STRATEGY
RESEARCH
PROJECT

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

DECISION AIDS AND WARGAMING FOR INFORMATION OPERATIONS

BY

COLONEL CHARLES R. BALL
United States Army

USAWC CLASS OF 1999

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

DECISION AIDS AND WARGAMING FOR INFORMATION OPERATIONS

by

COL Charles R. Ball
United States Army

COL Ralph Ghent
Project Advisor

The views expressed in this academic research paper are those of the author and do not necessarily reflect the official policy or position of the U. S. Government, the Department of Defense, or any of its agencies.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Charles R. Ball, COL, Army

TITLE: DECISION AIDS AND WARGAMING FOR INFORMATION OPERATIONS

FORMAT: "USAWC Strategy Research Project"

DATE: 7 APR 1999 PAGES: 46 CLASSIFICATION: Unclassified

Information operations are an essential component of our current and future warfighting strategy as outlined in the latest National Military Strategy and Joint Vision 2010. Simulations such as WARSIM 2000 are an important enabler that will permit us to train for and execute this strategy. However, information operations are not included in any current simulation nor are they addressed in any automated decision aids supporting these simulations. The Defense Advanced Research Projects Agency developed a constraint based decision aid to support Course of Action Analysis (COAA) for simulation support at the School of Advanced Military Studies. This decision aid can be extended to represent information operations courses of action. This SRP recommends changes to the decision aid to support the Electronic Warfare (EW) component of Information Operations. It also describes example constraints that can be used to represent the EW component of a division attack scenario. Finally, it recommends a strategy for adding information operations components to joint and army warfighting simulations and for extending the COAA program to address campaign level planning.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

LIST OF TABLES

Joint Vision 2010 (JV2010) establishes Information Superiority as a key foundation for success. The four concepts of Dominant Maneuver, Precision Engagement, Full-Dimension Protection, and Focused Logistics depend upon our complete control and dominant exploitation of the information domain. Information Operations (IO) are all actions taken to affect adversary information and information systems while defending one's own information and information systems[1] and are thus the means by which we affect this control and exploitation. As now captured in joint doctrine, Information Operations "are a critical factor in the joint force commander's capability to achieve and sustain the level of information security required for decisive joint force operations.

INFORMATION OPERATIONS, SIMULATIONS AND DECISION AIDS

Given the importance of Information Operations to Joint Warfighting, it would be reasonable to conclude that they are represented in the major wargaming simulations in use by the services as well as in the models supporting long range programmatic decision making. In fact, none of the current wargaming simulations (Army's Corps Battle Simulation (CBS), Air Force's Air Warfare Simulation (AWSIM), Navy's Research, Engineering, and Systems Analysis (RESA) Model) in common use today provide automated support for information operations, nor does the Joint Simulation System (JSIMS) program plan address the addition of significant IO capability through at least 2003. It might also be reasonable to conclude that numerous tools exist to support the IO planning process. A review of current and planned

GCCS tools reveals few that provide support for Information Operations.

GENESIS OF THIS SRP

What steps are being taken to correct these problems? Within the Army, the Land Information Warfare Activity (LIWA) is the focal point for land Information Operations. It has the responsibility to provide subject matter technical expertise to the Office of the Deputy Chief of Staff for Operations and Plans (ODCSOPS) regarding all IO and command and control warfare (C2W) issues. It also supports Joint Force Commanders (JFCs) by providing field support teams and tools to the land component commands. In support of these responsibilities, LIWA is coordinating with the JSIMS and WARSIM program managers to have IO capabilities added at the earliest opportunity. Additionally, LIWA is developing decision aids and tools for the field support teams.

In September 1998, LIWA approached COL Ralph Ghent of the Army War College seeking assistance, looking particularly for subject matter expertise support of the development of these decision aids within the context of a Strategy Research Project (SRP). Given this author's, then a student, post graduation assignment as Project Manager for the Warfighter Simulation (WARSIM), thus was born this SRP. In a series of coordination meetings, the SRP topic was both focused on a specific decision aid and broadened to address providing recommendations for incorporating IO into other decision aids, wargaming simulations, and models.

OUTLINE OF THIS SRP

Accordingly, this SRP will proceed from the specific to the general in the following course. First I will review LIWA's chosen decision aid, the Course Of Action Analysis tool developed by the Defense Advanced Research Projects Agency (DARPA) describing its objectives, capabilities, limitations and its potential application to IO. After briefly reviewing the components of IO and their potential to be implemented within the COAA tool, I will describe how the information attack component of IO can be incorporated into COAA. Next, I will describe what additional changes might be required within the COAA tool to broaden its scope as well as provide support for other areas of IO. Finally, returning to the broader perspective, I will provide recommendations for adding IO to wargaming simulations and models while addressing the difficulties therein.

THE COURSE OF ACTION ANALYSIS PROGRAM

PROGRAM DESCRIPTION

"Corps and Division planning staffs in the US Army continue to apply manual techniques in their planning for combat operations, even in the face of the ongoing revolution in information technology."[2] This clear lack of exploitation of available technology to enhance military planners' ability to reduce the planning cycle time and get inside the adversaries' decision cycle time led the DARPA to investigate potential solutions. DARPA's Course of Action Analysis (COAA) program developed a Proof of Principle (PoP) system supporting the course of action development and analysis phases of the military decision making process. The long-term goal of the COAA program is the development of a system supporting multi-echelon planning, execution monitoring and control, real-time modification of plans, and real-time dissemination of plans done in parallel at all echelons[3].

The Military Decision-Making Process consists of seven steps. They are mission receipt, mission analysis, COA development, COA analysis, COA comparison, COA approval, and operations order preparation. The COAA PoP system focused primarily on the COA analysis step while providing necessary tools for COA development and COA comparison. From a scope perspective, the COAA PoP focused on Army Mechanized Division level operations in force-on-force operations. DARPA successfully demonstrated the PoP system at a pilot test conducted at the School of Advanced Military Studies (SAMS). In addition to developing and testing the PoP system, DARPA conducted several studies to investigate other approaches to supporting COAA.

HOW COAA WORKS

So how does the COAA PoP system work? Stripping away all of the user interface, at its core the PoP system uses a technique called constraint satisfaction. Well established within the Artificial Intelligence community, this technique has been used to solve a broad range of problems including some which affect us on a daily basis such as airline scheduling. Constraint satisfaction solves problems by first describing them in terms of relationships between unknowns (or variables). Together, all of the constraints that describe a particular problem are called a constraint set. We then attempt to find values for those unknowns that satisfy all the constraints. It is important to focus on the word "attempt". Some groups of constraints (our problem definition) do not have a solution meaning that no assignment of values to our unknowns satisfies all the constraints. Others have only one, and still others have many solutions. If we can describe a course of action using a set of constraints, this means that we will be able to identify COA that are infeasible (have no solutions). For those COA for which many or multiple solutions exist, it is possible to apply an evaluation criteria to choose among those potential solutions.

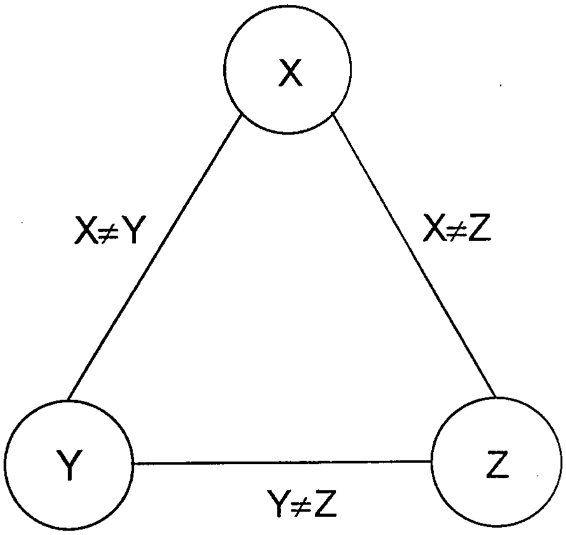

Figure 1: A simple constraint network

Figure 1 shows a simple example of a constraint set also known as a constraint network. The vertices of the diagram represent variables or unknowns. The arcs between vertices represent constraints between unknowns. In this example, there are three unknowns and three constraints. Some valid solutions for this constraint set are X=4, Y=5, and Z=6. In fact, the number of solutions for this particular constraint set is infinite. How does this seemingly simple method of describing a problem translate to the military domain? Figure 2 shows a simple tactical example: a main attack supported by fire from the flank.

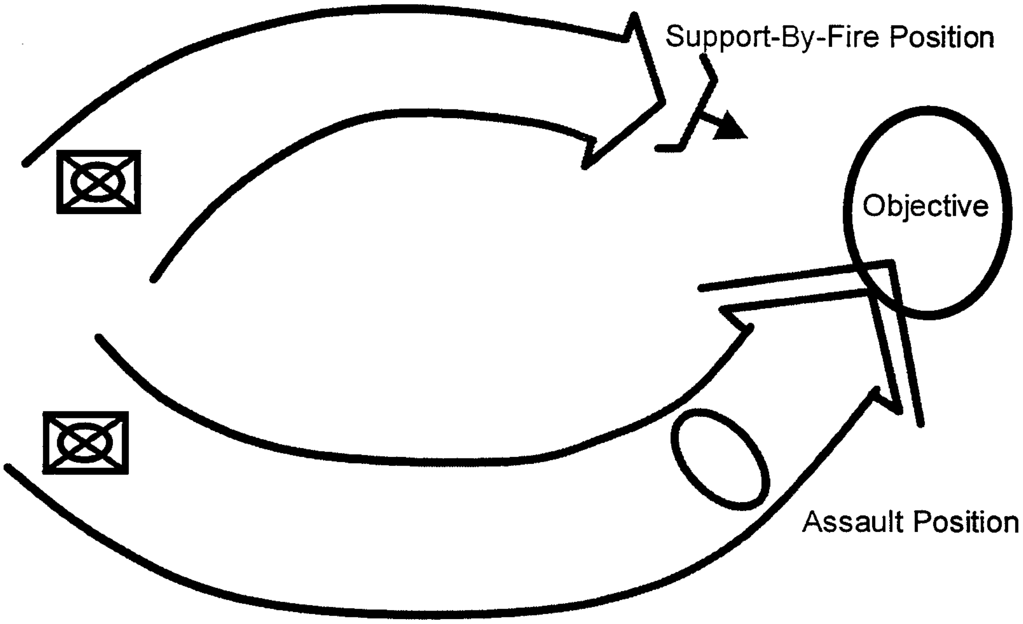

Figure 2: Attack with support by fire from the flank

Figure 3 shows the corresponding constraint network and Table 1 lists the different constants, variables, and constraints used within the network.

CONSTANTS	VARIABLES	CONSTRAINTS
Starting Location	Main Assault Force	strength
Objective	Support By Fire (SBF) Force	+=
Friendly Force	SBF Position	area size
Enemy Force	Assault Position	covered and concealed
	Route to SBF	within weapons range
	Route to Assault Position	area not contained within
		overwatch
		angle between

Table 1: Constants, Variables, and Constraints for the Attack Supported by Fire Network

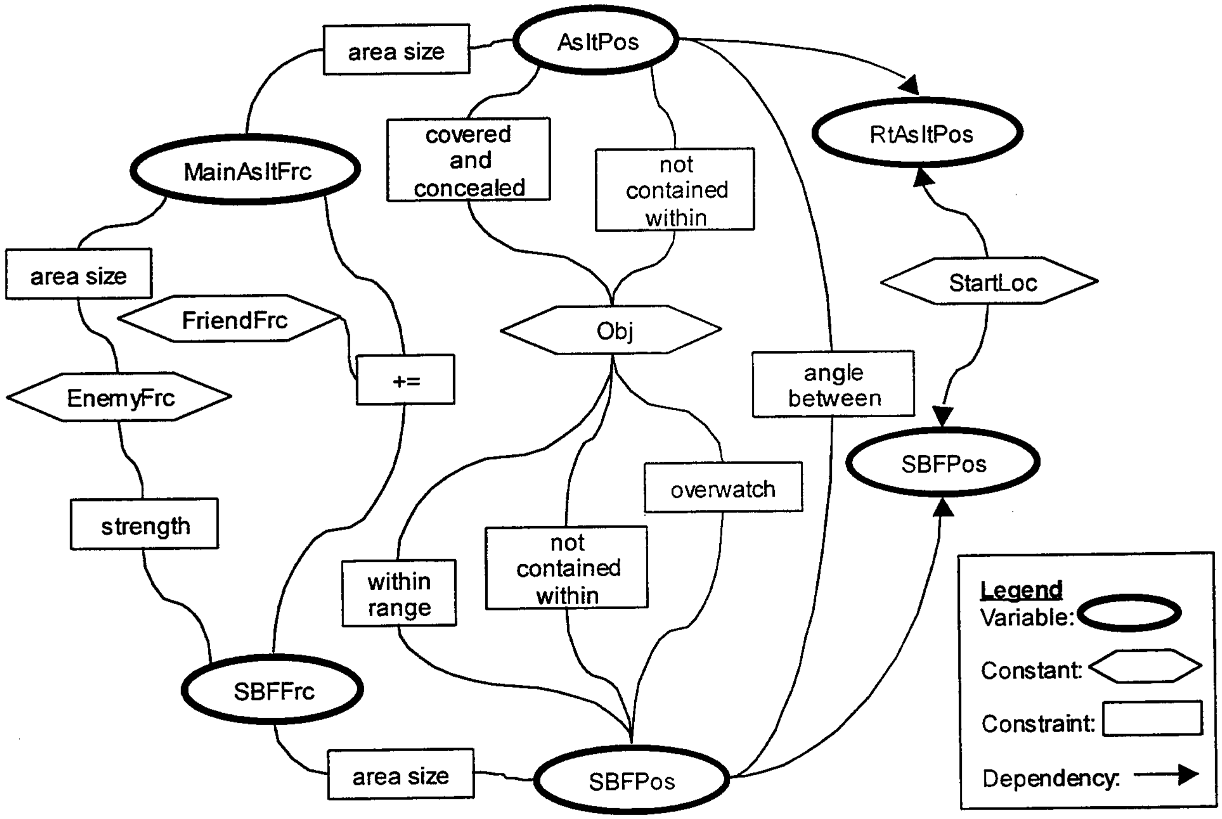

Figure 3: Constraint Network for Attack supported by fire

To interpret the constraint network, pick any two vertices (circle or hexagon) with an arc between them. The box between them defines the constraint between the two vertices. For example, the constraint labeled "area size" joins the two vertices MainAsltFrc and AsltPos. In more understandable terms this means that the assault position must be large enough to contain the main assault force. The constraint "+=" with arcs to vertices FriendFrc, MainAsltFrc, and SBFFrc is interpreted as "The size of the main assault force plus the size of the support by fire force must equal the size of the friendly force." Note that arrows join some vertices rather than a constraint. This means that the two variables are dependent upon one another. In our example network, the route to the assault position (RtAsltPos) is dependent upon both the starting position (StartPos) and the assault position (AsltPos). The dependency could also be represented by adding an additional constraint such as "must join."

The PoP system uses constraint networks similar to the one described above to define and evaluate courses of action. Now, one might say that the example shown above is trivial and does not capture the complexity of military operations nor does it deal with the problem of enemy reaction and friendly attrition or reinforcement. The PoP system solves the problem by using decomposition and sequencing. Decomposition means breaking operations into component parts, usually along unit lines. Continuing with the example above, assume the constraint set is describing a brigade-level operation. Decomposition along unit lines means that a subordinate constraint set for each subordinate unit is required. Sequencing helps to solve both the complexity and reaction/ attrition problems. To create operations that are more complex the PoP links constraint nets together in sequence. For example, the simple attack shown above might be combined with the tactical move required to get forces in place. Sequencing solves the attrition problem by breaking the COA analysis into manageable chunks. After verifying that the variables input by the user for a particular constraint set (which describes a single phase of an operation) constitute a valid solution, the PoP executes a simple simulation to calculate friendly and enemy attrition at the completion of the phase. Once the combat results for a phase are calculated, the PoP determines fuel and ammunition usage. The PoP uses these combat and logistical results as starting values for the beginning of the next phase. Finally, the PoP permits the addition of new forces or the definition of other constraints at the beginning of each phase. By using all of these techniques, the PoP can support generation and evaluation of complex courses of action.

Finally, how does the PoP operate in practice? It is an interactive system, involving the user in each step of the COA generation process. The user starts the process by identifying a mission, the units available and the threat. The PoP system retrieves the appropriate constraint set from its database. The user then uses a map-based interface to create a course of action, specifying subordinate unit missions, establishing control measures and identifying operational phases. For each friendly phase, another user completes the same tasks for the enemy, in effect defining the enemies' responses. Once each phase of a course of action has been fully defined, the PoP system evaluates whether any constraints have been violated. If they have, the user adjusts the course of action until PoP validates the COA. Finally, the PoP runs the force-on-force simulation to determine the forces available to start the next phase. The user repeats this process until all phases of the COA are evaluated.

As stated earlier, DARPA successfully demonstrated the PoP system at Ft Leavenworth using students from SAMS. Based upon that experience, it is reasonable to conclude that constraint satisfaction can be used to represent and evaluate military courses of action, at least at the tactical level. Given that we can use constraint networks to describe military courses of action, can we represent information operations as well? Before answering that question, a brief review of information operations is in order.

REVIEW OF INFORMATION OPERATIONS

According to JCS Pub 3-13, Information Operations are those actions we take to affect adversary information and information systems while protecting our own[4]. Information Operations are applicable across the spectrum of war from Operations other than War through Major Theater War. One needs look only to the importance of information operations in Bosnia and Desert Shield/Storm for recent examples. Information operations also apply at all levels of war from strategic to tactical and consist of both offensive and defensive aspects. As I review the components of IO, I will highlight the spectrum and levels of war in which they are normally used. This review is not a primer on information operations; rather the focus of this review is to determine what aspects of IO might be modeled within the COAA tool. Finally, because the COAA tool supports course of action development for offensive operations, this section will only briefly review defensive information operations.

OFFENSIVE INFORMATION OPERATIONS

Offensive information operations have three primary components. They are perception management, attack, and supporting activities[5].

Perception Management

The first component, perception management, includes those operations designed to manage the threat's perceptions. Within perception management, operational security (OPSEC) is those actions we take to deny the adversary critical information about friendly capabilities and intentions. OPSEC is applicable to all levels of war, but particularly to operational and tactical. During Operation Desert Storm, OPSEC regarding the movement of VII Corps to the left flank was key to making the ground attack successful. Representation of OPSEC within models and simulations requires full modeling of the adversary's intelligence system as well as modeling of all actions we take to protect information regarding our capabilities and intentions.

Psychological operations (PSYOP), the second element of perception management, are actions designed to convey selected information to foreign audiences. They are designed to "get inside our adversaries heads" and influence their behavior. PSYOP is applicable to strategic through tactical levels of war. At the strategic level, PSYOP is focused on the adversary's leadership and public opinion. Bosnia provides a current example of PSYOP at the tactical level. The daily interactions between our forces enforcing the Dayton Accords and the local populace promote a reduction of ethnic tensions that are the root of the Bosnian problem. Psychological operations are very difficult to incorporate within models and simulations. Foremost among the problems is the requirement to model human perception and thinking. An additional complication is the requirement to model the different delivery systems for the PSYOP message. Yet another problem, common to modeling many aspects of IO is the requirement to determine the impact of the PSYOP on the combat operation. This evaluation function or metric may be the greatest common problem in modeling and simulation of information operations.

The final element of perception management is military deception. Also applicable at every level of war, deception is actions we take to affect our adversary's intelligence system to cause it to reach inaccurate conclusions regarding our capabilities and intentions. The end goal of military deception is to cause our adversary to react in specific ways at critical points in the battle. While applicable at every level of war, military deception is most commonly employed at the operational level. The resources required to effectively implement a deception plan are not typically available at the tactical level. In addition, many of the components of a deception operation, if discovered, have the potential for revealing significant information about our own intelligence capabilities. Thus, decision-making regarding a deception operation is likely to be retained at the operational level. Like OPSEC, modeling of military deception requires modeling of the adversary's intelligence system. In contrast, where OPSEC attempts to deny that intelligence system access to information, military deception attempts to portray a specific picture. The devices and methods used to portray this picture or scene must be modeled. Next, the effect of the deception operation on the adversary's decision-making process must be modeled. Finally, the impact of changed adversary decisions on combat outcomes must be modeled. The evaluation of potential outcomes from a successful deception operation appears to be easier than evaluation for OPSEC or PSYOP. However, the complexity of modeling required to portray and assess deception operations combined with deception's probable use only at operational and strategic levels makes it a poor candidate for modeling within COAA.

Attack Options

The next major component of offensive information operations is Attack Options. This is broken into three subcomponents: Electronic Warfare, Physical Attack, and Computer Network Attack. The next three sections will address each of these in turn.

Electronic Warfare

"EW is any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy."[6] Electronic warfare has three major subdivisions: Electronic Attack, Electronic Protection, and Electronic Warfare Support. Within the realm of offensive operations, electronic attack is actions taken against adversary communications and non-communications emitters (radars, etc.) with the intent of degrading, disrupting, or destroying the adversary's capability to exploit the electromagnetic spectrum[7]. Electronic protection involves those actions we take to preserve our own ability to exploit the spectrum during offensive operations. Electronic warfare support is actions we take to enable electronic attack and protection. The strikes against Iraqi surface to air missile sites are a good example of all elements of EW. Electronic warfare support employs the intelligence system to accurately locate adversary SAM sites and associated radars. Electronic protect uses self protection jamming to protect the aircraft operating in the no-fly zone. The physical attack component of EW is executed when HARM missiles are fired at SAM sites which illuminate friendly aircraft with target acquisition radars. Effective modeling of electronic warfare requires modeling of adversary communications systems and radars (targets of EW), friendly intelligence systems, friendly degrade and disrupt systems (jammers), adversary command and control, and determination of effects. Electronic warfare is typically conducted at the operational and tactical levels primarily because the friendly assets normally employed for degrade/disrupt missions are not capable of affecting strategic information targets.

Physical Attack

Closely related to electronic attack is physical attack. Like electronic attack, physical attack targets adversary critical nodes with the goal of destroying the adversary's ability to control his operations or conduct critical operations. Unlike electronic attack, the goal of physical attack is to destroy a capability rather than eliminate it from action temporarily. Physical attack is frequently the preferred offensive information operation when the target has long term value to the adversary or when the target does not have lasting intelligence value. The opening salvo of the air campaign in Desert Storm provides a classic example of broad ranging physical attack of information targets. The initial attack on the Iraqi airborne early warning site opened a corridor through the air defense network. The follow on attacks through that corridor targeted critical air defense, intelligence, and command and control nodes effectively eliminating Iraqi capability to respond to the remainder of the air campaign. Physical attack has the same requirements for modeling as electronic warfare except that the modeling of degrade/disrupt systems must be replaced by modeling of physical attack systems. Physical attack against information targets is employed in tactical through strategic levels of war. When offensive information operations are conducted against strategic targets, physical attack is preferred over electronic attack due to the limitations discussed in the previous paragraph.

Computer Network Attack

The final attack option is computer network attack (CNA). CNA involves actions directed at degrading, disrupting, or destroying adversary computer networks[8]. Typical attacks might include the insertion of viruses or Trojan horses. Because of the potentially far-reaching consequences of CNAs, use is likely to be reserved for the strategic level only. Emerging doctrine places decision-making authority for use of CNA with the National Command Authority. Modeling of CNA requires detailed knowledge of the adversary communications and computer systems, adversary command and control, and friendly CNA capabilities. Along with most other offensive IO, the most significant modeling challenge is the determination of effects upon combat operations.

Supporting activities

The final component of offensive information operations is supporting activities. They include but are not limited to Public Affairs (PA) and Civil Affairs (CA). Public Affairs operations support the overall operation through numerous means, but primarily by keeping internal (own forces) and external (adversary, public) audiences informed. In many cases, PA works hand in hand with PSYOP. In no case will PA be used as an element of a military deception operation[9]. PA is an element of every military operation but is primarily employed within the strategic and operational contexts. "Civil Affairs encompass activities that military commanders take to establish and maintain relationships between their forces and the civil authorities, general populations, resources, and institutions in friendly, neutral, or hostile areas where their forces are employed."[10] While employed across the spectrum of conflict from MOOTW through war, CA is the core activity of many operations other than war. Like Public Affairs, Civil Affairs are conducted at all levels of war but are most important within the strategic and operational context. The battalion aid station operating a health clinic for the local populace may be performing a tactical Civil Affairs operation, but that operation is being conducted within the context of a larger operational or strategic Civil Affairs plan. In any case, modeling of both Public Affairs and Civil Affairs presents daunting challenges. Public Affairs modeling must address all of the same considerations as PSYOP. It must also address additional delivery means, friendly (as opposed to adversary) public perception, reaction, and impact of that reaction on operations. Civil Affairs modeling starts with the same models as Public Affairs but must be extended to address military/civilian interaction and its resulting impact on the desired outcome of an operation. Because of the difficulties in modeling, no current automated models or simulations address Public or Civil Affairs' impacts on military operations.

DEFENSIVE INFORMATION OPERATIONS

Defensive information operations are the friendly counter to all of the offensive capabilities described above. As such, they share many of the same characteristics. According to JCS Pub 3-13 defensive information operations "ensure the necessary protection and defense of information and information systems upon which joint forces depend to conduct operations and achieve objectives."[11] Defensive IO is comprised of four interrelated processes. They are information protection, attack detection, capability restoration, and attack response[12]. Defensive IO are conducted through information assurance, information security, physical security, OPSEC, counterdeception, counter-propaganda, counter intelligence, electronic warfare, and special information operations[13]. As you may conjecture, offensive information operations play an integral role in executing defensive IO. Modeling and simulation of defensive IO require addressing the same processes and functions listed above for offensive IO. But, processes that were modeled for the adversary must now be modeled for our own forces.

INFORMATION OPERATIONS SUMMARY

In summary, many aspects of information operations are difficult to model. In addition, they exceed the scope of tactical operations addressed by the COAA program. The following table summarizes the different components of information operations, their scope, and the problems they present for modeling and simulation. Based upon the analysis above, Electronic Warfare appears to be the most tractable component of information operations to consider for inclusion within the task suite of COAA. The next section will more closely examine EW and attempt to define a corresponding constraint set applicable to division level electronic warfare operations. The final section will provide recommendations on steps required to solve some of the more difficult modeling issues addressed in this section.

Operation	***Range of Military Operations***	***Levels of War***	***Modeling Issues***	***Applicability to COAA***
OPSEC	All	All	Adversary Intel Identification of Essential Elements of Friendly Information Friendly OPSEC Measures	Scope too broad
PSYOP	All, most effective for MOOTW and MTW	All, mostly operational and strategic	Human perception PSYOP delivery means PSYOP plan Measures of effectiveness	Beyond state of the art
Military Deception	All, most important for MTW	Mostly operational and strategic	Adversary Intel Deception delivery means Adversary command and control Adversary decision making Measures of effectiveness	Beyond state of the art
EW	Mostly MTW	Mostly operational and tactical	Adversary communications and non-communications emitters Adversary critical nodes Friendly intelligence systems Friendly degrade/disrupt systems Measures of effectiveness	Limited representation possible with constraint-based system
Physical Attack	Mostly MTW	All	Adversary communications and non-communications emitters Adversary critical nodes Friendly intelligence systems Friendly physical attack systems Measures of effectiveness	Limited representation possible with constraint-based system
CNA	MTW	Strategic	Adversary command and control systems Friendly CNA methodology and systems Measures of effectiveness	Beyond state of the art

Public Affairs	MTW, MOOTW	All, mostly operational and strategic	Adversary public perception Friendly public perception Public affairs delivery means Public affairs plan Public reaction to public affairs announcements Measures of effectiveness	Beyond state of the art
Civil Affairs	MTW, MOOTW	All, mostly operational and strategic	Adversary public perception Civil affairs plan Military/civilian interaction Public reaction to civil affairs operations Measures of effectiveness	Beyond state of the art

Table 2: Summary of Offensive IO Modeling Considerations

ELECTRONIC WARFARE AND COAA

As you may recall from the description of the COAA tool, its primary purpose is to assist in the development and analysis of operational plans. Therefore, the major focus of this section will be the identification of planning considerations for the execution of electronic warfare missions. By logical extension, these planning considerations relate directly to constraints. If these constraints can be implemented within COAA, then it can be used in planning EW missions and assessing their impact on proposed courses of action. With that as a starting point, lets transition to a review of EW planning using Army doctrine defined in FM 34-20 as a reference.

According to FM 34-20, five different missions comprise the task set for electronic warfare. The missions are defend, deceive, disrupt, destroy, and support. While this mission set is different from the IO components described in JCS Pub 3-13 it addresses exactly the same tasks. Defend corresponds to the electromagnetic components of defensive IO, deceive corresponds to the electromagnetic components of military deception, disrupt and destroy correspond to electronic warfare and physical attack respectively. Support refers to the intelligence, command and control, information systems operations, and security required to execute any of the other EW missions. Recalling the analysis of modeling and simulation difficulties described above for the defend and deceive missions, I will focus only on planning for the disrupt/destroy missions.

Review of the EW Planning process

Before proceeding to the details of EW planning, a basic understanding of the EW planning process is required. The EW planning process most closely resembles the targeting process. The first step of this process is intelligence preparation of the battlespace (IPB) to determine high value/high payoff targets (HVT/HPT). High value targets are those targets that are critical to our adversary's operations. High payoff targets are high value targets which if disrupted/destroyed will have the most impact on our own mission success. The next step in the process is an assessment of the HVT/HPT to determine which are susceptible to EW, commonly referred to as electronic preparation of the battlespace. The next step in the process is an evaluation of terrain and line of sight issues. The main point of this step is to determine which vulnerable adversary targets can potentially be affected by friendly jamming assets. If a target node is positioned behind obscuring terrain, there may be no way to affect it with available EW assets that require line of sight to operate effectively. Once this analysis is complete, friendly capabilities against vulnerable targets are assessed. The outcome of this process is a list of target nominations and recommended attack methods. After this initial process is completed, the operations officer, the fire support element (FSE) and the electronic warfare staff officer (EWSO) identify the focus of the electronic warfare plan during each phase of the operation. One example of this might be "Target intelligence and reconnaissance assets during the initial phase; switch to suppression of enemy air defense and artillery units during the attack; finally switch to counter command and control during the exploitation." After determining the general concept for the EW operation, the FSE and EWSO link the target list with the operational synchronization matrix, select the final targets, and determine the specific attack methodology. The creation of the EW Annex to the operations order completes the EW planning process. With that as an overview, lets review the process in more detail and identify the specific planning considerations or constraints that must be addressed.

Development of a constraint network for EW disrupt

IPB is a step-by-step process used to understand the battlespace and the options it presents to friendly and adversary forces. It is a systematic, continuous process of analyzing the adversary and environment in a specific geographic area and consists of four steps: defining the battlespace; describing battlespace effects; evaluating the adversary; and determining adversary COAs. The commander and staff use the results of the

IPB process to wargame adversary COAs, evaluate future adversary actions, and perform situation and target development.[14] For purposes of EW planning, the most important result of this process is target development. Target development produces HVT/HPT for input to the next phase of the process. The COAA system does not have any capability to conduct automated IPB thus HVT/HPT would be input by the user as variables within the constraint set. HVT/HPT are identified by node and probable location as determined by the IPB process. Examples of nodes might be "Division Command Post" or "Regimental Artillery Group Headquarters."

The next phase of the process is assessment of the HVT/HPT to determine susceptible nodes. While this process can be performed each time a HVT/HPT is identified, it is typically performed during routine analysis of the adversary. This routine analysis identifies adversary critical nodes and their common attributes. At a minimum, attributes include equipment, manning, physical distribution, signatures (visual, electromagnetic, acoustic, etc.), limitations, and vulnerabilities (including to jamming and deception). Together these attributes comprise a target folder. Susceptibility analysis consists of comparing the proposed HVT/HPT to the target folders and selecting those that are vulnerable to jamming for further analysis. Within COAA, this vulnerability assessment is expressed as the constraint "vulnerable." All HVT/HPT must satisfy the "vulnerable" constraint.

The next step in the process is evaluation of terrain and line of sight issues. The primary goal of this process is determining whether friendly jamming assets have line of sight to the potential targets. Line of sight is required for the jammer to affect the potential target. The constraint "Has LOS" expresses this requirement within COAA. "Has LOS" requires the introduction of an additional set of variables within our constraint set, namely "Friendly jammer location." Each vulnerable HVT/HPT must also satisfy the "Has LOS" constraint with at least one friendly jammer location.

The next step is evaluating friendly jammer capabilities against the targets that satisfied both "Vulnerable" and "Has LOS" constraints. The capability of a jammer against a specific target depends upon many factors. In simple terms, the effectiveness of a jammer against a specific target depends upon whether it can overpower the legitimate received signal strength of a communications signal at the target. Something called "the link equation" captures the specifics of determining whether this is possible. The details of the link equation are not important for purposes of this discussion but they must be considered in determining the capability of each jammer against its potential targets. We will use the constraint "JmrCapable" to express this constraint within our constraint set. We must also introduce another set of variables within the constraint set. The purpose of communications jamming is to break a communications link between two or more adversary elements. Because communications is typically bi-directional, we only need to break one side of the link to be effective. If the power of our jamming signal is greater than the power of the adversary's received signal at his receiver, then we have successfully achieved our jamming goal. In order to determine our potential for success, we need to know the locations of adversary nodes to which our targets are talking. We will call these adversary nodes "Opposite Ends."

As described above, the next phase of the process is determining the focus of the EW plan and determining the impact of disrupting targets upon the overall course of action. Constraint sets cannot represent this step of the process. Commanders and their staffs must consider several factors during this process including the importance or value of the target to the adversary; the adversary target echelon; and the potential intelligence value of the target. The result of this phase is designation of specific targets to engage as well as those we specifically do not want engaged (guarded or protected targets).

The final phase of the planning process is linking the target list to the operational synchronization matrix. This process must be completed manually. However, we can establish constraints to verify the EW plan can be executed at the proper time(s). We need to introduce several other variables to accomplish this. First, we need to ensure that intelligence assets are available to collect the support data required to execute the jamming mission. For the constraint network, we will use the variable "FrdIntel" and the constraints "CanCollect" and

"Available." "FrdIntel" represents all friendly intelligence assets. "CanCollect" verifies that a given asset can collect the required jamming support information. "Available" verifies that a capable intelligence asset is not tasked to collect against other targets. Next, we need to ensure that none of our nominated targets are on the guarded list. Guarded targets typically have high intelligence value and are not jammed because of the potential intelligence loss. We will use the constraint "NotGuarded" to represent this concern. The final issue of concern is verifying the availability of jamming assets to execute the desired missions at the desired times. The constraint "Available" applies here. The use of "Available" as the constraint is intentional. While it might seem that we should use another constraint such as "JammerAvailable", this would unnecessarily introduce another constraint to the network. "Available" checks on the availability of any resource. All resources (jammers, intelligence collector systems, indirect fire weapons, etc.) have associated scheduling data indicating when they are committed to tasks. The "Available" constraint simply verifies that a resource is not committed at the desired time and thus can be applied to any resource.

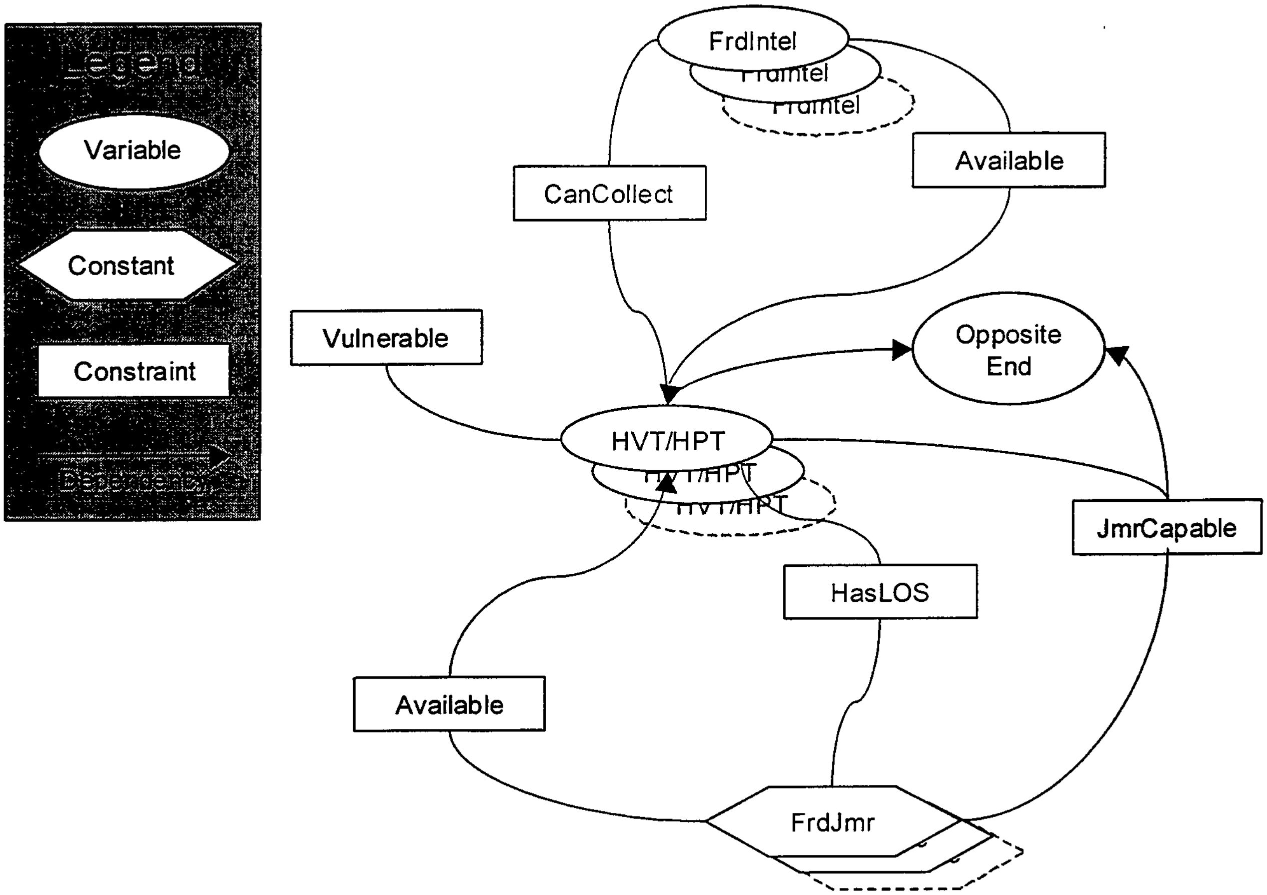

Figure 4: Constraint Net of EW Disrupt Mission

That completes the constraint network for a jamming operation and it is shown in Figure 4 above. It uses the same conventions as the example in section 2. One might question the lack of constraints and dependencies associated with the "Opposite End" and "FrdJmr." The reason that few are required is because the jammer must only overpower the received signal strength from "Opposite End" at the target. If both ends of a link are targets, then the "Opposite End" which is also a target is added to the list of HVT/HPT and considered separately. When multiple targets are considered, the constraint net considers each one in turn while appropriately marking which resources have been consumed before proceeding to the next target. This constraint network can be used to validate whether a proposed jamming operation is feasible. The critical remaining issue for integrating this capability within the COAA tool is the assessment of effectiveness. Given that the proposed jamming operation is executed on schedule and it achieves the desired results, what is the impact on the overall operational plan? The simplified inter-phase combat model used in the COAA tool uses combat power ratios to determine outcomes. Perhaps the COAA user could assign a combat multiplier ratio to each jamming mission. This could then be factored into the inter-phase combat model.

CONCLUSIONS/RECOMMENDATIONS

As shown above, the COAA tool and constraint satisfaction can address some components of information operations, particularly those limited to the tactical and operational levels. However, in its present form COAA cannot address either strategic level issues or the soft components of IO such as PSYOP, Deception, PA and CA. The problem lies not with the COAA's methodology, but with the general lack of models addressing the difficult problems of human perception, societal response, and corresponding measures of effectiveness. Where then do potential solutions to these problems lie? Can COAA be extended to encompass strategic planning? What methods are appropriate for addressing the difficult modeling issues presented by IO? While it is not within the scope of this paper to identify solutions for all these issues, the next several paragraphs provide some guidance and recommendations on paths to follow.

First, to the question of extension of COAA to address strategic planning. In fact, no significant extension is required to the underlying concepts embodied in the COAA program. The primary work that must be completed lies within the knowledge acquisition arena. Strategic level tasks must be codified in terms of constraint nets. COAA must then be extended to recognize the new constraints, variable types, and constants that are sure to be required to describe strategic level tasks. The other required extension is the incorporation of a strategic level simulation to calculate the inter-phase results so that updated variables and constants can be propagated from one phase to the next.

Recalling the modeling issues described in the review of IO, several presented consistent problems for almost every subcomponent of IO. In particular, modeling of human perception and resultant response are required to support OPSEC, PSYOP, Deception, PA, and CA in simulations and models. While no solution to this problem appears on the near horizon, several research areas may provide assistance. First, the blend of artificial intelligence research and cognitive psychology has long been a topic of research. An analysis of the existing work in this area should provide significant insight into methods for incorporating perception management issues into simulations. Another potential source of insight into these issues lies within the commercial strategy gaming community. Games such as Microprose's "Civilization" and Microsoft's "Age of Empires" have long incorporated diplomatic models. Maxis' "Simcity" and its descendents incorporate components that model citizens' happiness. Because of commercial pressure to make games more "real," their artificial intelligence and personnel modeling represents the state-of-the-art. DoD should open a formal technical research program with the gaming community to take advantage of these advances.

Finally, as discussed previously, perhaps the most difficult challenge lies in linking simulation outcomes with IO actions. No simple or immediate solutions exist for this problem and there are many underlying causes. Foremost among these is the lack of empirical data linking operational outcomes to information operations, particularly within the PSYOP, CA and PA subcomponents of IO. LIWA is collecting data based upon its experiences in Bosnia as well as other operations. Once a sufficient database has been collected, analysis may reveal valid measures of effectiveness that can be applied within models and simulations. A potential method for gaining additional insight might be the identification and analysis of historical IO using the same data gathering criteria employed by LIWA today.

In summary, IO represents a daunting challenge to the modeling and simulation community. The COAA program provides some answers for the tactical and operational employment of IO and can be extended to support strategic level issues. AI research in cognitive psychology may help solve some of the problems regarding human perception and interaction. An interface with the commercial gaming community may provide additional assistance. The biggest IO challenge to modeling and simulation is the linking of IO to operational results. The solution to this awaits collection and analysis of empirical data to determine proper measures of effectiveness.

WORD COUNT = 6172

ENDNOTES

[1] U.S. Department of Defense, Joint Doctrine for Information Operations. Joint Pub 3-13 (Joint Warfighting Center, Fort Monroe, VA: October 1998), p. vii

[2] DARPA COAA program report, Executive Summary

[3] Ibid., 2

[4] JCS Pub 3-13, II-1

[5] Ibid., II-3

[6] Ibid., II-5

[7] Ibid., II-5

[8] Ibid., GL-5

[9] Ibid., II-6

[10] Ibid., II-6

[11] Ibid., III-1

[12] Ibid.

[13] Ibid.

[14] U.S. Department of the Army, Intelligence and Electronic Warfare Operations, Field Manual 34-1 (US Army Intelligence Center and School, Fort Huachuca, AZ: September 1994), 2-9.

BIBLIOGRAPHY

Alexander, Robert S.; Schow, Greg. Course of Action Analysis for Corps and Division Level Military Decision Making. Proceedings of the Fall 1998 Simulation Interoperability Workshop, September 1998.

Bartak, Roman. Guide to Constraint Programming. http://kti.ms.mff.cuni.cz/~bartak/constraints/index.html

Calder, Robert B.; Alexander, Robert S.; Richardson, Russell; Lunceford, W. H. Using Constraint Satisfaction for Course of Action Analysis. SAIC Report prepared for DARPA, September 1998.

Defense Advanced Research Projects Agency. Course of Action Analysis. SAIC Briefing prepared for DARPA. November 1998.

Defense Advanced Research Projects Agency. DARPA Course of Action Analysis Program Final Report. Prepared by SAIC for DARPA. December 1998.

Defense Information Systems Agency. OSF GCCS/DII COE System Support Software User's Manual. Washington, D.C.: April 1998.

Kumar, Vipin. Algorithms for Constraint Satisfaction Problems. AI Magazine. Vol 13(1). 1992.

Lunceford, Jr., W. H.; Richardson, Russell; Alexander, Robert S.;Turner, Gregory A.; Tarbox, Glenn H. Course of Action Analysis. SIMTECH T98-016. Proceedings of SIMTECH98. June 1998.

Pountain, Dick. Constraint Logic Programming. Byte Magazine. February 1995.

U.S. Army War College. Communicative Arts Program Directive, AY99. Carlisle Barracks: U. S. Army War College, 1998.

U.S. Department of Defense. Electronic Warfare in Joint Military Operations. Joint Pub 3-51. Joint Warfighting Center, Fort Monroe, VA: June 1991.

U.S. Department of Defense. Joint Doctrine for Information Operations. Joint Pub 3-13. Joint Warfighting Center, Fort Monroe, VA: October 1998

U.S. Department of the Army. Division Operations. Field Manual 71-100. US Army Combined Arms Center, Fort Leavenworth, KS: July 1994.

U.S. Department of the Army. Information Operations. Field Manual 100-6, US Army Combined Arms Center, Fort Leavenworth, KS: August 1996.

U.S. Department of the Army. Intelligence and Electronic Warfare Operations. Field Manual 34-1. US Army Intelligence Center and School, Fort Huachuca, AZ: September 1994.

U.S. Department of the Army. Multiservice Procedures for Command, Control, and Communications Countermeasures. Field Manual FM 90-24. May 1991.

U.S. Department of the Army. Signal Support and the Information Mission Area. Field Manual 24-1. May 1993.

U.S. Department of the Army. Staff Organization and Operations. Field Manual 101-5. US Army Combined Arms Center, Fort Leavenworth, KS: May 1997.