Anticipatory Planning in Information Operations

John M. D. Hill, John R. Surdu
Members, IEEE
Department of Computer Science
Texas A&M University
College Station, Texas 77845

Daniel J. Ragsdale, Joseph H. Schafer
Members, IEEE
Information Technology Operations Center
United States Military Academy
West Point, New York 10996

Abstract

The doctrinal definition of Information Operations (IO) focuses exclusively on offensive and defensive activities. This paper proposes extending the definition of IO to include *information efficacy*. Then it describes a new approach to military planning and execution called Anticipatory Planning. This approach seeks to merge planning and execution, and replaces reaction to events with anticipation of events, making more effective use of the information that is available during the conduct of military operations. This paper presents a methodology for the development of a prototype *decision support system* (DSS) for military decision makers, called the Anticipatory Planning Support System (APSS). This DSS facilitates in-depth analysis of the voluminous data that is available to military decision makers during the course of operations. The paper concludes with an example of the application of Anticipatory Planning to intrusion response operations.

1 Introduction and Motivation

The current definition of Information Operations (IO) focuses on offensive and defensive operations. This definition should be expanded to include information efficacy. There is a tendency to discuss IO separately from conventional operations. In order to gain important synergies the planning and execution of IO and conventional operations should be considered a single activity. Current military planning processes segregate deliberate planning and the execution of the plan. Often, this results in reactive planning once the situation diverges from the original plan. The Anticipatory Planning process discussed in this paper accounts for the chaotic nature of warfare in which possibilities appear and disappear. A proposed Anticipatory Planning Support System (APSS) addresses information efficacy by providing a sophisticated decision support system for the planning and execution of operations. With the advent of APSS, other information age technologies, and the melding of IO and conventional operations, U.S. military planners will have the capability to plan faster and better and stay inside the enemy decision cycle [9].

2 Information Operations

In recent years, the term *information operation* has been *en vogue* as information technologies play an ever-increasing role in military operations. Information Operations (IO) are defined by the Department of Defense (DoD) as "actions taken to affect adversary information and information systems while defending one's own information and information systems." [4] This formal definition places strong emphasis on the offensive and defensive aspects of IO. Unfortunately, while offensive and defensive actions are obviously essential components of IO, this definition neglects a critical issue – the respective *value* of the information available to decision-makers on both sides of the conflict.

The value of information can be measured in term of its usefulness and its usability, or in the most general sense, in terms of its usage. The significance of information usage can be clearly seen from a recent statement made by Secretary of Defense William Cohen. In a March 18, 1999, speech at the National Training Center he stated that "The Army's ability to *use* information to dominate future battles will give the United States a new key to victory, I believe, for years, if not for generations to come." (Emphasis Added) [3]

Information usefulness includes timeliness, accuracy, and analysis of information. The expressed purpose of the APSS methodology is to provide timely and accurate analysis of discrepancies between the planned operation and the actual operation. When agents detect significant differences that impact on the likelihood of success of the mission, the system alerts planners and decision makers so that current and future plans and actions may be adjusted to compensate.

Information usability concerns the decision maker's ready access to the resulting information. International Standards Organization (ISO) Standard 9241 defines usability in terms of the effectiveness, efficiency, and satisfaction of a specified set of users for a specified set of tasks in a particular environment.

Figure 1 depicts the activities and capabilities of Information Operations as they are viewed by the Department of Defense (DoD) [4]. The two large circles illustrate the activities of offensive and defensive IO respectively. The overlap includes activities that are included in both offensive and defensive IO.

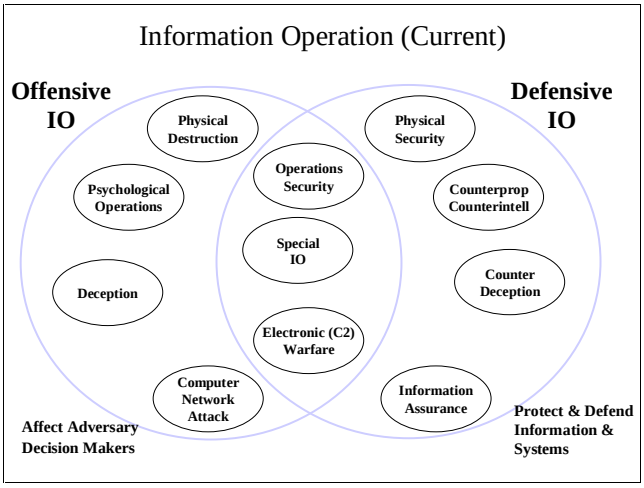

Figure 1: Current Doctrinal Definition of Information Operations

Figure 2 shows the proposed addition of Information Efficacy (IE) to IO. IE is depicted as a foundation for offensive and defensive IO. This addition allows the addition of Situational Awareness, Decision Support, and Command and Control capabilities to the activities of Information Operations, as shown in the figure. The methodology proposed in this paper directly addresses the darker oval, Decision Support.

Information technologies, such as computers and telecommunication and, in particular, simulation and decision support systems enable the execution of sophisticated information operations in which highly useful and usable information is made available to decision makers on one side of a conflict while denying an adversary's access to such information.

In a military operational setting, some of the most useful information comes from information systems that provide *situational awareness* and *decision support*. According to the Army manual for Information Operation, FM 100-6, "situational awareness combined a clear picture of friendly and enemy force dispositions with the commander's assessment of the situation and the commander's intent." [7] The enhanced situational awareness that the proposed system provides will help to reduce the *fog of war* that permeates actual military operations.

Decision support systems "are a collection of tools designed and developed to aid managers in their decision-making processes." [10] The agent-based simulation-enabled methodology described in this paper provides highly useful information to provide for both decision support and situational awareness for military decision makers. In addition, the prototype implementation of this methodology puts this information in a very usable form.

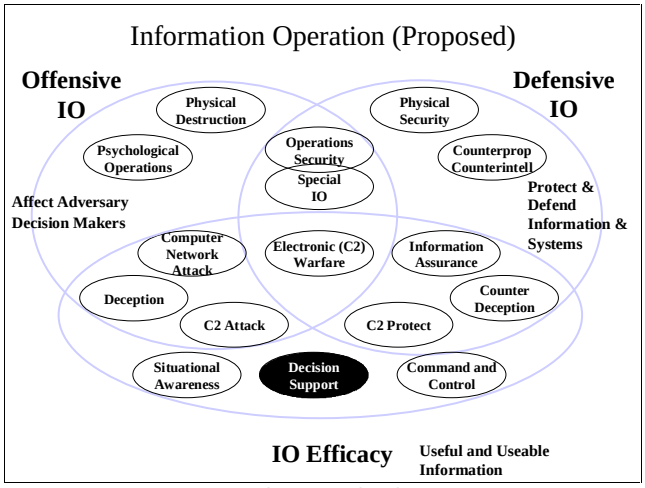

Figure 2: Proposed Definition of Information Operations

While there are no "how we fight" manuals describing the conduct of Information Operations (IO) as there are for conventional operations, it is clear that the conduct of offensive or defensive IO will have many parallels to conventional military operations. One way to make these parallels clear is to have the IO community redefine the traditional military terminology, such as seize, secure, destroy, defend in depth, etc., to apply in this new domain. For instance, the conventional definition of seize is to gain control of a piece of terrain and deploy to prevent its destruction or loss to enemy action. In IO, this might mean to gain control of an enemy database server and block all enemy access to the database for some amount of time.

Traditional military operations and Information Operations are usually seen as disparate activities, with one possibly in support of the other. In order to gain important synergies the planning and execution of IO and conventional operations should be considered a single activity, much as indirect fire or aviation planning is part of the overall plan of operations. New definitions of old terms are insufficient to integrate IO into military operations; a full range of IO procedures, processes, and tasks must be developed.

3 Anticipatory Planning

General (ret.) Wass de Czege has proposed a radically new approach to military planning and execution, which he calls Anticipatory Planning [11]. There are two main thrusts of the General's proposal. The first is that planning and execution should be treated as a tightly coupled, single process, rather than as distinct events. The second is that Anticipatory Planning is necessary in a dynamic and information-rich battlefield environment of the future.

In the traditional Military Decision Making Process (MDMP) various enemy courses of action (COAs) are posited by the intelligence officers, and the operations and planning officers propose various friendly COAs to counter them [8]. Each of these friendly COAs are war-gamed in order to determine their viability. A COA is viable if it is suitable, feasible, and acceptable. *Suitable* means the COA accomplishes the mission and complies with the commander's guidance. *Feasible* means that constraints of available time, space, and resources are met. *Acceptable* means that the tactical or operational advantage gained justifies the cost in resources, especially casualties. Commanders often describe viability concerns in terms of desired end-state conditions at the conclusion of execution. The result of this analysis is a single, chosen COA for use in execution.

There is a well-known axiom that the plan never survives the first shot, which is another way of saying that a branch that was not considered in planning has occurred in execution. Consequently, the commander and staff are forced into a reactive planning mode. Rather than a long detailed plan stemming from comparisons of complete friendly and enemy COAs, the planners need a methodology that merges planning and execution. Such a methodology would develop and consider as many reasonable branches in the plan as possible in the initial planning process, and continuously update the plan as execution progresses. This coupling of planning and execution requires a new process.

According to Wass de Czege, it is futile to try to predict one most likely future and build a plan just for that case. Such plans have too little chance of survival. Uncertainty about the success of an operation is caused by clever, unpredictable enemy commanders who want to win as badly as do friendly commanders. Another source of uncertainty is how successful the friendly forces will be. Staffs are as often surprised by successes, which they are unable to exploit, as they are about slower than anticipated progress or higher than anticipated losses [11].

What is needed, he argues, is to plan against as many of the enemy's options as possible, and to create a plan that addresses those most likely and most dangerous ones. The plan for the conduct of the upcoming (or currently being executed) operation must provide as many branches as planning time allows to deal with the next most likely or dangerous eventualities in priority. As a general rule, Wass de Czega argues, the initial course of action must be able to deal with several of the most likely eventualities with simple, "muscle movement" adaptations. The current generation of planning tools does not help planners generate the many-branched plans rapidly enough to stay ahead of the pace of decisions. Those that were available seemed too simplistic or attrition-paradigm oriented [11].

The ability to develop and consider many branches in a plan necessitates an Anticipatory Planning process. Rather than choosing a single course of action and following it to conclusion, Anticipatory Planning involves maintaining as many possible friendly actions against as many enemy actions as possible. The plan is then considered to be a tree. The nodes of the tree represent states (i.e., snapshots of planned or anticipated dispositions of forces on the battlefield) and decision points in the plan. The branches represent the transition to a new state based on a particular enemy or friendly action. As new branches are developed, the Anticipatory Planning process will continue planning along those branches. In this way, Anticipatory Planning for a branch can be done well in advance and many options can be maintained as long as possible, rather than reactive planning once the branch occurs. Anticipatory Planning will increase the importance of the information collection plan to quickly confirm or deny the viability of branches.

4 Anticipatory Planning Support System

Hill and Surdu presented a methodology for building an automated system to support Anticipatory Planning [5]. See Figure 3 for a depiction of the methodology. A Plan Description is developed to manage the many tree-like branches that occur in planning and execution of an operation. A Planning Executive can use the differences between the plan and the actual operation to control the activities of Planners and Execution Monitors in anticipating future branches to the plan. At the heart of the system are inference mechanisms for determining branches in the plan and simulations for predicting future states.

Information from a World Integrator provides a World View that represents the actual status of execution. The location and/or status of some entities in the actual operation may be estimates. A Planning Executive controls the Anticipatory Planning process and the use of system resources. A Plan Description represents and manages the plan tree. Execution Monitors compare the Anticipated State of the plan derived from the Actual State of the operation with the Planned State at that Node and notify the Planning Executive if there is a potential problem.

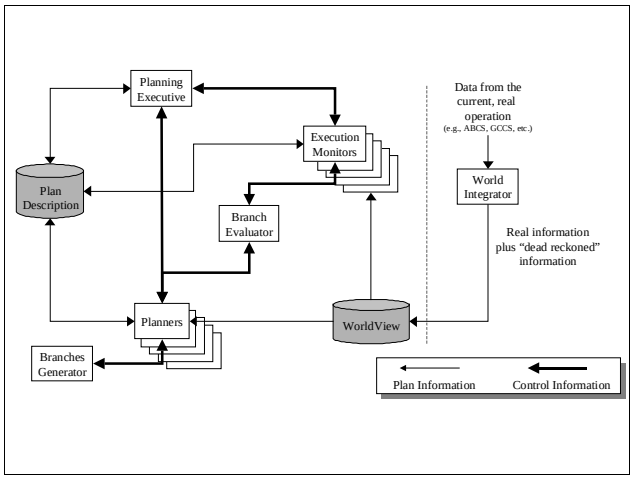

Figure 3: Anticipatory Planning Support System

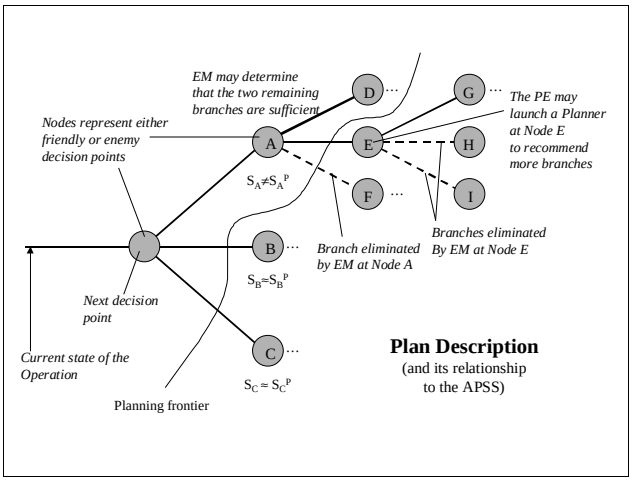

Figure 4: Plan Description

The Planning Executive launches Planners to generate and evaluate new Branches. Planners use a Branch Generator with inference mechanisms that consider possible friendly or enemy actions and produce new Branches. Planners also use a Branch Evaluator to examine a Branch to provide the Planning Executive with viability measures and outcome confidences. The Execution Monitors and Branch Evaluators use simulations to perform their evaluations.

The Plan Description is a representation of the possible ways the operation can proceed (see Figure 4 for a depiction). The Plan Description is a directed tree with the possible states of the plan held by Nodes. The Branches of the tree represent the significant changes between states caused by the actions of the friendly and enemy participants. These transitions can be the result of multiple actions by multiple entities. Normally in simulation literature, an event is something that causes a change in state. APSS is only concerned with significant changes in state, so Branches correspond more directly with transitions composed of several actions rather than with the traditional notion of an event.

A state is the "minimal collection of information with which the system's future state can be uniquely predicted in the absence of chance events." [6] There are three kinds of states maintained in this system: the Actual State, the Planned State, and the Anticipated State. The Actual State comes from the World View. A Planned State is generated when a Planner initially creates a Branch in the plan, and is held in a newly created Node in the Plan Description. If an Execution Monitor is observing a Node, it periodically creates an Anticipated State by using simulations to project the Actual State forward to its observed Node.

Each Node maintains a Planned State of the plan, as described above. The Nodes connect to any Branches that have been produced by Planners. The Nodes also provide an important function in communicating the viability measure associated with the Branches. Measures of viability are computed for Branches after planning or re-planning.

A Branch represents significant state transitions caused by actions taken by the friendly or enemy forces. APSS incorporates a priority scheme that the Planning Executive uses to control when and how much planning is done. If the Planning Executive decides that further planning is required for a Node, a Planner is launched and given the state (Planned State or Anticipated State) of the Node. The Planner examines the outcomes of different possible transitions. The transitions have associated preconditions, viability measures, and a confidence measure. Within the constraints placed on the Planner by the Planning Executive (PE), several of the best transitions become Branches in the Plan Description.

The human planners will not accept or rely on the system unless they understand the system's "logic." If the recommendations of the system "make sense" to the human planners, or if the system provides a reasonable explanation capability, then it is more likely to be accepted and used. Regardless of how flexible and sophisticated the simulation and analysis system is, it still may not provide results that the planner will accept. Accordingly, the system provides the means for the planner to override the results with an outcome that makes more sense. This postpones the need to re-code the event resolution mechanism or the simulation.

5 Intrusion Response Example

As an example, let's consider a hypothetical intrusion response (IR) system based on work done by Carver, et al., who have examined an adaptive agent-based approach for an IR system [1]. Such a system has one or more intrusion detection systems that identify intrusions. Separate modules classify the nature of the intrusion and determine appropriate responses based on an intrusion response taxonomy [2]. The chosen responses draw from a toolbox of available responses mechanisms that are allowable within current response policy constraints.

For the purposes of this example, a Plan Description has been built that includes responses to various possible intrusions. See Figure 5 for a depiction of a portion of this Plan Description that concerns responses to port activity. The Planning Executive has placed an Execution Monitor on a Node corresponding to port probing attacks. There are three planned follow-on states to this intrusion, two of which involve actions (Branches) establishing a "honey pot" to attract the intruder. Note that the branches involve multiple actions by both the defender and the intruder.

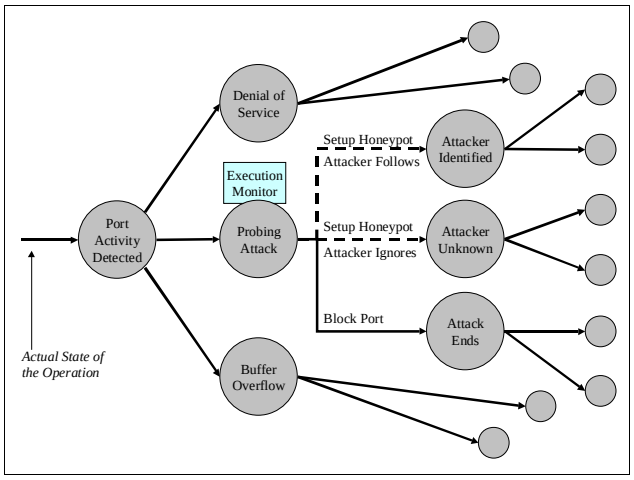

Figure 5: Execution Monitor Invalidates Branches

The operation is ongoing, and the actual, current state of the operation is shown in Figure 5. For whatever reason, something in the Actual State indicates that the honey pot is unavailable. Possibly that machine is being rebuilt, reconfigured, or replaced. The Execution Monitor, subscribing to information about the honey pot from World View, receives a report that the honey pot is unavailable. The Execution Monitor then checks the preconditions associated with each of the Branches leaving the Node to which it is connected and sees that two Branches are no longer valid. The Execution Monitor must decide whether the remaining, valid Branches provide sufficient utility. In this case, a single Branch (i.e., no options) is insufficient. The Execution Monitor then recommends to the Planning Executive that a Planner be attached to the Node.

Problems that invalidate Branches may not be as clear-cut as the one described in this example. The Execution Monitor uses forward simulation to predict the Anticipated State of the operation based on the Actual State. The Execution Monitor can then use heuristics to compare the Anticipated State to the Planned State of the Node to which it was attached. If the differences between these two states are significantly different, the Execution Monitor may recommend to the Planning Executive that a Planner be assigned to the Node.

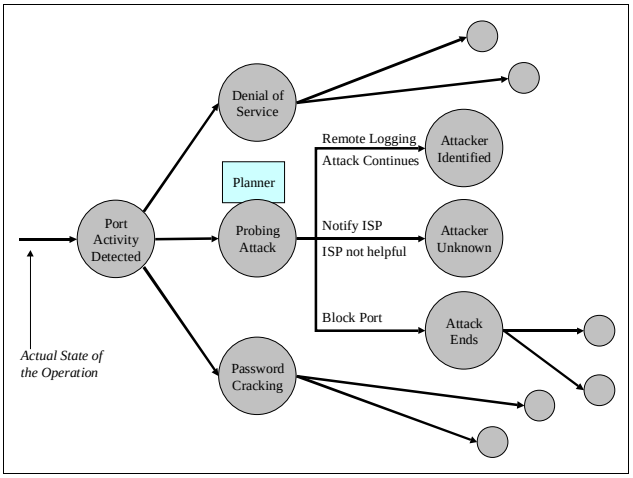

Figure 6: Re-planning by the Planner Module

After being notified by an Execution Monitor that a Planner is needed, the Planning Executive may attach a Planner to the Node. See Figure 6 for the situation after the Planner has been attached. The Planner has invoked a Branches Generator and Branch Evaluator to create new options (note that no honey-pot options are generated), determine their viability, and select the most appropriate ones. In this example, the Planner revalidated the "Block Port" action but also generated two new actions: enabling remote logging and trying to enlist the help of the intruder's Internet Service Provider (ISP). The Planner also created expected states at the Nodes that follow those actions (Branches). For instance, if the system contacts the ISP, but they choose not to cooperate, the identity of the attacker will most likely remain unknown.

Once the new Plan Description segment has been built by the Planner, the Planning Executive may choose to expand the new Nodes by placing new Planners on them. For

example, the "Attacker Unknown" state is probably unsatisfactory, and the system ought to examine possible follow-on actions beyond that Node.

Clearly this is a very simple example; however, it illustrates the interactions between the Execution Monitors, Planning Executive, and Planners. The Execution Monitor identified planned branches that were in danger of failure. The Planning Executive launched a Planner to address the problem. The Planner developed new options. All of this activity served to focus planning effort where it was most needed in anticipation of the actual occurrence of the attack.

6 Conclusion

The current definition of Information Operations (IO) should be expanded to include three parts: offensive operations, defensive operations, and information efficacy. The Anticipatory Planning Support System (APSS) described in this paper addresses this third (new) aspect of IO by providing a sophisticated decision support system for the planning and execution of operations. The Anticipatory Planning process accounts for the chaotic nature of warfare in which possibilities appear and disappear. With the advent of information age technologies and by melding IO and conventional operations, U.S. military planners will have the capability to plan faster and better and stay inside the enemy decision cycle. In this way, rather than two disparate operations, with one possibly in support of the other, they would be part of a single operation.

References

[1] C. A. Carver, Jr., J. M. D. Hill, and U. Pooch, "A Methodology for Using Intelligent Agents to Provide Automated Intrusion Response," in *IEEE Systems, Man, and Cybernetics Information Assurance and Security Workshop*, West Point, New York, June 6-7 2000.

[2] C. A. Carver, Jr. and U. Pooch, "An Intrusion Response Taxonomy and its Role in Automatic Intrusion Response," in *IEEE Systems, Man, and Cybernetics Information Assurance and Security Workshop*, West Point, New York, June 6-7 2000.

[3] W. S. Cohen, "Remarks by Secretary Cohen at the National Training Center (March 18, 1997)," Available at http://www.defenselink.mil/news/Mar1997/t032097_t0318irw.html, April 6 2000.

[4] Department of Defense, *Joint Pub 3-13: Joint Doctrine for Information Operations*, Washington, DC: U. S. Government Printing Office, 1998.

[5] J. M. D. Hill, J. R. Surdu, and U. W. Pooch, "A Methodology to Support Anticipatory Planning," in *Advanced Simulation Technologies Conference: Military, Government, and Aerospace Simulation*, Washington, DC, April 17-20 2000, pp. 22-28.

[6] U. W. Pooch and J. A. Wall, *Discrete Event Simulation: A Practical Approach*, Boca Raton, FL: CRC Press, 1993.

[7] U. S. Army, *FM 100-6: Information Operations*, Washington, DC: U. S. Government Printing Office, 1996.

[8] U.S. Army, *Field Manual 101-5: Staff Organization and Operations*, Washington, D.C.: U.S. Government Printing Office, 1997.

[9] U.S. Army, *FM 100-5: Operations*, Washington, DC: Headquarters, Department of the Army, 1993.

[10] A. Vinze and A. Sen, "Expert Assistance for the Decision Support Process Using Hierarchical Planning," *IEEE Transactions on Systems, Man and Cybernetics*, vol. 21, no. 2, Mar-Apr 1991, pp. 390-401.

[11] H. Wass de Czege, Personal Communication (regarding Anticipatory Planning), retired Army Brigadier General and military theorist, October 1999.