Also, planners arrived in theater that were coincidentally cross-trained in kinetic targeting, EW, and intelligence.[38]

Iraqi Freedom saw some positive examples of counter-command IW attacks. In contrast with the Iraqi Air Force, the Iraqi air defense system was active at times during the war. However, the limited number of Coalition aircraft losses was at least partially due to a successful effort aimed at Iraqi C2. Additionally, the Army's OIF lessons-learned report noted that "kinetic and electronic attacks to disrupt or destroy critical command and control infrastructure proved more effective [than PSYOP]." [39]

One reason the Army may have had more confidence in the EW "arm" of the IW campaign was CENTCOM's use of centralized EW planning *outside* of the JFC IO Cell.

CENTCOM delegated control over all theater EW to the CFACC, and the CFACC established an EW Coordination Cell (EWCC) to control airborne electronic fires. This organization consisted of EW operators from various platforms and dedicated reconnaissance and intelligence support.[40] There was some concern that placing theater EW under the CFACC would make the IO campaign too "air-centric" (some tactical EW platforms below the battalion level remained under component control). But "the CFACC had the preponderance of the EW assets and, most importantly, a theater-wide C3 structure based on the CAOC that allowed effective C2 over EW to be executed."[41]

Most observers claim that the EWCC was successful. The Joint Information Operations Center (JIOC) reported that coordination was sufficient to allow dynamic re-direction of EW assets.[42] Again using the EA-6B example, "non-traditional" EW support to ground, maritime, and special operations forces was a significant portion of EA-6B tasking**.** But the OIF EW cell was a special situation enabled by a pre-war planning conference**.**[43] An IW Fires System must codify these manning arrangements, going beyond the ad-hoc organizations used in Iraq and Afghanistan.

Improving Force Assignment and Target Development

So centralized EW planning was a good step in the right direction, but improvements can still be made in force assignment and target development. Again using the EA-6B example, there was no possibility of supporting every EW support request. The EWCC therefore used the CFACC commander's intent from the daily ATO, apportioning EW support sorties using the same priority as the air component as a whole.[44] This was an innovative way of doing business for the EW community (airborne EW platforms have historically been weighted to the air campaign). But this approach may need to become even more sophisticated.

Traditional commander's guidance should be modified for non-kinetic weapons based on technical or cognitive differences within an adversary. For example, an elite enemy division facing a JFLCC "main effort" might be unsusceptible to influence, or equipped with newer C2 equipment and not susceptible to C2 disruption. Conversely, another enemy division (with different leadership or equipment) in front of the JFLCC "secondary effort" might be more susceptible to either influence or counter-command attacks. In this case, kinetic CAS and interdiction sorties should be weighted to the former, but non-kinetic IW capabilities weighted toward the latter.

There were other good force assignment lessons from centralized EW management. First, the line between EW and PSYOPS has become increasingly blurred. Future IO platforms will likely be multi-tasked in the IO environment. As JIOC noted after OIF Phase III, "a single tasking authority must be retained" to de-conflict among EW uses.[45] Thus an IW Fires System must not only allocate IW forces across component priorities, it must internally distribute targets among multi-role IW platforms.

Target development for non-kinetic weapons can also be improved. IW attacks lack some of the "infrastructure" that is resident within kinetic target development systems. For example, strike aircrew are familiar with target folders and Joint Munitions Effectiveness Manuals (JMEMs), which allow the pairing of kinetic weapons to targets. FIWC has proposed improving the target folder to include some data fields for IO capabilities.[46] Similarly, service IW communities own a great deal of "in house" knowledge on their systems' performance. This knowledge needs to move from platform and service experts to standardized targeting organizations.

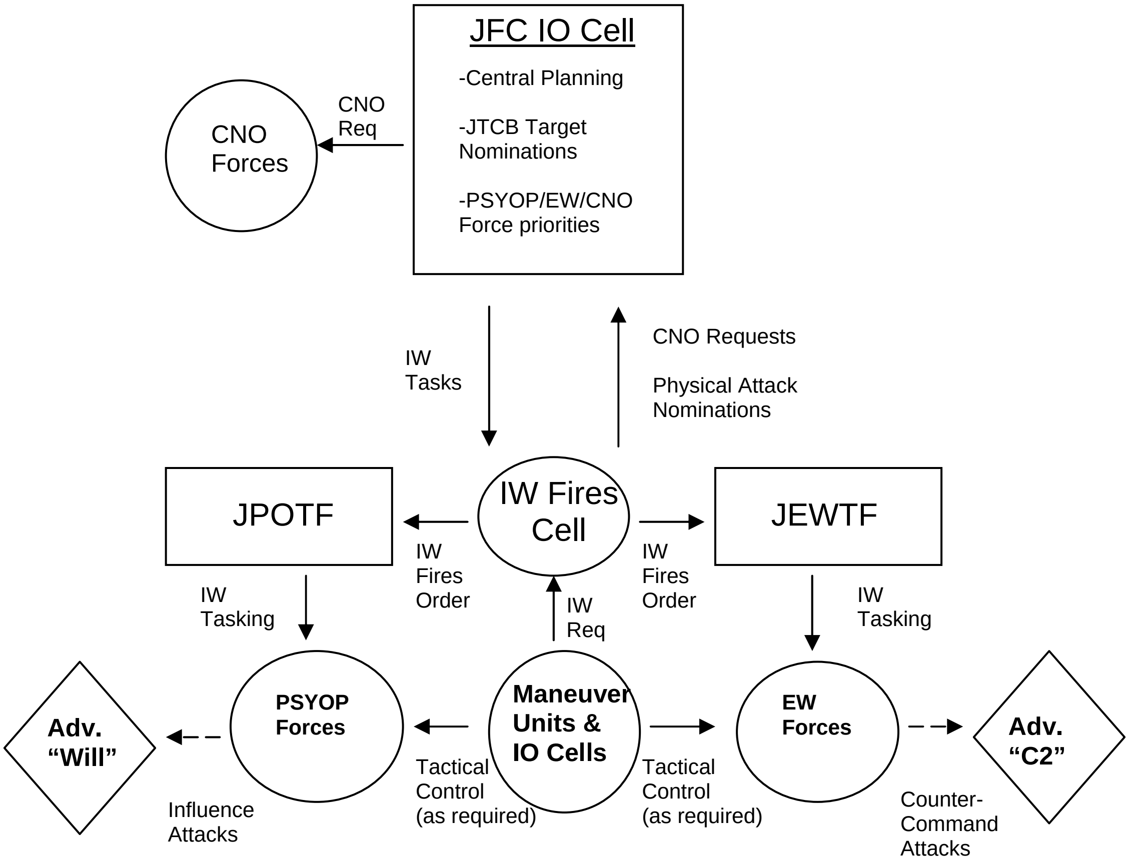
Improving Mission Planning and Execution

The Joint Fire Support System already includes a wide array of organizations that synchronize and control fires in support of component elements. Some examples of these are Army Battlefield Coordination Detachments and Deep Operation Coordination Cells, USAF Theater Air Control System components, USMC Direct Air Support Centers, and SOF Special Operations Coordination Elements.[47] Therefore, one alternative to a separate IW Fires System might be the distribution of IW fires expertise among these C2 organizations.

However, IW manning is probably inadequate to push EW, PSYOP, and CNA experts down to lower levels of the Joint Fire Support System. As a FIWC observer noted after OIF, "efforts to provide EWOs [Electronic Warfare Officers] to all component IO cells would have diffused available assets, severely impairing the EW effort."[48]   Additionally, the classification of many IW capabilities is an impediment to more universal distribution. So a solution like the OIF EWCC might be a good compromise.

Recommendation: An IW Fires System

Managing the IW targeting cycle requires a fires system with several attributes. First, it must meet the need for centralized targeting but also be responsive to changing situations in the battlespace. IW targeting must also mitigate the target development, force assignment, execution, and assessment challenges of non-kinetic weapons.   This system would not replace the JFC IO Cell. Rather, it would serve as the controlling mechanism for execution, in much the same way that kinetic fires are controlled through existing Joint Targeting and Joint Fire Support organizations. Figure (3) shows a nominal IW Fires System design.



. Figure 3. IW Fires System

The IW Fires System shown here divides responsibility for the IW targeting cycle among several functional elements. First, the JFC IO Cell maintains its current role as the central IO planner, transforming broad commander's objectives into specific tasks. This includes the integration of core and related capabilities into the overall IO plan. Additionally, the IO Officer should retain responsibility for nominating physical targets in support of IO objectives. Finally, due to classification and approval timelines, the JFC IO Cell should continue to control or task CNO forces.

As theater operations become more complex in a crisis or conflict, the IO Officer would establish three organizations to control information warfare attacks. Under the IW

Fires System, the JPOTF would manage influence targeting while a new Joint EW Task Force (JEWTF) would control counter-command targeting. An IW Fires Cell would execute day-to-day management of both organizations. The division here is necessary because, once assigned, the "will" cycle might never be complete. Thus the IW Fires Cell, along with the JFC IO Officer, would maintain a "referee" mindset – dispassionately evaluating influence effects. When a JFC objective requires a *certain* IW effect, under most circumstances this would be filled by a JEWTF capability (or a physical attack nomination).

Unlike current doctrine, the JPOTF would exercise operational control over all PSYOP forces. This would allow the PSYOP commander to allocate forces to either the highest priority *or* most susceptible target audience. Additionally, this arrangement would improve the speed at which influence messages could be coordinated between the PSYOP commander and PSYOP forces (perhaps a "menu" of pre-approved messages could be continuously updated for tactical PSYOP units). Keeping the JPOTF as a separate organization allows a high degree of focus to "work" the influence targeting cycle.

The JEWTF, on the other hand, would focus primarily on the "capability" target set. As with the JPOTF, the JEWTF would coordinate mission planning and execution among EW forces. Force assignment to specific EW capabilities would also be managed here, in much the same way the OIF EWCC allocated EW support requests. Of course, some information targets might require both influence and counter-command attacks to be successful. For example, an influence message might replace normal C2 information during a counter-command disruption.

This kind of coordination would be integrated at the IW Fires Cell. Subordinate commanders or the JFC IO Cell would request IW fires from the IW Fires Cell, and the IW

Fires Cell would offer either an influence or counter-command attack (or both) to achieve the desired effect. The IW Fires Cell would have knowledge of IW weapons effectiveness (the IW "JMEMs") so that correct weapons pairing could be achieved. PSYOP and EW experts within the rest of the IW Fires System would also have this capability, as some IW fires missions might not demand specific capabilities. Finally, the IW Fires Cell would operate under a JFC prioritization scheme to fill IW requests according to the JFC IO Cell's guidance.

The JFC IO Cell could, of course, expand in manning and connectivity and embed these organizations within its own structure. This would allow the JFC IO Officer to control IW fires directly out of the joint force staff. But in the IW Fires System, the JPOTF, JEWTF, and IW Fires Cell would be self-contained and deployable units (similar to elements of existing fire support C2 systems). This would allow them to embed at the most appropriate level, at times within physical contact with "customer" units. When operations were heavily weighted toward a single functional component, some of the IW Fires nodes might embed directly with that component's IO and fire support cells. In more complex situations, elements of the IW Fires System would be hosted differently based on the preponderance of assets, C2 capability, or specific expertise requirements. Either way, these nodes would place expertise and knowledge at the *lowest level possible* in the joint force.

Conclusion

Recent operations have seen many IW success stories. There have also been some "misses." Some of these have been due to the inherent challenges of applying force against information targets. Other problems have been more basic: shortfalls in the coordination and integration of IW fires. The system proposed here is a starting point for a formalized and connected IW fires capability. Of course, non-kinetic weapons may never achieve a decision-cycle that can offer the assurance of kinetic targeting. But doctrinal and organizational changes – the IW Fires System - *can* improve the integration and responsiveness of IW fires.

Notes

[1] U.S. Army Center for Lessons Learned, On Point, The U.S. Army in Operation Iraqi Freedom (Leavenworth, KS: 2003), Ch 7. <http://www.onpoint.leavenworth.army.mil/ch-7.htm> [30 December 2004].

[2] Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Pub 3-13 (Washington, D.C: 9 October 1998), vii.

[3] Edward Waltz, Information Warfare: Principles and Operations. (Norwood, MA: Artech House 1998), 9.

[4] U.S. Army Center for Lessons Learned, On Point, The U.S. Army in Operation Iraqi Freedom, Ch 7.

[5] Ibid.

[6] Joint Chiefs of Staff, Joint Doctrine for Information Operations, GL-7.

[7] Joint Chiefs of Staff, Joint Doctrine for Information Operations, viii; Department of Defense, Information Operations Roadmap (U) (Washington, DC: 30 October 2003), SECRET NOFORN, 9. <http://iotf.js.smil.mil/files/io_roadmap_30_october_2003.pdf> [28 December 2004].

[8] Joint Chiefs of Staff, Joint Doctrine for Information Operations, II-13.

[9] Joint Chiefs of Staff, Joint Doctrine for Information Operations, IV-4.

[10] Joint Forces Staff College, Joint Information Operations Planning Handbook (Norfolk, VA: July 2003), V-1.

[11] Ibid, II-5.

[12] John Kurtz, "Electronic Fires Deserve Joint Targeting Cycle Tasking," U.S. Naval Institute Proceedings, (October 2004): 59.

[13] Joint Chiefs of Staff, Joint Doctrine for Fire Support, Joint Pub 3-09 (Washington, DC: 12 May 1998), I-1.

[14] Joint Chiefs of Staff, Joint Doctrine for Targeting, Joint Pub 3-60 (Washington DC: 17 January 2002), II-2.

[15] Joint Chiefs of Staff, Joint Doctrine for Psychological Operations, Joint Pub 3-53, (Washington, DC: 5 Sep 03), III-3 to III-5.

[16] Mark Maiers and Timothy Rahn, "Information Operations and Millennium Challenge," Joint Forces Quarterly, 35: 87.

[17] U.S. Marine Corps Combat Development Command, A Concept for Information Operations, (Quantico, VA: 19 April 2002), 1.

[18] U.S. Army, Information Operations: Doctrine, Tactics, Techniques, and Procedures, FM 3-13 (Washington, DC: November 2003), 6-4.

[19] United Kingdom Ministry of Defense, Information Operations, Joint Warfare Publication 3-80 (Shrivenham, UK: June 2002), 2-2.

[20] Michael Miller, "The Evolution of Information Operations Effects: Learning From Experiences in Afghanistan and Iraq," Fleet Information Warfare Center Infoscope, Vol. 3 Issue 1 (Spring 2004): 3. <http://www.infoscope.fiwc.navy.smil.mil/vol3_issue1/io_effects.pdf > [30 December 2004].

[21] RAND Corporation, Rand Research Brief: Operation Allied Force, Lessons for the Future, (Santa Monica, CA: 2001), 2.< http://www.rand.org/publications/RB/RB75.html.> [29 January 2005]

[22] Benjamin Lambeth, NATO's Air War for Kosovo: a Strategic and Operational Assessment. (Santa Monica, CA: RAND Corporation 2001), 68. <http://www.rand.org/publications/mr/mr1365> [28 December 2004].

[23] Information Operations – The Hard Reality of Soft Power," (Unpublished Text, Joint Command and Control & Information Warfare Staff, Joint Forces Staff College: 2002), 102.

[24] Andrew Koch, "Information War Played Major Role in Iraq," Jane's Defense Weekly, Vol. 40 No. 3 (23 July 2003): 5.

[25] Steven Collins, "Mind Games," NATO Review, 2 (Summer 2003): 3. <http://www.nato.int/docu/review/2003/issue2/English/art4.html.> [20 January 2005].

[26] MGEN Gene Renuart, quoted in Andrew Koch, "Information War Played Major Role in Iraq," Jane's Defense Weekly. Vol. 40 No. 3 (23 July 2003): 5.

[27] Koch, 5.

[28] Ibid, 5.

[29] Collins, 3.

[30] "U.S. Army Center for Lessons Learned, On Point, the U.S. Army in Operation Iraqi Freedom, Ch-7.

[31] Joint Chiefs of Staff, Joint Doctrine for Targeting, GL-8.

[32] Carrie Gray and Edwin Howard, "IO MOE Development and Collection: A Paradigm Shift, " Fleet Information Warfare Center Infoscope, Vol. 3 Issue 2. (Winter 2004): 2.
< http://infoscope.navy.smil.mil/vol3_issue2/IO_MOE.pdf > [30 December 2004].

[33] Joint Forces Staff College, II-6.

[34] Chairman of the Joint Chiefs of Staff, Joint Psychological Operations Supplement to the Joint Strategic Capabilities Plan FY 2002, CJCSI 3110.05C (Washington, DC: 18 July 2003), A-3.

[35] U.S. Army Center for Lessons Learned, On Point, the U.S. Army in Operation Iraqi Freedom, Ch-7.

[36] Ronald Reis and Glenn Robbins, "Integrating Carrier-Based Electronic Attack into Conventional Army Doctrine." Military Review, Vol. LXXXIII No. 3 (May-June 2003): 25. <http://www.leavenworth.army.mil/milrev/download/English/mayjun03/reis.pdf > [16 Jan 05]; Kernan Chaisson, "Till Their Ears Bleed, Compass Call's Contributions to the War on Terror" Journal of Electronic Defense, Vol. 25 No. 7 (July 2002): 22-23.

[37] Reis and Robbins, 25.

[38] Ibid, 25.

[39] U.S. Army Center for Lessons Learned, On Point, The U.S. Army in Operation Iraqi Freedom, Ch-7.

[40]Kurtz, 59.

[41] Joint Information Operations Center, Summary Report for Operation Iraqi Freedom (OIF: Pre-Phase I-III) (U) (San Antonio, TX: 2003), SECRET NOFORN, 37. <http://jllpio.jioc.smil.mil/resources/external/ref_doc/jioc_oif/jioc_oif_ll_report.pdf> [30 December 2004].

[42] Joint Information Operations Center, Summary Report for Operation Iraqi Freedom (OIF: Pre-Phase I-III), 37.

[43] Ibid, 37.

[44] Kurtz, 59.

[45]Joint Information Operations Center, Summary Report for Operation Iraqi Freedom (OIF: Pre-Phase I-III) (San Antonio, TX: 2003), 35.

[46] Gray and Howard, 2.

[47] Joint Chiefs of Staff, Joint Doctrine for Fire Support, II-8 to II-10.

[48] Colin Claus, “The Role of the Electronic Warfare Coordination Cell in Operation Iraqi Freedom,” Fleet Information Warfare Center Infoscope, Vol. 3 No. 1 (2003): 1. <http://infoscope.fiwc.navy.smil.mil/col3_issue1/ew_oif.pdf> [30 December 2005].

Bibliography

Bowman, Paul. "Information Operations: Strategy or Mission? Reflections on Allied Force." Cybersword, Vol. V No. 1 (Summer 2001): 18-21.

Chaisson, Kernan. "Till Their Ears Bleed, Compass Call's Contributions to the War on Terror" Journal of Electronic Defense, Vol. 25 No. 7 (July 2002): 22-23.

Claus, Colin. "The Role of Electronic Warfare Coordination Cell in Operation Iraqi Freedom," Fleet Information Warfare Center Infoscope, Vol. 3 No. 1 (2003): 1. <http://infoscope.fiwc.navy.smil.mil/col3_issue1/ew_oif.pdf> [30 December 2005].

Collins, Steven. "Mind Games," NATO Review, 2 (Summer 2003). <http://www.nato.int/docu/review/2003/issue2/English/art4/html>[20 January 2005].

Gray, Carrie and Edwin Howard. "IO MOE Development and Collection: A Paradigm Shift, " Fleet Information Warfare Center Infoscope, Vol. 3 Issue 2. (Winter 2004): 2. < http://infoscope.navy.smil.mil/vol3_issue2/IO_MOE.pdf > [30 December 2004].

Hubbard, Zachary P. "Information Operations and Information Warfare in Kosovo: A Report Card We Didn't Want to Bring Home." Cybersword Vol. IV No. 1 (Spring 2000): 27-29.

"Information Operations – The Hard Reality of Soft Power." Unpublished Text, Joint Command Control & Information Warfare Staff at the Joint Forces Staff College. Norfolk, VA: 2002.

Koch, Andrew. "Information War Played Major Role in Iraq," Jane's Defense Weekly. Vol. 40 No. 3 (23 July 2003): 5.

Kurtz, John W. D. "Electronic Fires Deserve Joint Targeting Cycle Tasking," U.S. Naval Institute Proceedings (October 2004): 58-61.

Lambeth, Benjamin S. NATO's Air War for Kosovo: a Strategic and Operational Assessment. Santa Monica, CA: RAND Corporation, 2001. <www.rand.org/publications/mr/mr1365 > [28 December 2004].

Maiers, Mark W. and Timothy L. Rahn. “Information Operations and Millennium Challenge.” Joint Forces Quarterly, 35: 83-87.

Miller, Michael. “The Evolution of Information Operations Effects: Learning From Experiences in Afghanistan and Iraq.” Fleet Information Warfare Center Infoscope, Vol. 3 Issue 1 (Spring 2004). <http://www.infoscope.fiwc.navy.smil.mil/vol3_issue1/io_effects.pdf > [30 December 2004].

Patschke, Gregory M. “Information Operations and J-3; a Perfect Union.” Unpublished Research Paper, U.S. Naval War College, Newport, RI: 9 February 2004.

RAND Corporation. Rand Research Brief: Operation Allied Force, Lessons for the Future. Santa Monica, CA: 2001. <http://www.rand.org/publications/RB/RB75.html.> [29 January 2005]

Reis, Ronald and Glenn F. Robbins. “Integrating Carrier-Based Electronic Attack into Conventional Army Doctrine.” Military Review, Vol. LXXXIII No. 3 (May-June 2003): 21-25. <http://www.leavenworth.army.mil/milrev/download/English/mayjun03/> [16 Jan 05].

Sevien, Frederic H. “Kosovo: An IW Report Card.” Journal of Electronic Defense, Vol. 22 No. 8 (August 1999): 47-51.

U. K. Ministry of Defense, Information Operations. Joint Warfare Publication 3-80. Shrivenham, UK: June 2002.

U.S. Air Force. Information Operations. Air Force Doctrine Document 2-5. Washington, DC: 04 January 2002.

_________. Concept of Operations for Information Operations. Washington, DC: 6 February 2004.

U.S. Army. Information Operations: Doctrine, Tactics, Techniques, and Procedures. FM 3-13 (FM 100-6). Washington, DC: November 2003.

U.S. Army Center for Lessons Learned, On Point, The U.S. Army in Operation Iraqi Freedom. Leavenworth, KS: 2003. <http://www.onpoint.leavenworth.army.mil/ch-7.htm> [30 December 2004].

U.S. Army First IO Command. TTP for Operational and Tactical IO. Washington, DC: April 2004. <www.1stiocmd.army.smil.mil/io_toolbox/web_data/io_toolbox.html>

[1 December 2004]

U.S. Chairman of the Joint Chiefs of Staff, Joint Psychological Operations Supplement to the Joint Strategic Capabilities Plan FY 2002, CJCSI 3110.05C. Washington, DC: 18 July 2003.

U.S. Department of Defense. Information Operations Roadmap (U). Washington, DC: 30 October 2003. <http://iotf.js.smil.mil/files/io_roadmap_30_october_2003.pdf> [28 December 2004]. SECRET NOFORN

U.S. Joint Chiefs of Staff. Joint Doctrine for Information Operations. Joint Pub 3-13. Washington, D.C: 9 October 1998.

_________. Joint Doctrine for Targeting. Joint Pub 3-60. Washington, DC: 17 January 2002.

_________. Joint Doctrine for Fire Support. Joint Pub 3-09 Washington, DC: 12 May 1998.

_________. Joint Doctrine for Psychological Operations. Joint Pub 3-53. Washington, DC: 5 September 03.

.

_________. Joint Information Operations Planning Handbook. Norfolk, VA: July 2003.

U.S. Joint Information Operations Center. Summary Report for Operation Iraqi Freedom (OIF: Pre-Phase I-III) (U). San Antonio, TX: 2003. <http://jllpio.jioc.smil.mil/resources/external/ref_doc/jioc_oif/jioc_oif_ll_report.pdf> [30 December 2004]. SECRET/NOFORN

Waltz, Edward. Information Warfare: Principles and Operations. Norwood, MA: Artech House, 1998.