

NAVAL POSTGRADUATE SCHOOL MONTEREY, CALIFORNIA



THESIS

DTIC QUALITY INSPECTED 2

USING EXPERT SYSTEMS TO CONDUCT VULNERABILITY ASSESSMENTS

by

Debra A. Lankhorst

September 1996

Thesis Advisor:

Carl Jones

Approved for public release; distribution is unlimited.

19970103 044

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE September 1996	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE USING EXPERT SYSTEMS TO CONDUCT VULNERABILITY ASSESSMENTS		5. FUNDING NUMBERS	
6. AUTHOR(S) Lankhorst, Debra A.			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey CA 93943-5000		8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.		12b. DISTRIBUTION CODE	
13. ABSTRACT An Information Warrior faces a complex and dynamic operating environment. To conduct an accurate Vulnerability Assessment and Risk Analysis of the enemy force (or a friendly force), a multitude of cause and effect relationships must be examined. Many times the person at the battle scene conducting the assessment may lack experience and/or knowledge, precluding a time-sensitive and effective assessment. The author proposes a framework for a global network of expert systems and decision support systems to conduct the Vulnerability Assessments and maintain Information Warfare readiness through realistic training. The author also presents a Vulnerability Assessment and Risk Analysis heuristic with the objective of expanding the knowledge base and decision speed at the on-scene commander level. In achieving and implementing this global network, numerous benefits can be realized, including increased speed and efficiency in the receipt of intelligence information, thereby allowing for improved decision-making capabilities. Since the technology and know-how are already available, this vision of the global network is attainable and can be successfully implemented and operated.			
14. SUBJECT TERMS System Dynamics, Simulations, Modeling, Software Engineering		15. NUMBER OF PAGES 111	
		16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL

NSN 7540-01-280-5500

Standard Form 298 (Rev.

2-89)

Prescribed by ANSI Std. Z39-18 298-102

Approved for public release; distribution is unlimited.

**USING EXPERT SYSTEMS TO CONDUCT
VULNERABILITY ASSESSMENTS**

Debra A. Lankhorst
Lieutenant, United States Navy
B.S., University of North Carolina at Greensboro, 1984

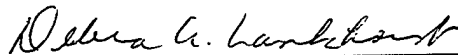
Submitted in partial fulfillment
of the requirements for the degree of

**MASTER OF SCIENCE IN INFORMATION TECHNOLOGY
MANAGEMENT**

from the

**NAVAL POSTGRADUATE SCHOOL
September 1996**

Author:



Debra A. Lankhorst

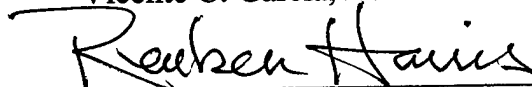
Approved by:



Carl R. Jones, Thesis Advisor



Vicente C. Garcia, Associate Advisor



Reuben Harris, Chairman
Department of Systems Management

ABSTRACT

An Information Warrior faces a complex and dynamic operating environment. To conduct an accurate Vulnerability Assessment and Risk Analysis of the enemy force (or a friendly force), a multitude of cause and effect relationships must be examined. Many times the person at the battle scene conducting the assessment may lack experience and/or knowledge, precluding a time-sensitive and effective assessment. The author proposes a framework for a global network of expert systems and decision support systems to conduct the Vulnerability Assessments and maintain Information Warfare readiness through realistic training. The author also presents a Vulnerability Assessment and Risk Analysis heuristic with the objective of expanding the knowledge base and decision speed at the on-scene commander level. In achieving and implementing this global network, numerous benefits can be realized, including increased effectiveness and efficiency in the receipt of intelligence information, thereby allowing for improved decision-making capabilities. Since the technology and know-how are already available, this vision of the global network is attainable and can be successfully implemented and operated.

TABLE OF CONTENTS

I. INTRODUCTION	1
A. EXPERT SYSTEMS IN INFORMATION WARFARE	1
B. PURPOSE OF RESEARCH	2
C. SCOPE OF RESEARCH	3
D. THESIS ORGANIZATION	5
E. ACKNOWLEDGEMENTS	7
II. INFORMATION WARFARE	9
A. INFORMATION WARFARE	10
B. THE FIVE PILLARS OF COMMAND AND CONTROL WARFARE	13
C. THE INTELLIGENCE PROCESS	18
III. MODELING INFORMATION WARFARE FOR AUTOMATED ANALYSIS	23
A. VISION	23
B. MODELING INFORMATION WARFARE FOR AUTOMATED ANALYSIS	24
C. HEURISTIC	25
IV. EXPERT SYSTEMS FOR INFORMATION WARFARE	47
A. EXPERT SYSTEMS FOR VULNERABILITY ASSESSMENT/VULNERABILITY ANALYSIS	47
B. DECISION SUPPORT SYSTEMS FOR RISK ANALYSIS	50
C. EXPERT SYSTEMS AND INTELLIGENT AGENTS FOR TRAINING ..	50
D. EXAMPLE SCENARIO	51

V. IMPLEMENTATION ISSUES	57
A. CURRENT TECHNOLOGY	57
B. SYSTEM REQUIREMENTS	60
C. MIGRATION PLAN	63
VI. CONCLUSIONS	67
A. LESSONS LEARNED	69
B. RECOMMENDATIONS FOR FUTURE RESEARCH	70
APPENDIX A. IMPACT TABLES	71
APPENDIX B. EXPERT SYSTEMS	83
APPENDIX C. EDUCATIONAL SKILLS REQUIREMENTS	89
LIST OF REFERENCES	95
INITIAL DISTRIBUTION LIST	101

I. INTRODUCTION

A. EXPERT SYSTEMS IN INFORMATION WARFARE

Information Warfare encompasses a broad area of operations, always hovering on the fringes of the battle space and beyond. Historically, battles have been won or lost not only on the "might" of the armies, but also on the value of the information gained on the opponent's capabilities and weaknesses, and denial to the enemy of the same valuable information. Today's technological advances have presented an opportunity for warfighters to gain an advantage over their adversaries. That advantage is knowledge of the enemy's capabilities and weaknesses.

In developing a Vulnerability Assessment of either enemy or friendly forces, Information Warfare experts look for weaknesses which can be exploited. With a finite group of experts available, scarce resources are spread thin. Expert systems can provide the breadth and depth of knowledge and experience of those experts at the battle-scene, thereby enabling less knowledgeable personnel to identify and evaluate an adversary's weaknesses. Expert Systems and Decision Support Systems can perform this important facet of Information Warfare. In addition, using modeling and simulation, the same expert system can also train personnel in the theoretical and practical application of the concepts of Information Warfare while giving hands-on experience on the computer system. Finally, with today's technological advances in artificial intelligence, using expert systems/decision support systems and modeling/simulation techniques to assist in

conducting Vulnerability Assessments and training can realize great benefits for the military in the realm of Information Warfare.

B. PURPOSE OF RESEARCH

Information Warfare and the use of expert systems/decision support systems to support the conduct of Vulnerability Assessments are the primary foci of this thesis. In order to automate this process, the author develops a heuristic for conducting Vulnerability Assessments, with applicability to a global network of expert systems and decision support systems in mind. To effectively employ this system, training is another issue that must be considered. The author presents the requirements for using the same expert system to conduct Vulnerability Assessments and training. The author examines the various training techniques to determine which ones will work well with the proposed expert system network. The training should cover the concepts and practical application of Information Warfare and provide expert system familiarization. In addition, several issues concerning the implementation of the global system, such as the necessary Educational Skills Requirements, system requirements, and the delivery path, are also addressed. In realizing the vision of a global network of expert systems/decision support systems conducting Vulnerability Assessments and training, benefits can be realized, such as increased speed and efficiency in the receipt of intelligence information. Improved decision-making capabilities and sailors trained in the practical application of Information Warfare concepts are the end results.

C. SCOPE OF RESEARCH

Some of the topics presented in this thesis are discussed from a broad point of view since they are already discussed in current literature and an in-depth discussion is beyond the scope of a single thesis. Information Warfare is one of these topics. References annotated throughout Chapter II will provide the reader access to a further explanation. Expert Systems are treated similarly, again because the focus of this thesis is on a specific application of expert systems and not on the abundance of material that has been written on this particular subject over the past twenty years.

Automated analysis is discussed with a more narrow focus to achieve clarity in presentation. The purpose of this thesis is to develop an heuristic to conduct Vulnerability Assessments and Risk Analysis that is non-specific to any particular target. This thesis examines the suitability of an expert system in actually conducting the Vulnerability Assessment based upon input from the battlefield commander or his designated representative, the cryptologist. That same expert system along with simulation software can also provide training in conducting Vulnerability Assessments, offering a more robust dual system to the command. The challenge of maintaining the currency of the information is also an issue addressed in this thesis. The potential for implementing a global network of many expert systems will provide for the most recent information available. The last topic presented includes a few of the practical implementation issues for the installation and operation of the global network. Therefore, the resources consulted during the course of this thesis include:

- a literature review of Vulnerability Assessments
- a review of the methodology involved in developing Vulnerability Assessments
- interview(s) of personnel who have conducted Vulnerability Assessments
- a literature review of expert systems and decision support system technology
- a literature review of current and planned training for Information Warfare for Vulnerability Assessments, Computer Science, and Information Technology.

To research the feasibility of successfully achieving the vision of an expert system conducting the Vulnerability Assessment and providing the pertinent training, the following research questions are addressed in this thesis:

- How can Expert Systems and Decision Support Systems assist in improving Vulnerability Assessments?
- What Expert System technologies are being used in the civilian and/or the military sector that could be used in developing Vulnerability Assessments or Information Warfare training?
- To what extent are Expert Systems and Decision Support Systems currently being used in the military for analysis of activity?
- What are the core competencies/educational skills requirements for Information Warfare, Computer Science, and Information Technology?

- What role does Expert Systems have in Information Warfare? How can Expert Systems/Intelligent Agents/Simulation help in training for Information Warfare?
- Is there a reasonable expectation that a global network of expert systems and decision support systems can be successfully implemented?

D. THESIS ORGANIZATION

Information Warfare is a broad area to discuss because of its relatively recent emergence into the limelight. While many personnel have been conducting Information Warfare over the years, these same personnel usually have different perspectives on what Information Warfare really entails. Therefore, following MOP 30 and Joint Pub 3-13 guidance, the author provides a summary of Information Warfare as defined by the United States Naval Service.

Technology has provided the means to achieve the objectives of Information Warfare. Assessing the capabilities and weaknesses of the enemy are vital to the success of Information Warfare; therefore, the author explores the possibility of automating the Vulnerability Assessment process. The other chapters in this thesis support this same process. This thesis is divided into six chapters and two appendices:

- Chapter I - Introduction. This chapter introduces the topic and goal of developing a methodology for conducting Vulnerability Assessments, with an explanation of the purpose and scope of this thesis.

- Chapter II - Information. This chapter presents a discussion on Information Warfare and Command and Control Warfare based on the guidance provided within Naval instructions.
- Chapter III - Modeling Information Warfare for Automated Analysis. This chapter presents the heuristic for conducting Vulnerability Assessments and Risk Analyses.
- Chapter IV - Expert Systems for Information Warfare. This chapter discusses the use of Expert Systems within the Information Warfare and Command and Control Warfare arena.
- Chapter V - Implementation Issues of Expert Systems for Information Warfare. This chapter presents a discussion on the issues involved in implementing a global network of expert systems and decision support systems.
- Chapter VI - Conclusion. This chapter presents the author's viewpoint on the feasibility of using a global network of expert systems and decision support systems to conduct Vulnerability Assessments and provide realistic training.
- Appendices
 - Appendix A - Impact Tables (Virus, Technology, Geopolitics, Economics). These tables summarize the information currently available on the impact of these four variables on a computer or computer system.

- Appendix B - Expert Systems/Decision Support Systems. This appendix presents a further explanation of expert systems and decision support systems.

E. ACKNOWLEDGMENTS

I would like to acknowledge several individuals whose contributions made the thesis process enjoyable and meaningful. Thank you for your patience, guidance, and assistance.

Dr. Carl Jones provided the initial impetus (germ of an idea) to research the possibility of expert systems performing Vulnerability Assessments. His superb ability to guide and mentor students helped me throughout the entire thesis process.

Professor Vicente Garcia gave freely of his time, helping me to sort through the minutiae of Information Warfare and its application.

LT David Jacobson is a great listener, acting as a sounding board and sanity check; basically keeping my head out of the clouds.

[THIS PAGE LEFT INTENTIONALLY BLANK]

II. INFORMATION WARFARE

Information Warfare plays a vital role in battle. The commander with the most current intelligence information gains crucial minutes to formulate an attack or prepare for a counter-attack, giving that same commander a distinct advantage over the adversary. Today's technological advances have presented an even better opportunity for warfighters to gain an advantage over their adversaries. An historical example is the information obtained from space surveillance assets which gave Allied forces an advantage during the air supremacy campaign of Desert Storm. Consequently, one can say that advanced knowledge of the enemy's intentions and capabilities gained from the use of Information Warfare gives the battlefield commander the ultimate advantage.

In developing a Vulnerability Assessment for Command and Control Warfare (C2W) either of enemy or friendly forces, Information Warfare experts look for weaknesses to exploit or attack. Since subject matter experts are a scarce resource and not always available on-scene, capturing their valuable knowledge in an integrated expert system and decision support system is critical to helping to identify an adversary's and one's own weaknesses. Technology, in the form of an integrated Decision Support System and Expert System, can handle this important facet of Information Warfare. This type of technology offers the greatest opportunity to expand the capabilities of Information Warfare in the C2W environment from both a strategic and tactical perspective.

A. INFORMATION WARFARE

However, before delving into how this technology can be employed in the Information Warfare arena, it is necessary to discuss the precepts of Information Warfare. Admiral Boorda had this to say about Information Warfare,

“Information Warfare is about warfighting – making sure that the people who go fight have the very best chance to get their mission done, win that fight, and come home safely.” [Ref. 1]

The Joint Doctrine for Command and Control Warfare (C2W): Battlefield Application of Information defines Information Warfare as “those actions taken to achieve information superiority in support of national strategy by affecting adversary information and information systems, while leveraging and protecting our own information and information systems.” [Ref. 2: p. I-5] The major difference between Information Warfare and C2W is that Information Warfare operates in support of national strategy and supports the full range of combat and non-combat missions across the range of military and non-military operations. C2W is the battlefield application of Information Warfare. [Ref. 2: pp. I-5 to I-6]

C2W is the integrated use of the five Pillars of Information Warfare to achieve superiority over the enemy. The five pillars are:

- Psychological Operations
- Military Deception
- Operations Security

- Electronic Warfare
- Physical Destruction.

All of these are mutually supported by intelligence to deny information to, influence, degrade, or destroy the adversary's C2 capabilities. [Ref. 2: p. I-7] These actions occur while protecting friendly C2 capabilities from similar efforts by the enemy. To be effective, C2W must allow the joint battlefield commander to affect the adversary's decision-making without degradation of his own assets. In order to accomplish this goal, the friendly commander could use one or a combination of the following actions:

- *"disrupt the enemy's decision cycle*
- *delay the enemy's processing and dissemination of information through the decision cycle*
- *influence the enemy's perception of the military situation to prevent the enemy commander from affecting the friendly commander's decision-making."* [Ref. 2: p. I-7]

Any or all of these actions might impair the adversary's decision-making capabilities. A joint commander can affect these actions by any of the following means:

- slowing the enemy's operational tempo
- disrupting any plans the adversary might have

- disrupting the enemy commander's ability to focus combat power
- influencing the enemy commander's estimate of the situation.

At the same time, the friendly commander must minimize his vulnerabilities against the possibility of the same enemy actions directed at his forces. [Ref. 3: p. 2] Therefore, the battlefield commander must coordinate C2W tactics to ensure minimal interference from friendly forces.

The Chairman of the Joint Chiefs of Staff, Memorandum of Policy No. 30 states that the objective of C2W is to "maximize U.S. and allied military effectiveness by integrating C2W into military strategy, plans and operations, exercises, training, communications architectures, computer processing, systems development, and professional education." [Ref. 3: p. 1] By employing IW techniques in all aspects of C2W, friendly forces can achieve the end result of decapitating the enemy's command structure from its body of combat forces. [Ref. 3: p. 3] The underlying rationale for this reasoning is that military forces are highly dependent upon timely and accurate information for effective application of combat power. Modern combat forces achieve this information through their command and control structure. [Ref. 3: pp. 3-6]

Policy and decision makers agree that the speed and pace of battle and the agility of combat forces continually increase as the battle progresses. [Ref. 3: pp. 3-6] Therefore, the battlefield commander with the greater ability to evaluate the battlefield, expose, and exploit the enemy's vulnerabilities will have a greater chance to prevail. [Ref. 3: pp. 3-6] The battlefield commander uses this knowledge to seize the initiative,

hopefully forcing the enemy into a reactive mode. As noted by Jomini, purely defensive maneuvers rarely win the war. [Ref. 4: p. 168]

Synergistic application of the Five Pillars of Command and Control Warfare maximizes combat power, which is the force applied by either friendly or adversary troops that is necessary to achieve the objective. [Ref. 3: pp. 3-6] The combined use of operations security, military deception, psychological operations, electronic warfare, and physical destruction can effectively disrupt the enemy force's decision cycle, thereby allowing the friendly commander to seize the initiative. Paralysis, misdirection, fear, and insecurity are just a few of the potential outcomes.

B. THE FIVE PILLARS OF COMMAND AND CONTROL WARFARE

1. Operations Security

Operations Security (OPSEC), is defined as a process used for denying the adversary information about friendly intentions, capabilities, or limitations. [Ref. 5: p. 265] The effective employment of the OPSEC process can:

- *“protect U.S. and allied forces from an enemy C2W strategy*
- *identify friendly actions that an adversary can observe*
- *determine indicators that an adversary could use to derive critical information*
- *develop and execute measures that eliminate or reduce friendly vulnerabilities to exploitation by adversary collection means.”* [Ref. 6: pp. I-32 to II-33]

Military forces achieve these actions by first performing a Vulnerability Assessment. Putting OPSEC into practice means avoiding mention of upcoming battle plans or supporting activities in areas easily observed by the enemy. An enemy agent can piece together isolated comments or activities such as numerous unscheduled cargo flights or military leave being canceled, to accurately guess friendly intentions. Denying the enemy commander this advance information can help achieve the element of surprise.

2. Military Deception

The second pillar of C2W is Military Deception which involves actions taken to mislead enemy decision makers or protect friendly capabilities. [Ref. 7: p. 23] Its stated goal is to cause the enemy decision maker to respond in a manner that assists in the accomplishment of friendly objectives. [Ref. 5: p. 230] In plain terms, displaying actions that would lead the enemy to believe a person or unit will take a particular action, eliciting a desired incorrect reaction from the opponent. However, in reality, the action will be conducted in a totally different way. In short, the battlefield commander will deceive his opponent. Several key factors have been identified for Military Deception to be effective. These key factors include:

- *“the deception must have an objective*
- *the targeted enemy commander must have the decision authority to make the desired decision*
- *a story complete with a notional order of battle must be available to back up the executed deception*

- *a means must exist to evaluate the effectiveness of the deception.*” [Ref. 2: p. GL-5]

A military commander must carefully plan and coordinate military deception operations in concert with conventional battle plans to achieve maximum effectiveness.

Throughout history, military commanders have used deception against the enemy. For example, during the Revolutionary War, General George Washington’s forces created forged documents stating that the total number of American troops in Pennsylvania reached 40,000 men instead of the actual number of 3,000 men. These documents were “captured” by the British, who of course believed the forged documents. [Ref. 8: p. 23] Another example is from the Persian Gulf War. The coalition forces continually conducted amphibious rehearsals and exercises along the Persian Gulf. Those exercises combined with other deception operations convinced the Iraqis that the coalition’s primary intention was to conduct an amphibious assault. The coalition achieved total immobilization when they instead commenced operations in a totally different direction. [Ref. 9: p. 24] These examples exhibit how effective military deception operations can be in changing the enemy commander’s decisions.

3. Psychological Operations

The objective of Psychological Operations (PSYOP), the third pillar, is to cause or reinforce attitudes and behavior that will result in the favorable attainment of friendly force objectives. [Ref. 7: p. 24] The aim of these operations is to lower morale, reduce the efficiency of enemy forces, and cause “dissidence and disaffection within their ranks.”

[Ref. 10: p. 1-1] In order to attain this goal, the message conveyed to the enemy troops must:

- be based in fact
- be verifiable by whatever means the adversary has available
- consider the perceptions and considerations of those who are targeted.

If the enemy does not believe that a deceptive message is true or that friendly forces cannot carry out the threat or action, then the effectiveness of PSYOP will be greatly reduced. [Ref. 11: pp.12-14]

For a military commander to plan and execute a psychological operation, he/she requires extensive information about the location and identity of the target, any vulnerabilities, and knowledge of the existing political, economic, social, cultural, and historical infrastructure within the target area. [Ref. 10: p. 1-1] Once this information is gained from intelligence sources, the military commander decides what “message” he/she wants the enemy to receive and may employ a variety of means to deliver it. These methods could include, but are not limited to political and diplomatic communiqués, leaflets, or loudspeaker broadcasts. These tools can be used in any manner to encourage enemy forces to desert or surrender. [Ref. 12: pp. III-44 to III-45]

Historically, military deception has played a part in many wars. For example, in World War II, the U.S. spread propaganda through leaflets and radio broadcasts in the hopes of undermining the enemy’s will to resist, demoralizing the enemy’s troops, and sustaining the morale of allies. [Ref. 13: pp. 20-21] Years later during the Persian Gulf

War, coalition forces dropped radios tuned to American propaganda stations, pamphlets, and leaflets combined with the BLU-82 bombs. The bombs blasted a path through Iraqi ground forces. The radios, pamphlets, and leaflets, combined with the bombs, contributed to a significant increase of Iraqi soldiers surrendering to coalition forces.

[Ref. 13] More recently, U.S. forces dropped pamphlets and leaflets in Haiti encouraging the populace to follow the legal Haitian president. Military deception can be used to gain an advantage over the enemy by creating vulnerabilities within the enemy ranks.

4. Electronic Warfare

Electronic Warfare, the fourth pillar, is any military action that involves the use of electromagnetic or directed energy to attack an enemy or control the electromagnetic spectrum. [Ref. 12: pp. GL-7 to GL-8] This broad area is divided into three subdivisions: electronic attack, electronic protect, and electronic warfare support. The offensive arm of electronic warfare is *electronic attack* which involves the use of electromagnetic or directed energy to attack the enemy with the intent of degrading, neutralizing, or destroying combat capabilities. It also includes actions such as anti-radiation or directed energy bombs or missiles that prevent the enemy from using the electromagnetic spectrum. The defensive arm of electronic warfare is *electronic protect* and includes actions to protect friendly forces from the use of enemy electronic warfare measures. [Ref. 12] One example of electronic protect is to stop the enemy from jamming the portions of the electromagnetic spectrum used by friendly forces. In order to employ either the attack or protect mode, the friendly forces need information to assist in making decisions. Electronic warfare support uses intelligence assets to collect and disseminate

information for immediate decisions involving electronic warfare operations. [Ref. 12]

The use of electronic warfare can have a catastrophic effect on the enemy. For example, during Desert Storm, coalition forces jammed Iraqi communications and sensors and disrupted their command and control to limit the Iraqi ability to gather information and transmit decisions. [Ref. 7: p. 26]

5. Physical Destruction

The fifth pillar of Information Warfare is Physical Destruction, which is the ability to identify, locate, and prioritize enemy targets accurately and then destroy them selectively. [Ref. 5: p. 113] Since the overall guiding principle of C2W is to integrate disruptive means without using large amounts of limited destructive resources, the battlefield commander must decide on the relative importance of each target. [Ref. 14: p. viii] If the target is important to achieving the battle plan, the battlefield commander must determine the amount of destructive resources that will destroy or neutralize the target. In short, the importance of the enemy target in the overall battle objective is the deciding factor on whether or not that target should be destroyed, neutralized, or ignored.

C. THE INTELLIGENCE PROCESS

1. Intelligence Support

The Five Pillars of Command and Control Warfare enable the military commander to employ various measures to achieve victory on the battlefield. Individually, the use of each pillar will attain limited success; however, the integrated use of all or some of the pillars increases the chances of exploiting the enemy's vulnerabilities to the fullest extent.

But battle plans formulated without considering the use of Intelligence Support denies the military commander necessary information. One can say that intelligence support is critical to the success of C2W. The bottomline is that the operational commander must have the best intelligence on enemy situations, intentions, and capabilities to weigh the potential advantage of specific actions. [Ref. 3: pp. 6-7]

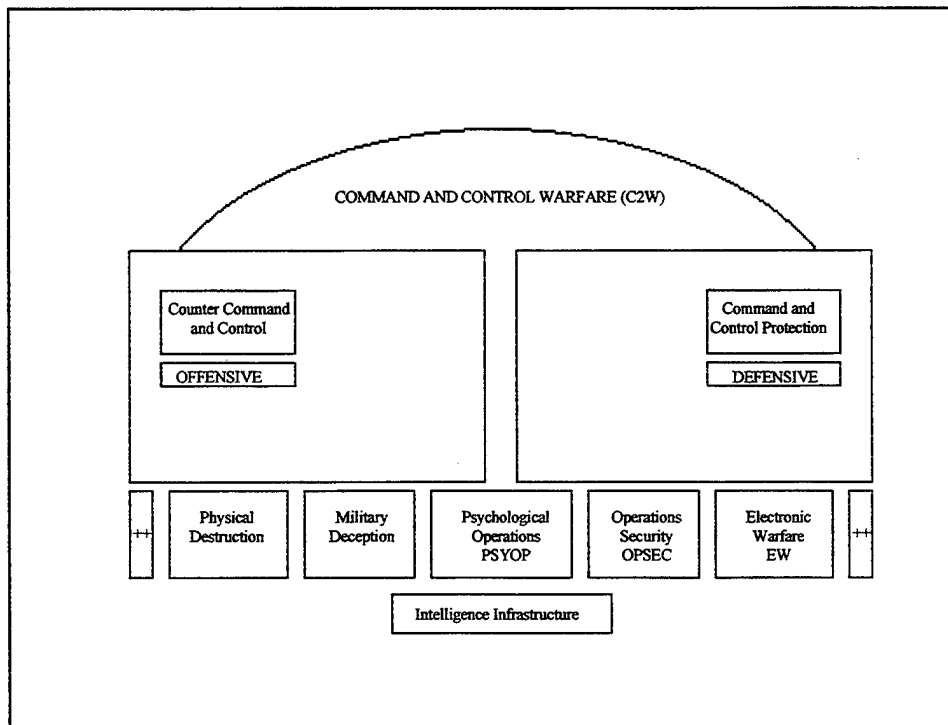


Figure 1. The Command and Control Warfare Umbrella [Ref. 7: p. 28]

Figure 1 shows how intelligence support underlies and supports the Five Pillars of Command and Control Warfare, contributing information to each pillar. This valuable information is gained through the collection, evaluation, analysis, and interpretation of all available information. [Ref. 3: p. 7] Examples of intelligence support include:

- developing and maintaining databases of sufficient detail to support C2W in geographic areas of potential conflict

- identifying critical C2 nodes, links and sensors of potentially hostile nations
- understanding of potential enemy C2, communications, peacetime and wartime operating modes of sensor systems, organizational structure and netting, procedures, and deployment to support precision-guided munitions/electronic warfare
- assessing capabilities, limitations, and vulnerabilities of potential C2 targets
- identifying the power structures of key political and military leaders in potentially hostile nations, and obtaining biographical data and psychological profiles of leaders
- estimating hostile counter C2 capabilities to assist in determining the vulnerability of U.S. C2 capabilities and impact on U.S. and friendly military operations
- providing timely and reliable indications and warning information to operational commanders
- providing timely information to persons and systems during actual engagement of enemy forces
- providing accurate direction finding
- supporting battle damage assessments. [Ref. 3: pp. 6-10]

This information is gained through the cooperation of many intelligence agencies (national, theater, and tactical levels), and all collection efforts (HUMINT, SIGINT, MASINT, IMINT, etc.). The information is then fused to provide the most up-to-date all-source intelligence to the military commander. It is important to recognize that the best

operational plan uses the optimal mix of assets. Intelligence is the key to achieving this mix, Figure 2 displays some of the information provided to the battlefield commander and to which of the five pillars it applies.

PHYSICAL DESTRUCTION	ELECTRONIC WARFARE	OPERATIONS SECURITY	MILITARY DECEPTION	PSYCHOLOGICAL OPERATIONS
Target identification	Target location	Friendly vulnerability assessments	Identification of deception targets	Identification of enemy perceptions, strengths, and vulnerabilities
Target location	Electronic preparation of the battlefield	Identification of C2 (enemy C2) threat	Selection of believable story	Selection of a focus for PSYOP campaign efforts
Time for optimal attack	Frequencies, critical nodes, modulations, and link distances	Denial of friendly capabilities and intentions	Identification of enemy order of battle to include intelligence collection system	Identification of enemy order of battle to include key commanders and their associated C2 support systems
Battle damage assessment	Time for optimal attack	Evaluation of deception efforts	Placement of assets	Placement of assets
Intelligence preparation of the battlefield	Battle damage assessment		Analysis/feedback	Analysis/feedback

Figure 2. Intelligence Support to Command and Control Warfare [Ref. 7: p. 30]

2. Feedback and Bomb Damage Assessment (BDA)

The importance of obtaining feedback and BDA on the effectiveness of the C2W measures cannot be stressed enough. This information will provide the friendly force's intelligence assets with an assessment on the degradation of the enemy's systems. Using this information, the C2W planners will be able to update their objectives and priorities and fine-tune the battle plan. [Ref. 15: p. 4-12]

[THIS PAGE LEFT INTENTIONALLY BLANK]

III. MODELING INFORMATION WARFARE FOR AUTOMATED ANALYSIS

Vulnerabilities are the Achilles Heel of an enemy or friendly force. In developing a Vulnerability Assessment, Information Warfare experts look for weaknesses which can be exploited. Since subject matter experts have many demands on their time and may not be readily available, capturing their valuable knowledge can assist others in helping to identify vulnerabilities. Technology in the form of an integrated Expert System and Decision Support System can perform this vitally important aspect of Information Warfare.

A. VISION

During peacetime operations, planning is even paced, allowing time to recheck plans for missed details. However, when the situation becomes stressful and time is a scarce commodity, real-time problem solving exaggerates many human limitations - "the tendency to overlook relevant information, to respond inconsistently, to respond too slowly, or to panic when the rate of information flow is too great." [Ref. 16: p. 264] All of us can imagine a normal day that suddenly changes because a situation has developed that demands your complete attention.

Picture this, the battlegroup commander wants to know where a particular enemy force is most vulnerable. Gathering as much information on the enemy force as possible, you begin inputting the information into the expert system. The intelligence headquarters provides an expert system using the latest technology and a knowledge base obtained

from the intelligence field's experts. Based upon the strategic goals of the battlefield commander, this expert system will help identify the most vulnerable area(s) of the enemy force, ensuring that all possible areas are explored. You are now engaged in Command and Control Warfare, the battlefield application of Information Warfare.

B. MODELING INFORMATION WARFARE FOR AUTOMATED ANALYSIS

Vulnerability assessments are a critical part of Information Warfare. They are a tool used to identify the enemy's weaknesses and evaluate them for future exploitation. To assist in performing this assessment more efficiently and effectively, the author developed a heuristic for automated analysis. The purpose of this heuristic is to provide non-experts with a suggested procedure to identify a target's vulnerabilities. The target encompasses a range of possibilities from the actual battlefield to the enemy command and control center(s) and pertinent systems.

The author reviewed approximately twenty-nine vulnerability assessments, [Refs. 17-45], to determine how each assessor had performed the analysis. From assessing cruise missiles, buried concrete bunkers, airplanes, or tanks, to assessing networks and computer systems, all of the vulnerability assessments followed the same general pattern, with some variation due to the specificity of the target. The heuristic below illustrates a general procedure for performing a vulnerability assessment that the author developed by comparing the procedures followed by the authors of the twenty-nine vulnerability assessments.

C. HEURISTIC

1. Identify the objective, mission and/or target.
2. Break the target down into subcomponents, and describe in detail the IW attributes of each subcomponent of the target. Develop a hierarchy of subcomponents or a network view of the target (this will help later with failure node analysis.) Either of these will help determine the interoperability of the components. The decomposition should consist of enough detail to “predict” the effect of actions such as disconnecting the command structure cohesiveness of enemy commander.
3. Identify the center of gravity. Use failure node analysis to identify the interoperability of components. Basically, failure node analysis is neutralizing a component of the target and determining what other target components will be affected by the “failure” of the first neutralized component. The importance of establishing the center of gravity cannot be stressed enough. As Clausewitz stated:

“One must keep dominant characteristics of both belligerents in mind. Out of these characteristics a certain center of gravity develops, the hub of all power and movement, on which everything depends...It is therefore a major act of strategic judgment to distinguish these centers of gravity in the enemy’s forces and identify their spheres of effectiveness.” [Ref. 46: pp. 595-6 and p. 468]
4. Categorize and identify vulnerabilities. Vulnerabilities are defined as “a weakness or lack of controls that would allow or facilitate a threat actuation against a specific asset or target.” [Ref. 47: pp. 69-88] Categories of vulnerabilities fall under four different classifications:

- Long-term investment (e.g., the ability to control the enemy's infrastructure)
- Lack of Discovery (e.g., friendly forces apply a threat without the enemy discovering the action)
- Possible Discovery (e.g., friendly forces apply a threat and the enemy might discover the action)
- Information denial (e.g., bomb the telecommunication antennas). [Ref. 48]

If possible, obtain lists of vulnerabilities already identified (from open and classified sources such as manufacturers and research efforts, assessments already completed, intelligence analyses, expert opinion, personal experience, other commands/agencies, etc.).

5. Perform a target assessment. This step correlates threats with vulnerabilities. In the case of offensive action, correlating friendly assets with enemy vulnerabilities, and in the case of defensive action, correlating enemy assets with friendly vulnerabilities. This step determines the highest impact per applied threat.
6. Evaluate vulnerabilities. Every system is vulnerable to some degree. The purpose of a vulnerability analysis is to determine the marginal or incremental importance of each vulnerability relative to all other possible vulnerabilities. The purpose of the evaluation is to categorize and hopefully depict clusters of vulnerabilities. [Ref. 31: p. 4] This is a critical step in the vulnerability assessment, because without the

clustering of vulnerabilities, the assessor cannot perform failure node analysis to discover the center of gravity. The evaluation is subjective because it depends upon the evaluator's personal experience and knowledge. Nevertheless, this subjective information must be translated into quantitative data in order to compare the relative importance of vulnerabilities. This will also assist in the implementation of an expert system to perform the vulnerability analysis. Location of the target, mission requirements, and even the hardware/software used within the target are some of the factors that are considered during the course of the evaluation. [Ref. 31: p. 4] A key challenge is to determine which of the target components are actually affected by each vulnerability. The failure node analysis process will also assist in determining the target components that each vulnerability affects. Another key challenge is to determine how to evaluate the vulnerabilities affecting each functional area to provide an overall vulnerability rating for each area.

7. Develop model of vulnerability assessment process. This includes a model of the target subcomponents compiled to achieve a model of the entire target. Determine the variables that impact the system, such as the effect of viruses, technology, geopolitics, and economics, see Appendix A. An additional step in this process is an adjustment for time; determining how changes in the variables change or impact a target over time. This factor is subjective and is determined by the battlefield commander. One point that should be mentioned is that the variables will change depending upon whether the "war" is considered Command and Control Warfare (cyberwar) or Information Warfare (netwar). [Ref. 49: p. 141]

8. Derive the incremental analysis. A method that will provide some objectivity involves determining how one subcomponent changes with respect to changes in another subcomponent. The objectivity results not from relying on the value of individual variables, but in examining their interdependence. Most of the vulnerability assessments that the author analyzed developed the methodology as if the vulnerability existed in a single part of a system. Using incremental analysis allows the assessor to account for the response of a system with interdependencies to different threats. As one variable changes, the impact of the change is reflected throughout the system. To use this method, a number of steps are required.
- Derive the Vulnerability index. The vulnerability index reflects a relative impact that successful exploitation will have on a system. Changing one variable will have some measure of an impact on the overall system performance and effectiveness. This index will model that impact.
 - Model the target using the detailed description from step 2 above. Include identified vulnerabilities from any associated threats and outside influences affecting the system. Figure 3 models one subcomponent of a target, allowing the user (assessor) to visualize the different variables (i.e., labor, capital, outside influences, time, and any vulnerabilities) that affect the target or system. Figure 4 is a linear perspective for this same model, which includes a subjective importance rating of the particular subcomponent to the overall

target. Figure 5 is a model for an entire target, depicting the independence and interdependence of the subcomponents.

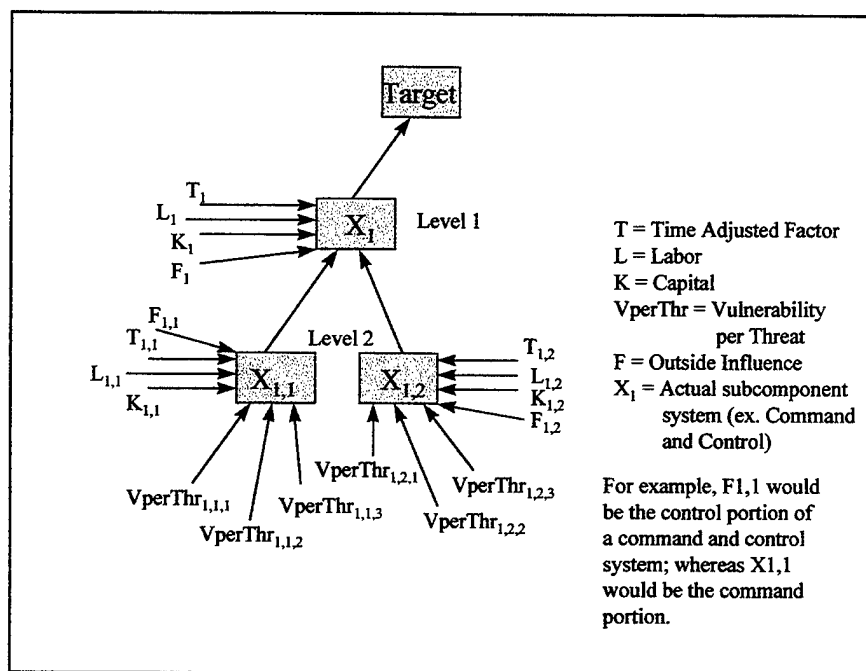


Figure 3. Subcomponent Model

Variables can affect the target at different levels. For instance, outside influences could affect the target at either Level 1 or 2, or even both levels. The assessor must determine this relationship.

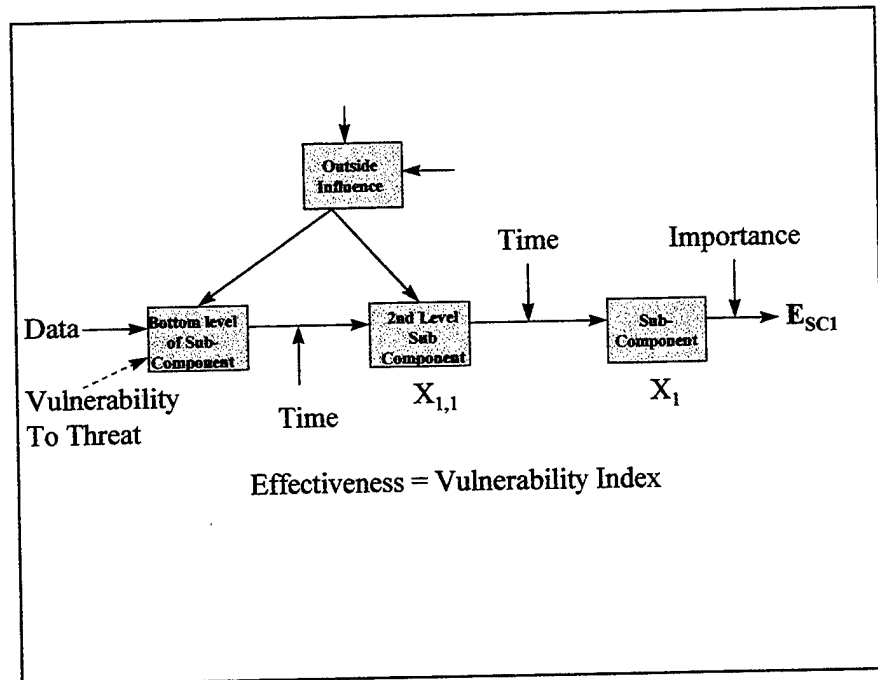


Figure 4. Model of Subcomponent of Target

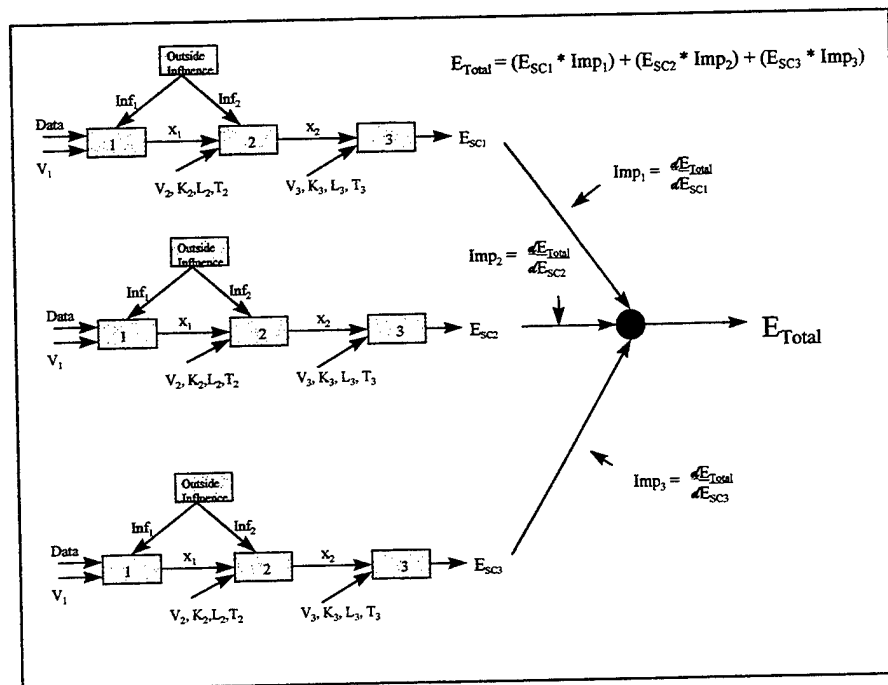


Figure 5. Target System Model

Figure 5 is a model of an entire target, complete with several subcomponents, as opposed to Figure 4, which models a single subcomponent.

- Determine the Impact of the Vulnerability. Exploiting a particular vulnerability may impact the entire system. This value quantifies the level of this impact. The actual value is determined by a subjective evaluation of factors, as determined by expert analysts and by the user. For example, since computers are the backbone of many military systems, exploiting their vulnerabilities by inserting a virus into the computer software can have potentially serious consequences on the entire military system at little cost to the attacker. Table 1 depicts the effect that a virus could have on a system and the potential impact this particular virus could have on the overall target. The expert or cryptologic/intelligence officer will assign a probability depending upon how the virus is predicted to impact the selected target, thereby achieving the military objective. Complementary Metal Oxide Semiconductor (CMOS) is a battery powered portion of memory that holds the date, time, and system setup parameters. The Basic Input/Output System (BIOS) contains all of the code required to control computer functions such as the keyboard, display screen, disk drives, etc. [Ref. 50] If one of these subsystems is infected, no one can use the computer. The Master Boot Record (MBR) is the portion of the computer that is accessed to start the operating system.

Table 1. Vulnerability Impact Assessment [Ref. 51]

Virus		
<u>Type</u>	<u>Effect</u>	<u>Impact (assigned by decision-maker)</u>
Boot Infectors		
AntiCMOS (LENART)	Blanks CMOS/BIOS values.	.6 (for example)
AntiEXE (Newbug)	Overwrites MBR.	.3 (for example)
Da' Boys	Overwrites the DOS 5.0 Boot Sector.	.7 (for example)
ExeBug	Makes small changes to MBR.	.2 (for example)
	Changes computer's CMOS.	
Form	Doesn't infect files.	.4 (for example)
	Moves original boot sector.	

- Determine the Time-Adjusted Factor. This value represents the amplification of the effects of Technology, Geopolitics, and Economic Factors on the target based on the time of threat application. Tables 2-4 depict a portion of a potential Impact Assessment for Technology, Geopolitics, and Economics. Table 5 shows how the battlefield commander would decide the changes in importance of Technology, Geopolitics, and Economics over time (from a cyberwar (C2W) perspective). The battlefield commander may decide that it is more important to attack sooner (in time periods 1 or 2) rather than later (in time periods 5 or 6). Therefore, the battlefield commander would assign a high number (like .6) to time periods 1 or 2, and a low number (like .1) to time periods 5 or 6. Examples of these three tables are contained within Appendix A and Tables 2-4. It is important to distinguish between netwar (IW) and cyberwar (C2W). *Netwar* applies to “societal struggles most often associated with low intensity conflict by non-state actors, such as terrorists or drug cartels. On the other hand, *cyberwar* refers to “knowledge-related conflict at the military level.” [Ref. 49: p. 141] Therefore, the impact of affecting the socio-economic balance (which would become a variable in the event of netwar) would not be considered if the friendly commander is conducting cyberwar. Table 2 lists the various technologies considered important by priorities (Priority 1, 2, and 3) and the potential effect that these technologies can have on current combat capabilities if breakthroughs occur. Table 3 lists the effects on the military and society in general (which would affect the mentality of the populace) of the different types of governments. Table 4 lists the effects of some of the various economic indicators, which are selected on the basis of impact on military spending.

Table 2. Potential Technology Impact Assessment [Ref. 52]

Technology			
<u>Type</u>	<u>Effect</u>	<u>Goal</u>	<u>Impact (assigned by decision-maker)</u>
Priority 1			
Force Protection			
Active camouflage, active thermoelectric ribbons, IR sensors, microprocessors, enhanced light weight power sources, heat	Makes soldier invisible, day or night, to whole range of battlefield sensors across electromagnetic spectrum.	Invisible Soldier Image Avoidance and Signature	.7 (for example)

Table 3. Potential Geopolitical Impact Assessment [Ref. 53]

Geopolitics		
<u>Type</u>	<u>Effect</u>	<u>Impact (assigned by decision-maker)</u>
Government		
Democratic	Free speech, free market economy	.6 (for example)
Isolationist	Poor economy	.2 (for example)
Participative (UN)	Deterrence and containment, sanctions, keep peace	.4 (for example)
Communist	No free speech, money for military	.7 (for example)
Socialist	No free speech, money for military	.7 (for example)
Fascist	No free speech, money for military	.7 (for example)
Totalitarian	No free speech, money for military	.7 (for example)
Dictatorship	No free speech, money for military	.7 (for example)
Change in Government		
Coup	Military enforcement	.7 (for example)
Election	Generally peaceful	.3 (for example)

Table 4. Potential Economic Impact Assessment [Ref. 54]

Economics		
<u>Type</u>	<u>Effect</u>	<u>Impact (assigned by decision-maker)</u>
Interest Rates	Adjusts for inflation.	.3 (for example)
Value of dollar	Can indicate inflation.	.5 (for example)
Inflation	Weakens currency's buying power.	.7 (for example)
Industry Prices	Affects prices on defense contracts.	.8 (for example)
Defense Budget	Determines how much military can spend	.9 (for example)

Table 5. Time Adjusted Factor [Ref. 55: p. 169]

Time-Adjusted Impact				
Total Impact = Impact(Technology) * Impact(Geopolitics) * Impact(Economics)				
See Technology, Geopolitics, and Economics Impact Tables				
<u>Time</u> <u>Period</u>	<u>Relative Importance</u> <u>of Time</u>	<u>Total</u> <u>x Impact</u>	=	<u>Time Weighted</u> <u>Fraction</u>
1	0.5	0.105		0.0525
2	0.3	0.105		0.0315
3	0.1	0.105		0.0105
4	0.1	0.105		0.0105
5	0	0.105		0
...n				
Total	1			Sum of Row = .105

Table 5 accounts for the impact of the three aforementioned variables over different time periods. This type of analysis allows the battlefield commander to judge the effect of either employing C2W or Information Warfare tactics on a short term or a relatively long term basis. These equations are very difficult if not impossible to complete at the local commands, which is why an expert system is necessary.

- Develop the system mathematically with the inherent interdependencies. For example, the vulnerability index is a function of subcomponent 1, subcomponent 2, and subcomponent 3, etc.. Once the interdependencies have been established, the equations shown below depict how a change impacts the other parts of system. This works by first establishing an initial estimate of the variable (i.e., Capital, Labor, Vulnerabilities, etc.) and then multiplying and changes in that initial estimate with respect to the subcomponent system. For example, investing money in a new operating system affects the command

and control portion of the target, so K will change with respect to its effect on the enemy's command and control system.

$K = \text{Capital}$

$L = \text{Labor}$

$T = \text{Time_Adjusted_Factor}$

$F = \text{Outside_Influences}$

$V = \text{Vulnerabilities}$

$X_1 = \text{Subcomponent_system_of_Target_X}$

$X_{1,1} = \text{Subcomponent_of_}X_1$

$X_{1,2} = \text{Other_Subcomponent_of_}X_1$

$E_{SC1} = \text{Effectiveness_of_Subcomponent_1}$

$$X_1 = [f(X_{1,1}, X_{1,2}, T_1, L_1, K_1, V_1, F_1)]$$

Equation 1. Variables affecting the Target X

Equation 1 defines the target as a function of several variables. The subcomponents of Target X_1 are derived below in Equations 2 and 3, quantifying the changes in the variables affecting the two subcomponents of the target. Equation 4 derives the incremental analysis for Target X_1 .

$$X_{1,1} = [(K_{1,1} * \frac{\partial X_{1,1}}{\partial K_{1,1}}) + (L_{1,1} * \frac{\partial X_{1,1}}{\partial L_{1,1}}) + (T_{1,1} * \frac{\partial X_{1,1}}{\partial T_{1,1}}) + (F_{1,1} * \frac{\partial X_{1,1}}{\partial F_{1,1}}) + (\frac{\partial X_{1,1}}{\partial V_{1,1,1}} + \frac{\partial X_{1,1}}{\partial V_{1,1,2}} + \frac{\partial X_{1,1}}{\partial V_{1,1,3}})]$$

Equation 2. Incremental Analysis for Subcomponent 1 of the Target X

$$X_{1,2} = [(K_{1,2} * \frac{\partial X_{1,2}}{\partial K_{1,2}}) + (L_{1,2} * \frac{\partial X_{1,2}}{\partial L_{1,2}}) + (T_{1,2} * \frac{\partial X_{1,2}}{\partial T_{1,2}}) + (F_{1,2} * \frac{\partial X_{1,2}}{\partial F_{1,2}}) + (\frac{\partial X_{1,2}}{\partial V_{1,2,1}} + \frac{\partial X_{1,2}}{\partial V_{1,2,2}} + \frac{\partial X_{1,2}}{\partial V_{1,2,3}})]$$

Equation 3. Incremental Analysis for Subcomponent 2 of the Target X

$$\begin{aligned}
X_1 = & [(K_{1,1} * \frac{\partial X_{1,1}}{\partial K_{1,1}}) + (L_{1,1} * \frac{\partial X_{1,1}}{\partial L_{1,1}}) + (T_{1,1} * \frac{\partial X_{1,1}}{\partial T_{1,1}}) + (F_{1,1} * \frac{\partial X_{1,1}}{\partial F_{1,1}}) + [(\frac{\partial X_{1,1}}{\partial V_{1,1,1}} + \frac{\partial X_{1,1}}{\partial V_{1,1,2}} + \frac{\partial X_{1,1}}{\partial V_{1,1,3}}) \\
& * \frac{\partial X_1}{\partial X_{1,1}}]] + [(K_{1,2} * \frac{\partial X_{1,2}}{\partial K_{1,2}}) + (L_{1,2} * \frac{\partial X_{1,2}}{\partial L_{1,2}}) + (T_{1,2} * \frac{\partial X_{1,2}}{\partial T_{1,2}}) + (F_{1,2} * \frac{\partial X_{1,2}}{\partial F_{1,2}}) + \\
& [(\frac{\partial X_{1,2}}{\partial V_{1,2,1}} + \frac{\partial X_{1,2}}{\partial V_{1,2,2}} + \frac{\partial X_{1,2}}{\partial V_{1,2,3}}) * \frac{\partial X_1}{\partial X_{1,2}}]] + [(K_1 * \frac{\partial X_1}{\partial K_1}) + (L_1 * \frac{\partial X_1}{\partial L_1}) + (T_1 * \frac{\partial X_1}{\partial T_1}) + (F_1 * \frac{\partial X_1}{\partial F_1})]
\end{aligned}$$

Equation 4. Incremental Analysis for Target X_1

$$I_1 = \frac{\partial E_{Total}}{\partial E_{SC1}}$$

$$I_2 = \frac{\partial E_{Total}}{\partial E_{SC2}}$$

$$I_3 = \frac{\partial E_{Total}}{\partial E_{SC3}}$$

$$E_{Total} = [(E_{SC1} * I_1) + (E_{SC2} * I_2) + (E_{SC3} * I_3)]$$

Equation 5. Effectiveness of the Threat

Equation 5 depicts the equation to determine the effectiveness of any changes in the variables affecting the Target X . The impact is determined by computing the incremental analysis effect of the target X with respect to the incremental analysis effect of each individual subcomponent of the target, (X_1) or (E_{SC1}). Equation 6 is the effectiveness of the threat on the entire target. This equation is a compilation of Equations 1-5.

$$\begin{aligned}
E_{Total} = & \left[\left[\left(\frac{\partial X_3}{\partial X_2} + \frac{\partial X_3}{\partial K_3} + \frac{\partial X_3}{\partial L_3} + \frac{\partial X_3}{\partial V_3} + \frac{\partial X_3}{\partial T_3} \right) * \left(\frac{\partial X_2}{\partial X_1} + \frac{\partial X_2}{\partial K_2} + \frac{\partial X_2}{\partial L_2} + \frac{\partial X_2}{\partial V_2} + \frac{\partial X_2}{\partial F_2} + \frac{\partial X_2}{\partial T_2} \right) * \right. \right. \\
& \left. \left. \left(\frac{\partial X_1}{\partial D} + \frac{\partial X_1}{\partial K_1} + \frac{\partial X_1}{\partial L_1} + \frac{\partial X_1}{\partial V_1} + \frac{\partial X_1}{\partial F_1} + \frac{\partial X_1}{\partial T_1} \right) \right] * \frac{\partial E_{Total}}{\partial E_{SC1}} \right] + \\
& \left[\left(\frac{\partial X_3}{\partial X_2} + \frac{\partial X_3}{\partial K_3} + \frac{\partial X_3}{\partial L_3} + \frac{\partial X_3}{\partial V_3} + \frac{\partial X_3}{\partial T_3} \right) * \left(\frac{\partial X_2}{\partial X_1} + \frac{\partial X_2}{\partial K_2} + \frac{\partial X_2}{\partial L_2} + \frac{\partial X_2}{\partial V_2} + \frac{\partial X_2}{\partial F_2} + \frac{\partial X_2}{\partial T_2} \right) * \right. \\
& \left. \left(\frac{\partial X_1}{\partial D} + \frac{\partial X_1}{\partial K_1} + \frac{\partial X_1}{\partial L_1} + \frac{\partial X_1}{\partial V_1} + \frac{\partial X_1}{\partial F_1} + \frac{\partial X_1}{\partial T_1} \right) \right] * \frac{\partial E_{Total}}{\partial E_{SC2}} \right] + \\
& \left[\left(\frac{\partial X_3}{\partial X_2} + \frac{\partial X_3}{\partial K_3} + \frac{\partial X_3}{\partial L_3} + \frac{\partial X_3}{\partial V_3} + \frac{\partial X_3}{\partial T_3} \right) * \left(\frac{\partial X_2}{\partial X_1} + \frac{\partial X_2}{\partial K_2} + \frac{\partial X_2}{\partial L_2} + \frac{\partial X_2}{\partial V_2} + \frac{\partial X_2}{\partial F_2} + \frac{\partial X_2}{\partial T_2} \right) * \right. \\
& \left. \left(\frac{\partial X_1}{\partial D} + \frac{\partial X_1}{\partial K_1} + \frac{\partial X_1}{\partial L_1} + \frac{\partial X_1}{\partial V_1} + \frac{\partial X_1}{\partial F_1} + \frac{\partial X_1}{\partial T_1} \right) \right] * \frac{\partial E_{Total}}{\partial E_{SC3}} \right]
\end{aligned}$$

Equation 6. Effectiveness of Threat Against Target X

- Determine the commander's rating of importance for the subcomponents using the Analytical Hierarchy Process (AHP) [Ref. 56: pp. 32-34], see Figures 6-9. The AHP forces discipline in structuring the problem and allows the problem to be broken down into manageable parts. This process also allows for the integration of the various criteria in the decision process and helps identify the most important element of the decision. [Ref. 56: p. 34] In this case, AHP will establish a prioritized list of vulnerabilities, by asking the battlefield commander to choose the more important vulnerabilities from a series of vulnerability pairs. By asking the commander a series of "Which is more important?" questions, the AHP system can produce a ranked list of vulnerabilities respective of the desired outcome, see Figure 7. The commander can then perform a "What if?" analysis with the results.

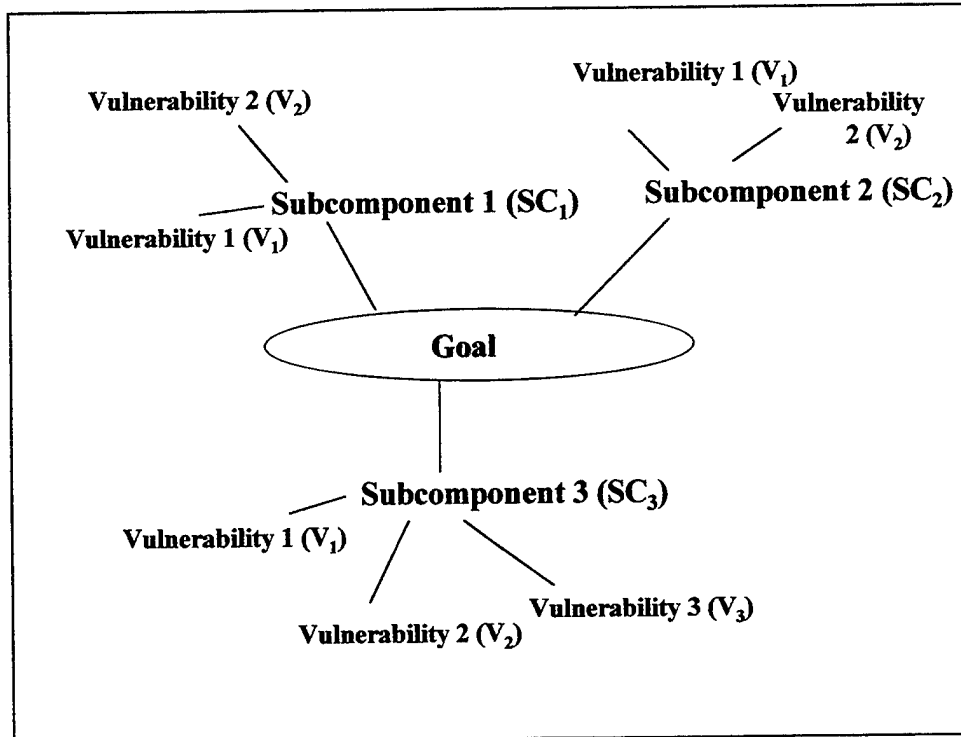


Figure 6. Pictorial Representation of AHP

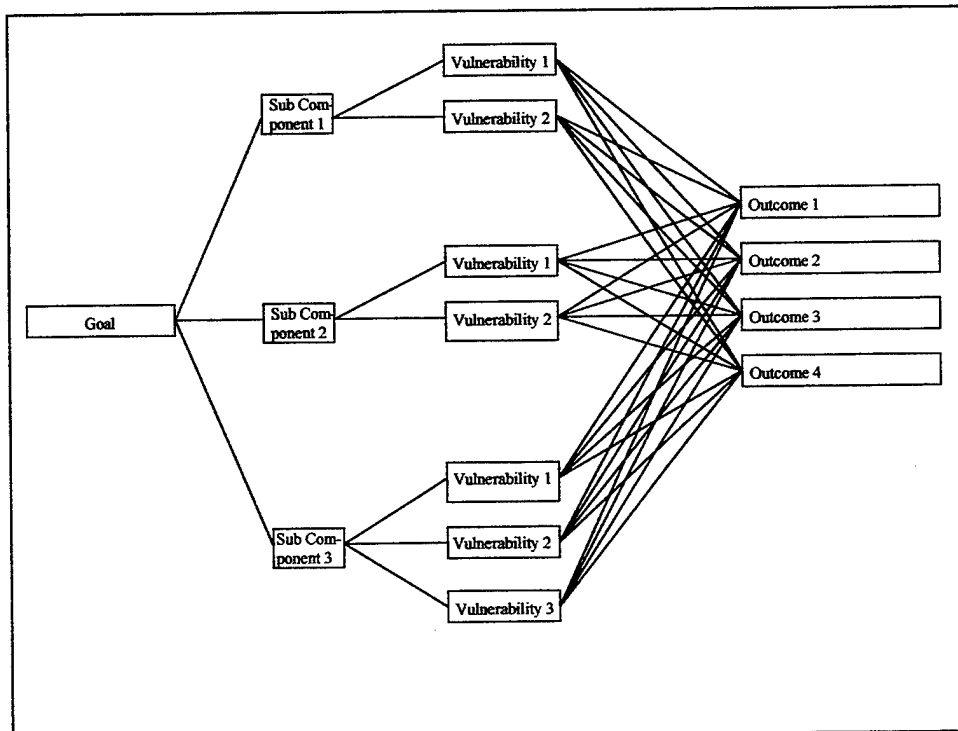


Figure 7. AHP Process

AHP Criterion Rating - Full Pairwise Method			
Method	View	Rules	Uncertainty
Criterion:	<input checked="" type="checkbox"/> Goal	<input type="checkbox"/> Next	<input type="checkbox"/> Notes
Descriptive Sentence			
With respect to Goal, on a scale measuring Preference and ranging from Absolutely Better to Equal, Vulner 1 rates Definitely Better than Vulner 2.			
Scale Information			
Units	Default	<input type="button" value="Assign Scale"/>	
Worst	1	Best	9
Subcriterion	Weights	Subcriterion	
Vulner 1	5	Vulner 2	<input type="button" value="↔"/>
	Definitely Better		<input type="button" value="↑"/>
Vulner 2	7	Vulner 3	<input type="button" value="↔"/>
	Very Strongly Better		<input type="button" value="↓"/>
Vulner 1	8	Vulner 3	<input type="button" value="↔"/>
	Critically Better		<input type="button" value="↓"/>
Consist. Ratio: 0.213		<input type="button" value="Restore Current Ratings"/>	
<input type="button" value="OK"/>	<input type="button" value="Cancel"/>	<input type="button" value="Information"/>	<input type="button" value="Help"/>

Figure 8. AHP Rating Process

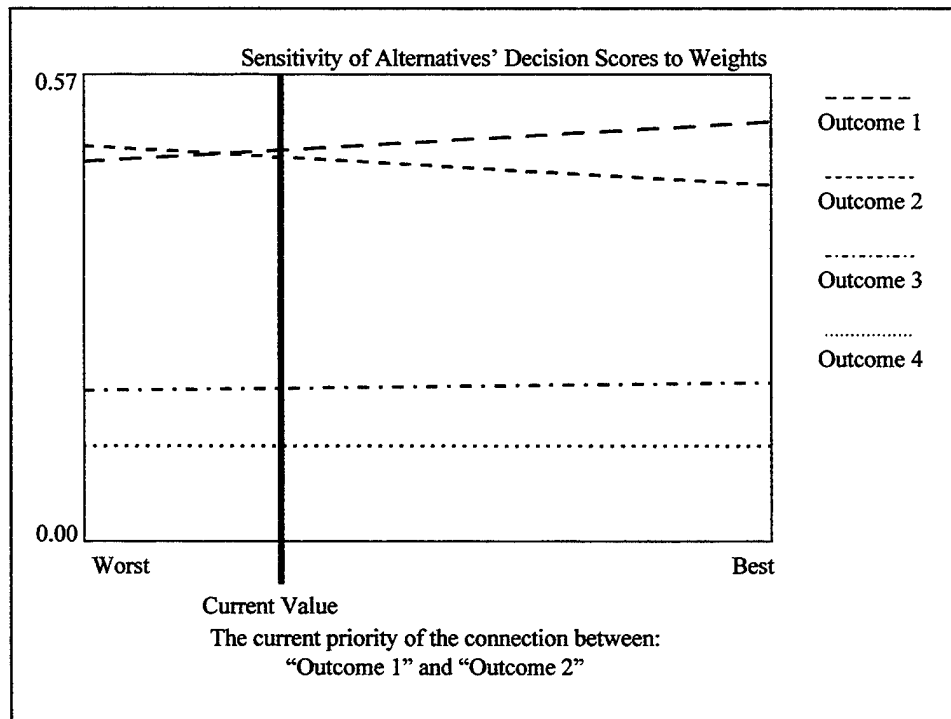


Figure 9. Sensitivity Analysis Chart

The Sensitivity Analysis in Figure 9 can assist the battlefield commander in determining the effects of exploiting the different vulnerabilities. By moving the current value line either left or right, the best option may change. For instance, moving the current value line to the left will show that outcome 2 becomes the best option based upon the priorities set during the AHP Rating Process, as depicted in Figure 8.

- Multiply the Importance Rating by the results of the incremental changes equation to obtain the Vulnerability Index for each subcomponent of the target. Then add these values together to obtain the Vulnerability of the Target, (E_{Total}), see Equation 6. This gives a relative value of the integrated target vulnerability. For example, after determining the effects of the changes on the various parts of the Command and Control system, the Value of the vulnerabilities within the Command and Control system is Y . The Importance Rating for the C2 system is .8. Therefore, the Vulnerability index for the Command and Control system is $.8 * Y$. After obtaining this value for each subcomponent of the target, then add the subcomponent values together to obtain the Vulnerability Index for the target.

8. Risk analysis.

Risk analysis is the process where the battlefield commander must determine how much risk he/she is prepared to take to achieve the objective. To accomplish this, several steps must be completed.

- Identify the risks associated with the application of each possible threat.
- Correlate the risks with the vulnerabilities.

- Use Analytical Hierarchy Process to help the battlefield commander to prioritize the risks, much the same as the process for the commander's rating of importance for each subcomponent, see step (f).

Determine which vulnerabilities have the most impact across the target as a whole (performed in the vulnerability analysis step) and the cost information (risk exposure) associated with each vulnerability being exploited. The best vulnerability to exploit may not have the highest impact because of the risk associated with it. The user (or assessor) must determine the most important criteria affecting the goal, then break each criteria into subcriteria, see Figure 10. Figure 11 depicts the criteria and subcriteria with the desired outcomes. Figure 12 allows the user (assessor) to determine the relative importance of the criteria and subcriteria. Figure 13 is the final product of risk analysis and indicates which vulnerability cluster(s) provide the most favorable balance of impact and cost (risk exposure), see Figures 10-13.

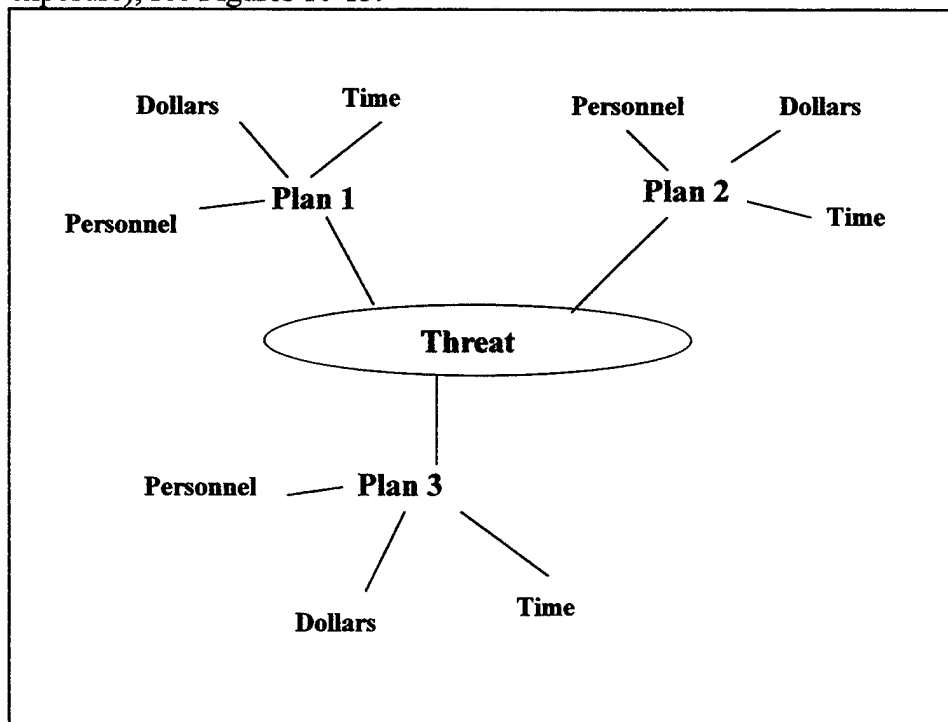


Figure 10. Risk Analysis

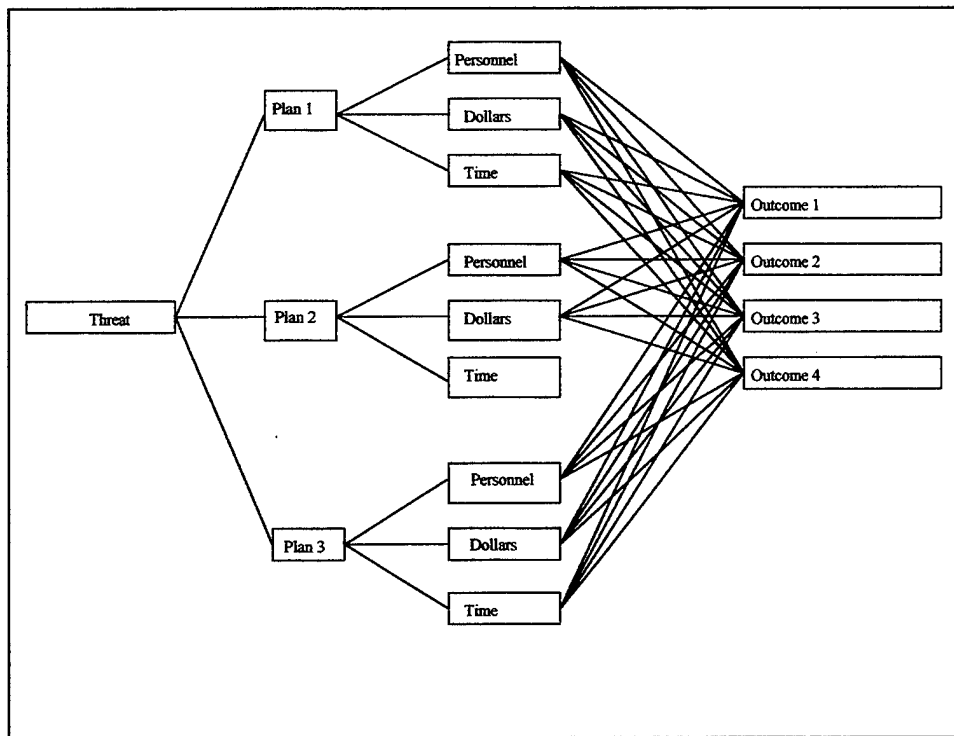


Figure 11. Risk Analysis AHP

AHP Criterion Rating - Full Pairwise Method					
Method	View	Rules	Uncertainty		
Criterion:	<input checked="" type="checkbox"/> Threat	<input type="button" value="Next"/>	<input type="button" value="Notes"/>		
Descriptive Sentence					
With respect to Threat, on a scale measuring Preference and ranging from Absolutely Better to Equal, Time rates Dollars.					
Scale Information					
Units	Default	<input type="button" value="Assign Scale"/>			
Worst	1	Best	9		
Subcriterion	Weights	Subcriterion			
Time	5	Dollars			
	Definitely Better				
Dollars	7	Personnel			
	Very Strongly Better				
Time	8	Personnel			
	Critically Better				
Consist. Ratio: 0.213			<input type="button" value="Restore Current Ratings"/>		
<input type="button" value="OK"/>	<input type="button" value="Cancel"/>	<input type="button" value="Information"/>	<input type="button" value="Help"/>		

Figure 12. AHP Rating Process

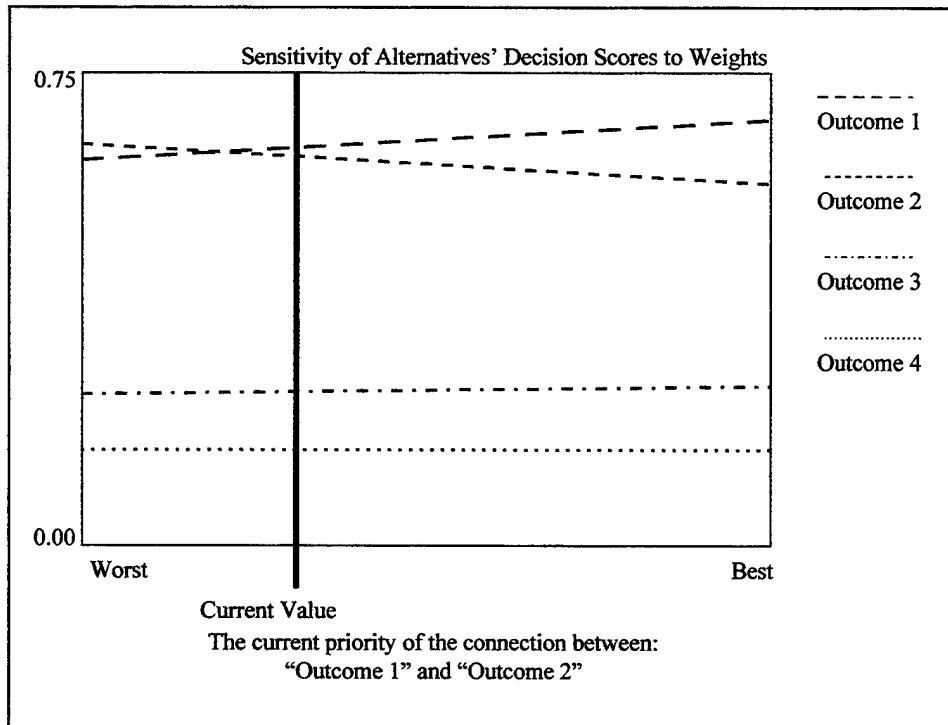


Figure 13. Sensitivity Analysis Chart

The user can perform a sensitivity analysis, depicting the effect on risk when the commander changes the mix of resources, see Figure 13. By moving the current value line to either side, the best option may change. For instance, moving the current value line to the left will show that outcome 2 becomes the best option based upon the priorities set during the AHP Rating Process, as depicted in Figure 12.

- Determine the probability of mission success. The person performing the assessment will determine the probability of the success of each option. To achieve this probability, the assessor must determine the probability of the threat occurring and the probability of the effect occurring, see Figure 14.

$$P(E / R) = P(E / T) * P(T / R)$$

Equation 7. Probability of Mission Success

$P(E / T)$ = Vulnerability Analysis (Probability of the Effect Occurring, given the threat) and

$P(T / R)$ = Risk Analysis (Probability of Threat Occurring, given the resources)

Equation 7 is the equation for determining the Probability of Mission Success. The two variables in this equation have already been calculated from Equation 6 and from the Sensitivity Analysis performed from Figure 13.

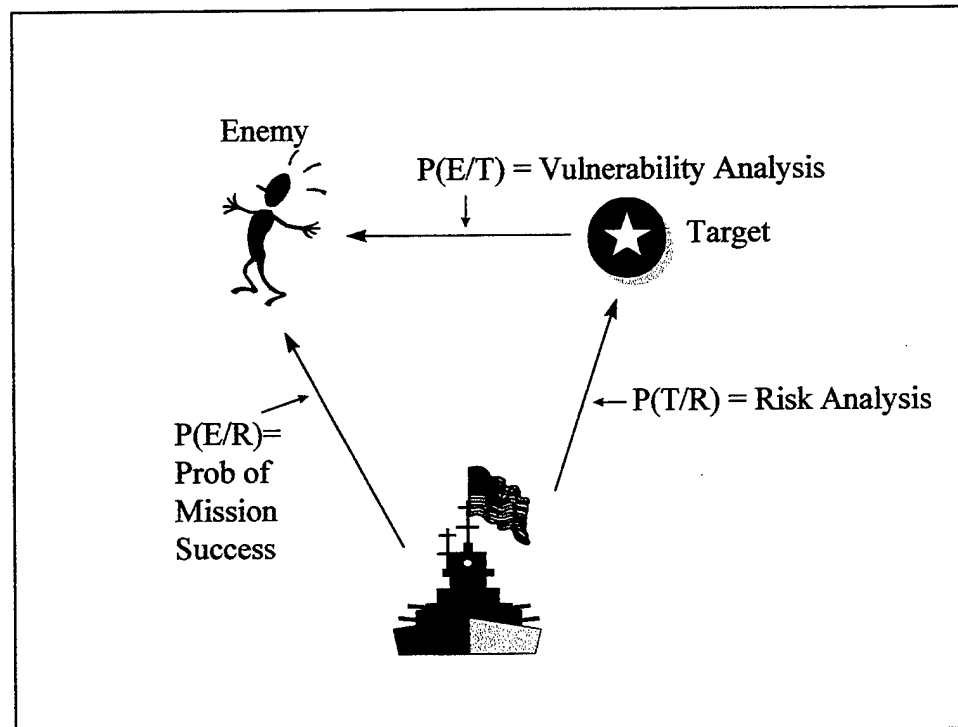


Figure 14. Probability of Mission Success Model

- Feedback loop. Providing feedback into the system improves the quality of information contained within the expert system. Therefore, the quality of the vulnerability assessments is enhanced as time progresses and as more feedback is provided.

This heuristic helps the user decide which vulnerabilities will have a greater impact on the target should exploitation or attack occur. Once the vulnerabilities to be exploited/attacked have been decided upon, the battlefield commander can use this knowledge to determine the combination of vulnerabilities and assets to use to achieve the desired effect. In essence, this heuristic gives the battlefield commander an idea of what IW tools to employ with respect to a given foe. As one of the tools of IW, the integrated use of the Five Pillars of C2W can now be more effectively incorporated into the battlefield planning, thanks to the wise use of Information Technology.

[THIS PAGE LEFT INTENTIONALLY BLANK]

IV. EXPERT SYSTEMS FOR INFORMATION WARFARE

Expert systems must be part of our vision of using a computer at the command post to assess the vulnerabilities of the adversary and friendly forces. The information content, accuracy, and speed required surpass the abilities of a human being performing the same tasks manually. Officer and/or Enlisted personnel at the battle scene may not have the depth and breadth of experience of the expert but will now have access to the experts' knowledge. In stressful situations, where personnel are required to respond as quickly as possible, expert systems enable the individual to ensure that all avenues are covered consistently, leaving no stone unturned (forgive the metaphor). For a more in-depth discussion of expert systems, see Appendix B.

A. EXPERT SYSTEMS FOR VULNERABILITY ASSESSMENT/VULNERABILITY ANALYSIS

The hardware and software required for an expert system is a computer (e.g., a PC or TACC-4) inference engine, an integrated database, appropriate software and a network interface. Figure 15 depicts the basic layout of an expert system and how the different components of the computer connect together. This gives the reader a visual representation of how the data will flow through the expert system. However, unless the computer is connected to an integrated database that is easily updated (whether it is located locally or remote), then the information contained within may not be optimal.

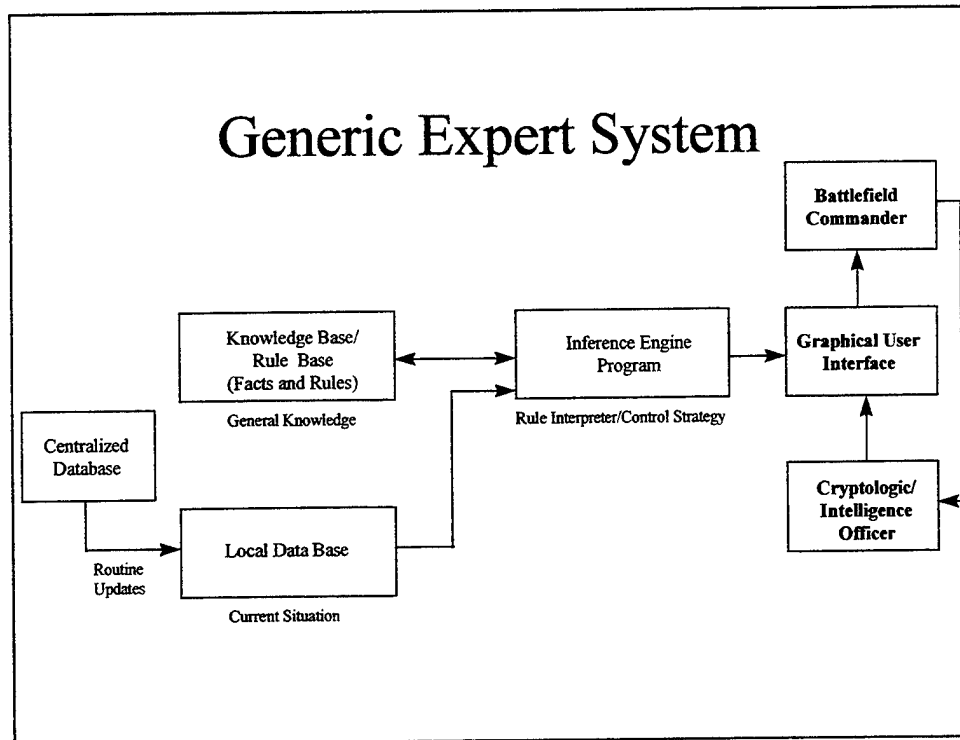


Figure 15. Generic Expert System Model

Without the availability of expert knowledge, decisions will be made based upon the information at the local command post or intelligence center (as they are now). The advantages of achieving the author's vision involving expert systems far outweigh the costs. Ensuring that all of the known details are included in an analysis enhances the decision-making process and thus the chance of success. Often, human beings in stressful situations forget details or ignore their own procedures. Expert systems ensure that this does not happen. The information is stored in the database, called upon when needed, and updated as events occur. The expert system ensures that the information is available on demand in a usable form and that decisions are accurate, regardless of the stress level.

The heuristic that the author has developed will be contained within the expert system. Experts, designated by central authority (the command so designated by the

military branch in charge of the network), or knowledge engineers will enter their knowledge into the central database via a global network. The information in the central database will be both historical and current and will be divided into topic areas such as country, command and control, and/or communications (or other divisions). The selected topic areas should conform to most, if not all, situations. However, in the event that a situation occurs that does not conform to these divisions, then the user and/or central authority must determine the pertinent topic areas.

The user will have access to the expert system at the command post, whether it is sea- or shore-based. The inference engine within an expert system is connected to the central database, see Figure 15 (Generic Expert System). The user enters the identified vulnerabilities into the expert system. The expert system then reviews the areas pertaining to the vulnerabilities, ensuring that all possible aspects of the target have been considered. For example, if the user does not include a vulnerability under the command and control area, the expert system would query the user to see if he/she had considered that particular vulnerability.

To assist in maintaining the currency of the information within the database, and therefore the effectiveness and credibility of the system, feedback on the validity of the information provided by the expert system will be sent to a central location for analysis by target specialists. After the objective is attained, the user should compile a lessons learned report to include the effectiveness of the rules, information, mission success, bomb damage assessment, etc., and submit it to the central authority, (e.g., Fleet Information Warfare Center (FIWC), for the Navy). Target specialists or experts will

review the report, evaluate it, and if warranted, modify the information in the central database.

The central authority is the command or organization designated by the military branch that owns the expert system network. This organization will basically oversee the global network with the ultimate authority and responsibility for the operational and other uses of the network. Included among the responsibilities are the determination of the identity of the experts and the performance of the maintenance functions of the global network, including the central database.

B. DECISION SUPPORT SYSTEMS FOR RISK ANALYSIS

Once the expert system has performed the vulnerability assessment, the commander must identify the risks associated with exploiting those vulnerabilities. Using a Decision Support System, the commander will have a pictorial representation of the different options. Sensitivity analysis is also an option to explore different combinations of the alternatives. The commander identifies the objective, the threats, vulnerabilities, and the desired outcomes. By placing more emphasis on a particular threat and/or vulnerability, the commander can influence the amount of risk associated with exploiting a particular vulnerability.

C. EXPERT SYSTEMS AND INTELLIGENT AGENTS FOR TRAINING

Training is equally as important as the mission. In order to provide a more robust system and save money, the same expert used to perform Vulnerability Analysis can also

support the training requirements for Information Warfare. This system will therefore greatly improve a sailor's performance. Learning what information has proven useful improves the quality of the future analyses and the quality of the information that is both input into the database and extracted from the expert system. Using training tools, such as expert systems and intelligent agents, to teach the concepts of Information Warfare, the "student's" understanding is assessed. Intelligent agents are a type of artificial intelligence software. The agent learns about the student's knowledge level as he/she progresses through the training material and can offer instruction and advice to help the student complete the task. [Ref. 57: pp. 97-104] If the student does not appear to fully understand the concepts, then the expert system/intelligent agent concentrates on the weak areas until the material is fully understood. In addition, many people learn more effectively by actually doing; therefore, having personnel actually practice identifying and assessing vulnerabilities improves knowledge retention and skills. Pilots have been using this method, with great success, for a very long time. Simulation is a great way to practice and hone skills at less cost than performing actual drills in an airplane. In having a dual-purpose system, i.e., meeting mission and training needs (simulation), the sailor will gain knowledge of both the required information and the actual computer system that will process that information.

D. EXAMPLE SCENARIO

To see how the proposed expert system can help in performing the Vulnerability Analysis, here is an example of how the expert system will play a part in future conflicts.

Nation A is experiencing a plague. Instead of requesting aid from the United Nations, Nation A decides to demand unrestricted access to a neighboring nation's (Nation B) medical knowledge and technology. However, because of inhumane practices against this same neighboring country (Nation B) and another neighboring country (Nation C) in a past war, the United Nations has placed trade sanctions against Nation A. Of course, Nation A has absolutely refused to place a request before the United Nations for assistance.

Instead, Nation A's government sends soldiers into Nation B to kidnap the president's wife and children. The soldiers have orders to hold these people until the required medical assistance is turned over to the designated representatives of Nation A's government, after which the soldiers are supposed to kill the hostages. Nation A has also amassed troops along the borders of Nation's B and C with orders to attack if the medical assistance is not delivered posthaste.

Of course, Nation's B and C believe that the troops will invade anyway, whether or not the medical assistance is delivered. In fact, they believe the reports of plague are highly exaggerated. Allies of both nations begin assessing the vulnerabilities of Nation A. One fact quickly becomes apparent. Nation A's militaristic society has poured massive amounts of money into its military infrastructure, but has totally ignored medical capabilities. The soldiers have been isolated from family and friends to prevent contagion, but some soldiers have contacted their families anyway. To date, only two soldiers have contracted the dreaded disease. Military leaders feel that force is the only way to obtain the necessary medical capability.

Allied forces are pressured by the United Nations to intervene. Allied sources discovered that Nation A's command and control communications network is highly sophisticated and has been operating for several years. Also known to the allied nations is that this country bought the system from international businesses, and the manufacturer resides and operates within the borders of an allied country. Thus, the allies prevail upon the manufacturer to identify any vulnerabilities on this particular system. Other sources were also consulted to obtain information regarding potential vulnerabilities of this system or similar systems. Previously completed vulnerability assessments completed on similar command and control systems have been obtained.

Following procedures developed some time ago for assessing vulnerabilities, a designated sailor performs a vulnerability assessment and risk analysis against Nation A. The officer looks at the Nation's IW attributes and divides it into component parts. For example, the officer discovers that the command and control communications network is a vital part of Nation A's military strategy and that the banking industry and the power grids are crucial to the country's social and economic infrastructure. Thus, they are vulnerabilities, perhaps even the center of gravity for this nation. The officer then divides the command and control communications network, the banking, and the power grid networks into their component parts.

Following the procedures contained within the manual given to him by headquarters and the expert system described in this paper (that automated those procedures), the sailor performing the vulnerability assessment determines that the system is vulnerable to attack or exploitation and proceeds to inform his superiors. The senior personnel begin developing a battle plan using the integrated use of the Five Pillars of

C2W and their knowledge of enemy's vulnerabilities to achieve their objective, isolating Nation A's leader from his command and control communications, the banking, and the power grid network. Other secondary objectives include degrading morale even more. The allies decided to drop leaflets and pamphlets over the citizens of Nation A, telling them that their leader and several key members of the government were sick and have fled the country to obtain medical assistance, leaving the citizens to the mercies of this fatal disease. Anti-radiation bombs are dropped over the capital city, denying the enemy the use of his command and control communications, banking, power grid network, a tactic that had been successful in a previous conflict. Computer viruses are transmitted over the internet to the main computer in the networks to ensure malfunction. Without communications, money and electricity, the inhabitants of Nation A surrender within 24 hours. Allied forces achieve their objective and the Red Cross enters the beleaguered country to deliver medical assistance, with minimal exposure of friendly forces to risk.

The example scenario above depicts how the heuristic in this paper can be used to develop a vulnerability assessment. To take this subject a step further, expert systems can apply this methodology much faster than humans can. In fact, expert systems lend themselves very easily to this procedural process. Automating this process can result in greater increases in efficiency and effectiveness, since expert systems can compute faster than humans and can ensure that important details are not overlooked.

Vulnerability assessments are not the only area of Information Warfare that will realize a benefit. Training can realize equal benefits. Equipping personnel with the knowledge and training necessary to perform duties to the best of their abilities is the job of today's leaders. In the civilian sector, expert systems are proving to be more effective

in computer-based training than many other methods, even classroom instruction. Being able to assess an individual's understanding of the fundamental concepts is a gigantic leap over today's training methods.

Imagine using expert systems not only to learn IW concepts, but also to apply them. Also imagine expert systems assisting in the decision-making process while assessing an adversary's vulnerabilities. For Information Warfare, the benefits that will accrue quickly in the quality of work, efficiency and effectiveness of personnel are substantial, especially if feedback on lessons learned are incorporated into the expert systems.

[THIS PAGE LEFT INTENTIONALLY BLANK]

V. IMPLEMENTATION ISSUES

Issues concerning the current technology, system requirements, and migration path are all critical to the successful implementation of any system. Is the current technology level sufficient to support the proposed plan? What are some of the system requirements to support this proposed plan? How does the military move from the design phase of the proposed system to the implementation of it? In the case of this research, the proposed plan is the implementation of a global network of expert systems supporting a centralized database, which in turn feeds information into an expert system being used at a command post. These questions and issues must be resolved before actual implementation in order to realize the full benefit of the system.

A. CURRENT TECHNOLOGY

The current technology level of the Navy is sufficient to support the implementation of a global network of expert systems. Existing expert systems, using more advanced technology than this proposed system, are prevalent in today's technologically advanced society. Appendix A discusses the wide variety of uses for which industry and the federal government employ expert systems. The United States military, mainly the Army, currently uses expert systems for a variety of purposes. Applications of these systems range from managing personnel matters at the Army's Personnel Command to the diagnosis of patients in the Medical Field to assisting senior officers in making decisions using Executive Decision Aids. The Army has invested a

large amount of money in researching and using expert systems. Perhaps the most promising area is in Maintenance. Army mechanics are responsible for a multitude of equipment. Since training personnel requires a huge outlay of resources, investing in expert systems can potentially realize cost savings in terms of decreased downtime for equipment, manpower costs, and training. Fault isolation is a big issue in the maintenance arena. A mechanic who is attempting to repair an unfamiliar piece of equipment consults the expert system. The expert system helps the mechanic identify the fault and gives the mechanic instructions on how to repair it. [Ref. 60: p. 63] The similarity between performing fault isolation analysis in maintenance and failure node analysis in Information Warfare/Vulnerability Analysis is striking. As a fault isolation routine decomposes a complicated mechanism to identify a fault, failure node analysis decomposes an enemy's force structure to isolate a critical vulnerability.

Another area in which expert systems are helping the Army is in Command and Control. Project Eagle is one of the Army's largest expert system projects. It is intended to be used as a "combat development tool for studying corps and division-level force effectiveness issues." [Ref. 59: p. 20] Basically Project Eagle analyzes the force structure effectiveness as it relates to the different systems such as command and control, weapons, and doctrine. In the Information Warfare/Vulnerability Analysis arena, a system like this can develop a decomposition of the enemy's forces and help identify the vulnerabilities.

From a training perspective, current technology has reached the point where advisory agents and expert systems can assess a student's level of understanding. This type of "insight" can help the teacher (human or computer) focus on areas that will increase the student's understanding and ultimately, the student's knowledge of the

subject. [Ref. 57: pp. 97-104] Using this kind of "intelligent" software can help sailors learn the fundamental concepts and uses of Information Warfare, and ultimately, how to perform Vulnerability Analyses. Additionally, simulators and expert systems have great potential in Information Warfare. Besides performing the operational mission, expert systems and simulators can teach the concepts of Information Warfare both from a theoretical and practical point of view. Whether in training or in an exercise to determine the potential outcome of different strategies, expert systems and simulators will be invaluable to the battlefield commander. As Vice Admiral Arthur K. Cebrowski stated,

"The military commander needs a real or near-real-time picture of the battlefield, and must be able to sort through hundreds or even thousands of scenarios, predict their outcome, and choose a course of action. At the same time, commanders must have the ability to distort the enemy's knowledge." [Ref. 60: p. 71]

Simulators and expert systems together can provide the battlefield commander and his staff with the opportunity to develop the appropriate courses of action in response to a given stimulus during non crisis times.

Thanks to military and civilian research efforts, the United States has achieved a high level of technology, which is certainly sufficient to support the vision of a global network of expert systems. As we speak, researchers are pursuing more advanced technology and uses for expert systems. With the wide variety of expert systems being used for military and civilian purposes and the subsequent positive results, more people

will realize the benefits to be accrued from capturing an expert's knowledge and using that knowledge to achieve the end goal, i.e., in a Information Warfare sense, exploiting an enemy's weaknesses.

B. SYSTEM REQUIREMENTS

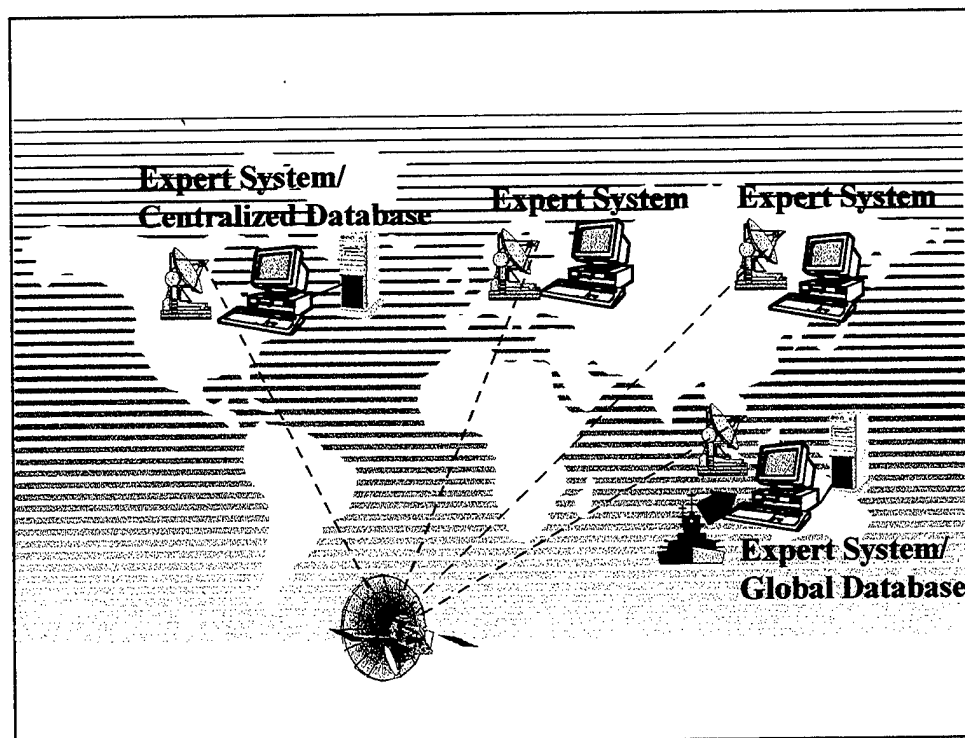


Figure 16. Global Network of Expert Systems

To support the dual requirements of expert system proposed in preceding chapters and depicted in Figure 16, (i.e., performing Vulnerability Analyses and training sailors to conduct them), the system requirements for an expert system are listed below. Speed of processing is a major consideration. Decisions must be made quickly; therefore, the processing speed must be faster than would be acceptable in a non-mission system. Also, non-proprietary hardware should be used to the maximum extent possible, which

will provide for more effective use of onboard maintenance resources. The requirements for the workstation are as follows:

Hardware - Workstation

- PC connection or TACC-4 connection to inference engine using windows-like graphical user interface (GUI)
- Support SVGA with resolution of 1024 x 768
- 2 GB hard disk capacity
- 32 MB RAM
- Pentium processor/200 MHz speed
- Local bus video
- Multi-media capability including Sound Card, Speakers, Digitized Voice, and Motion Video
- 6X-speed CD-ROM drive
- System must be "ruggedized" (portable)
- Non-proprietary hardware, replaceable by local shipboard computer parts inventory
- Backup capability (tape or zip drives)
- Uninterruptable Power Supply (UPS)

Hardware - Server

- Wide bandwidth capability to global network

- 128 MB RAM
- Large hard drive capability
- UPS
- Multiple drives
- Client-server software architecture
- Multi-processing capable

Software

- PC-based operating system
- Provide the decision-maker with enough quality information to make a single decision. Processing time for a single answer within 10-15 minutes.
- User-friendly Graphical User Interface (GUI), easy to understand presentation of data
- Step-by-step decision-making process for the user
- Allows forward-chaining, backward-chaining rules, object hierarchies, and LISP capable code

These requirements should result in an efficient, robust expert system, which can double as a training station. Therefore, instead of being used for performing only Vulnerability Analyses, the sailors can also train for Information Warfare. Realistic exercise scenarios could be used for training and/or educating the troops on Information Warfare.

C. MIGRATION PLAN

Before proceeding with a migration plan to develop and introduce the global network of expert systems, the military must decide what skills are necessary to support the operational use and maintenance of the system. Therefore, identifying the Core Competencies/Educational Skills Requirements is critical. The author's vision of the expert system performing Vulnerability Analyses for Information Warfare encompasses three areas: Information Warfare, Computer Science, and Information Technology. For the Naval Postgraduate School curricula, curriculum sponsors develop Educational Skills Requirements considered necessary for officers to operate in the increasingly complex technological world of today and tomorrow. These skills will help in realizing the vision of the expert system network by teaching military officers the basic knowledge required to operate and maintain such a network. The Educational Skills Requirements for Information Warfare, Information Technology, and Computer Science, listed in Appendix C, are the areas deemed necessary for the current and future success of a global network of expert systems.

These Educational Skills Requirements cover a broad area of knowledge that will support and maintain the operational use of the expert system network. The officer must understand the requirements of the battlefield commanders pertaining to Information Warfare and how to best employ technology to achieve the objective. Also, with more and more military systems becoming increasingly dependent on automation, understanding how the networks and computer systems interoperate is a necessity. As these requirements apply to the officers attending the Naval Postgraduate School, comparable requirements should be developed for the officers at the other military

graduate level educational institutions and for the technicians who will ultimately perform the myriad tasks involved in the use and upkeep of a system. The proposed expert system and simulation software will enable personnel to practice and apply the theoretical concepts and skills learned from the study of Information Warfare, Computer Science, and Information Technology. Establishing the criteria for training personnel is one of the first steps in planning for the implementation of a system.

Another area of concern in the migration plan is the delivery path of the core information. The operational information must be delivered and updated via the global network to each of the local commands because of the time sensitive nature of such information. However, a security concern such as interception or misrouting of the signal could give the enemy invaluable information about our Information Warfare training efforts. This concern might prohibit this transmission option for delivering the training information. Another method of delivery of the information which should be considered includes CD-ROMs. Using read-write CDs allows the local commands to develop more time-sensitive scenarios. If used on a wide basis, this storage medium would be the most cost effective means of delivering and storing training information. After the break-even point in creating the CD-ROMS, the cost of each successive CD-ROM rapidly decreases.

Security is another consideration. This option manifests itself in administrative concerns for classified storage and accountability issues, but the infrastructure supporting this classified delivery method of updates is already in place, i.e., by Sensitive Classified Information (SCI) channels. CD-ROMs may be mailed via secure mail to the local commands. Even with the administrative concerns, this method will work well for training, thereby leaving the transmission path free for operational use.

The maintenance necessary for the installation and upkeep for the proposed system can be provided by the current infrastructure. With minimal specific training on the expert system, the maintenance personnel could maintain the proposed system with relatively little effort. Some proprietary replacement parts will need to be placed in inventory, but as stated earlier, every effort will be made to design the envisioned expert system using non-proprietary equipment.

The key to a successful implementation of a system is to motivate people to actually use the system. Simulators not only give practical hands-on training to personnel, they can also make the learning process fun. With visually appealing screens and scenarios that have real world implications, personnel will be enticed to practice on the simulator. This practice not only provides the battlefield commander with trained personnel who have good situational awareness, but also with trained personnel who are intimately familiar with the expert system.

Resolving the issues surrounding implementation of a system in an expeditious manner can lay the groundwork for the successful use and good credibility of the system. Although the three areas addressed above are the primary issues during the implementation process, other smaller issues will arise during the actual implementation. The current technology is sufficient for both current and future use. Researchers are making great strides in the field of expert systems, and continued research should be encouraged and supported. The Educational Skills Requirements shape the future of Information Warfare, Computer Science, and Information Technology by determining what skills officers will need to solve future problems. As noted earlier, knowledge of expert systems and decision support systems has already been deemed necessary for

officers to learn. With the increased use of these systems throughout industry and government, knowledge of the capabilities of these systems become more and more important for Information Warfare officers. Finally, identifying and resolving the issues surrounding the implementation of an expert system network can assist in achieving a system that is highly credible and operationally useful. Planning and foresight in addressing the numerous issues involved in implementing a system can help in achieving a smooth migration plan and successful implementation. In short, keeping in mind the benefits to be realized from a global network of expert systems, the author believes that this vision can and should be achieved.

VI. CONCLUSIONS

A heuristic for conducting Vulnerability Assessments is invaluable for capturing the knowledge and experience of experts. Less experienced and knowledgeable personnel who do not have the expert's depth and breadth of professional expertise can benefit from the series of steps contained in the heuristic presented in this thesis. Since a heuristic is essentially a series of sequential procedures, it easily lends itself to encapsulation within an integrated expert system and decision support system. An opportunity for the military to expand into the realm of expert systems and decision support systems exists since relatively few examples of these systems performing Vulnerability Analyses abound. The United States Army is using expert systems to perform battlefield disposition and force composition requirements but not Vulnerability Analysis. The design of this network must also include a requirement for providing access to information on a global scale using a central database. The technology is available now and is making advances every day. This vision of a global network of integrated expert systems and decision support systems is attainable and can be successfully implemented and operated. This architecture will allow the information to be maintained and updated on a periodic basis throughout the day.

To provide for a more robust system, training should be conducted using the same expert system. With the Educational Skill Requirements (see Appendix C) already determined, the echelon command must develop the training plan to hone those skills. The Naval Postgraduate School as well as other educational institutions have developed curricula to satisfy the Educational Skills Requirements. Follow-on training at the command level using the expert system can assist in fine-tuning those skills. By providing

training using intelligent agents with the expert system and modeling and/or simulation techniques, officers and enlisted alike will be able to obtain and/or hone their knowledge of Information Warfare concepts and increase their knowledge with a practical application of those concepts. Using the same expert system and decision support system that conducts the Vulnerability Assessments provides a dual benefit of system familiarization for the users and more efficient use of resources for mission and training requirements.

By using the expert system and decision support system, the subsequent improvement in quality and timely receipt of information will help the battlefield commanders to take decisive action with the most accurate information possible in this technologically advanced society. Not only will the operational information be enhanced, but the training information will be more up-to-date and pertinent to the current mission. In short, due to the benefits to be gained from the implementation of a global network of expert systems, further research should be strongly encouraged and sponsored.

The heuristic contained within this thesis holds true for Vulnerability Assessments conducted on a wide variety of targets, ranging from cruise missiles to satellite systems. Although developed mainly from an offensive point of view, the heuristic also holds true for defensive operations. For further reading on a Vulnerability Assessment conducted from a defensive point of view, consult Charles Dunlap's "How We Lost the High-Tech War of 2007." [Ref. 61: p. 22]

A. LESSONS LEARNED

The author encountered only a few problems during the course of the thesis process. The greatest challenge involved locating personnel who have actually conducted Vulnerability Assessments. Extracting a heuristic from a body of literature is a starting point, but interviews with personnel experienced in Information Warfare is necessary to validate the process and discover anomalies. Another problem encountered involved selecting a presentation format for the wealth of vulnerability data. For example, some people work better with graphs and charts, while others work better with text. The author used a combination of both graphs and text in developing the Vulnerability Assessment procedure.

During the course of the whole thesis process, the author discovered a few “lessons” that might prove beneficial to others. These lessons include:

- Periodically reevaluate the thesis outline. This outline is the basis for the whole thesis, and it changes as the research progresses. Otherwise, the student will research on subjects that will later prove to be useless in writing the thesis.
- Developing good sources early in the thesis process is a necessity. The DTIC database provided invaluable documents on previous Vulnerability Assessments.
- Find another student that is willing to read the thesis while it is being written for grammar, spelling, and clarity. This allows the thesis advisor to spend more time on content (intellectual contribution).

B. RECOMMENDATIONS FOR FUTURE RESEARCH

With the possibility of using expert and decision support systems to conduct Vulnerability Assessments explored, other areas become available for research. The impact tables contained in Appendix A contain information provided from a cursory examination of literature. To fully determine what variables in today's society actually impact the enemy and how much effect the variable will have on the enemy, further research is necessary and encouraged.

Another potential area for further research is in performing a decomposition of enemy forces and failure node analysis. Developing a heuristic for these processes is also necessary to help non-experts determine the effects of exploiting an enemy or friendly forces' vulnerabilities.

Developing the requirements for a global network of expert systems and the resulting architecture is yet another area in which research should delve. For the whole vision of a group of experts updating a central database to work, the architecture, the requirements, and a feasibility study should be completed.

A fourth area ripe for more in-depth research is developing a prototype expert system to conduct the Vulnerability Assessment. Once a prototype is available, people will be able to see and experience the value of allowing an expert system to conduct the Vulnerability Assessment. Further research in all of these areas is a must.

APPENDIX A. IMPACT ASSESSMENT TABLES [Ref. 51]

Virus

Type Virus	Virus Name	Virus Effect	Virus Impact (assigned by decision-maker)
Boot Infectors	AntiCMOS (Lenart)	Blanks CMOS/BIOS values.	
	AntiEXE (Newbug)	Overwrites MBR.	
	Da' Boys	Overwrites the DOS 5.0 Boot Sector.	
	ExeBug	Makes small changes to MBR. Changes computer's CMOS.	
	Form	Memory resident. Does not infect files. Moves original boot sector.	
	Joshi	Memory resident. No damage to system.	
	Leandro and Kelly	Memory resident. Changes MBR.	
	LeHigh	Infects COMMAND.COM. Causes denial of service.	
	Michelangelo	Reformats hard drive on March 6	
	Monkey	Encrypts the Partition table. Memory	
	No_Int	Memory resident stealth virus.	
	NYB (alias B1)	Memory resident stealth virus.	
	Ripper	Encrypting, memory resident stealth virus. Relocates original boot sector and infects	
	Sampo	Memory resident. Works with Kampana to infect floppy disks. Does not corrupt saved files on system.	
	Stealth_C	Memory resident stealth virus. Moves original boot sector.	
	Stoned	Causes damage to directories or File Allocation Table. Moves original boot	
	V-Sign	Memory resident. Polymorphic. Problems booting system and accessing hard/floppy drives.	
	WelcomB	Memory resident stealth virus. Redirects calls to original MBR.	

Type Virus	Virus Name	Virus Effect	Virus Impact (assigned by decision-maker)
File Infectors	Cascade	Memory resident, parasitic, encrypting virus. Targets .COM files. Characters on screen fall down into a heap on the bottom	
	Die Hard 2	Symbiotic, memory resident that uses stealth techniques. Infects .COM and .EXE	
	Haifa	Memory resident, parasitic, encrypting virus. Infects .COM and .EXE files. Attaches to .ASM, .DOC, .PAS, and .TXT files in benign fashion.	
	Little_Red.A	Parasitic, stealth, memory resident virus. Infects COMMAND.COM. Targets .COM and .EXE files.	
	Predator	Parasitic, stealth, memory resident virus. Infects .COM files. Destructive. Randomly alters bytes in read buffers.	
Multi-Partite (both Boot and File Infectors)	Junkie	Memory resident, encrypting virus. Targets .COM files, DOS boot sector on floppies, and MBR.	
	Natas	Memory resident stealth virus. Infects system hard disk's MBR, diskette Boot Sectors, .COM, .EXE, and overlay files.	
	One Half	Memory resident, encrypting virus. Targets .COM files, DOS boot sector on floppies, and MBR (sector containing partition table).	

Technology [Ref. 52]

Technology Type	Priority	Technology Effect	Related Technologies	Impact (assigned by decision-maker)
Invisible Soldier Image Avoidance and Signature Reduction	Priority 1 Force Protection	Makes soldier invisible day or night, to whole range of battlefield sensors across electromagnetic	Active camouflage technology, active thermoelectric ribbons, IR sensors, microprocessors, enhanced light weight power sources, heat dissipation, and radar absorptive materials.	
Mine, Booby Trap & Explosives Detection and Neutralization		Protect personnel, equipment, facilities and vehicles by detecting and neutralizing explosives from a distance, without to enter danger areas where detection and simultaneous explosion are unacceptable.	Robotics, unmanned vehicles, fiber optics, display devices, air sampling, chemical trace detection, imaging technology capable of seeing through structures, magnetic, IR, acoustic and radar anomaly detection.	
Tactical Detection Weapons of Mass Destruction (WMD)	Priority 1 Force Enhancements	Stand-off means for small tactical units operating in non-permissive environments to detect location or assembly of nuclear weapons and chemical/biological agents to be used as weapons.	Nuclear radiation detection, air sampling, IR and radar photography.	
Advance Night Vision (NV) Equipment		Provide military forces/law enforcement with long-range night vision equipment allowing exploitation of full range weapons systems and equipment. Includes equipment for snipers and crews of aircraft, vehicles, and crew-served weapons.	Light-weight power sources, solar batteries and charging systems, optics, IR, lasers, and light amplification.	

Technology Type	Priority	Technology Effect	Related Technologies	Impact (assigned by decision-maker)
Mission Kill (Area and Point)		Precision or area weapons systems that will prevent enemy from carrying out intended mission by disabling person, equipment, or weapon with minimal or no collateral damage or casualties.	Non-nuclear EMP, directed energy weapons, lasers, high-power microwave, infra sounds, isotropic radiators, calmative agents, and carbon fiber conductors.	
Non-lethal Weapons		Temporary neutralization of enemy with no long-term debilitating effects and minimum casualties. Lasts at least 5 min. Used in crowds with combatants/non-combatants. Delivery via guided weapons, light, sound, gases, or aerosols.	Directed, variable strength energy weapons, non-lethal gases, acoustic research, non-nuclear EMP, super caustics, aerosol nets, adhesives, lubricants, aerosol dyes, intense light (strobe flash), and irritants.	
Low-Signature Unmanned Aerial Vehicles (UAV)	Priority 1 Command, Control, Communications, Computers, and Intelligence (C4I)	Not necessarily transparent to electromagnetic spectrum, but has reduced visual, audio and electromagnetic characteristics that will reduce probability of detection and attack.	Low- or non-reflective radar materials, propulsion systems, noise abatement technologies, aircraft and glider construction, battery technology, solar power technology, and advanced camouflage.	
Common Language Voice Recognition		Translates English language voice conversation into foreign language voice (and vice-versa). Developed on basis of likelihood of U.S. involvement in areas where languages are spoken.	Speech recognition, speech understanding, speech synthesis, speech-to-speech translation, and dialogue management.	

Technology Type	Priority	Technology Effect	Related Technologies	Impact (assigned by decision-maker)
Reduced Visibility Penetrator Aircraft	Priority 1 Force Projection & Sustainment	Application of reduced visual and radar visibility and reduced sound technologies to penetrator aircraft that insert/retrieve troops and equipment in denied areas. Present minimal or no signature.	Absorptive materials, noise abatement technologies, quiet rotor blades, propulsion systems, and radar non-reflective	
Anti-Mortar (Light Indirect Fire) Capability	Priority 2 Force Protection	Provides for detection and precise location of hostile indirect fire weapons (principally mortars) in time to warn friendly forces and engage weapon with precision weapons. Optimally include capability of neutralizing rounds before impact.	RF detection devices, radar, acoustic sensors, high-speed computers, and airborne (UAV) sensors.	
Extremities Protection		Develop individual protective armor for human body extremities coupled with existing body armor to protect soldier from injuries (shell fragments, small-arms fire) while allowing full mobility without degradation of combat capability.	Body armor development, camouflage technology, textiles, multi-spectral camouflage, heat venting and transfer.	
Anti-sniper System		Immediately identify source/nature of small-arms fire at friendly target and immediately direct lethal or non-lethal weapons or passive sensory devices to source. Mounted on vehicles, helicopters, on buildings, on ground, or hand-carried.	Acoustic sensors, IR sensors, microprocessors, laser target designators, and aim point designators.	

Technology Type	Priority	Technology Effect	Related Technologies	Impact (assigned by decision-maker)
Detection and Destruction of	Priority 2 Force Enhancements	Detect, identify, and characterize underground tunnels/cavities of significant size in permissive/denied areas for size, depth, use and estimated protective hardness. Map/locate vulnerable points (entrances/ vents) with precision (100-500 ft).	Radar technology, seismology, solid state imaging arrays, acoustic sensor technology, digital signal processing, image processing, ultra wide band, high-power signal generations, Geology, mining, and magnetic anomaly detection.	
Non-intrusive Drug Detection		Identify presence of illicit drugs, (primarily cocaine and heroin) in various preparatory and final states, with- out being in proximity.	Radar, chemical spectrum analysis, gaseous and nuclear diffusion analysis, and air sampling technologies.	
Room Monitor	Priority 2 C4I	Monitor activities occurring in a room without accessing room's outer walls or room proper to emplace devices or sensors. Operates from stand-off distance. Transportable and operable from light vehicle or person. Multiple power sources.	Radar, IR, heat, metal, and movement detection, power technologies, photography, micro-seismic	
Chemical/Biological Expert System		Immediately identify chemical/biological agent encountered. Provides critical information on agent's identity, immediate protective measures, appropriate antidotes, and handling instructions.	Database technology, chemical/biological weapons/detection, data transmission, micro processing, artificial intelligence, automated analysis, low probability of detection communications.	

Technology Type	Priority	Technology Effect	Related Technologies	Impact (assigned by decision-maker)
Virtual Reality Modeling and Simulations for Training, Planning and Rehearsals		Project variety of realistic OOTW operational environments. Ranges from projection of information in great detail (micro-environments faced by individuals/small units) to complex environments.	Computer graphics, modeling, and simulations.	
Survival Tag and Tracking System	Priority 2 Force Projection & Sustainment	Permits remote tracking of individuals, vehicles, or equipment. Undetectable to captors. Provides positive location and readable from high-altitude aircraft or satellites and from hand-carried monitors (3-5 km).	Global Positioning System, space-based positioning tracking system, microprocessors, biochemical tracers, mini-power sources, and electronic tags.	
Combat Search and Rescue (CSAR) Command and Control (C2) System		Tagging system or emergency communications system for downed pilots, special operations forces, or other military personnel at high risk of capture. Provides immediate and precise location, security status, and physical condition.	Global Positioning System, data processing, secure communications, world-wide telecommunications	
Biological-Medical Treatment Capability	Priority 3 Force Protection	Remotely monitor soldier's health (location/extent of injuries). Provide remote treatment/sustain life support during evacuation and expert medical assist from CONUS. Train surgeons on battlefield	Remote sensing and monitoring, geolocation and positioning, robotics and tele-presence, virtual reality and computer simulation, broad bandwidth communications, and high-performance computing and	

Technology Type	Priority	Technology Effect	Related Technologies	Impact (assigned by decision-maker)
Biological-Medical Treatment Capability cont.		casualties with advanced simulation and virtual reality models.	communications.	
Stand-off Precision Breaching Weapons (Squad/Team)	Priority 3 Force Enhancements	Person-portable weapons to penetrate walls/bunkers. Accuracy to within 1 meter square from beyond 500 meters. Future improvements include optically aided eyesight and implanted sensors/designators.	Laser designation, rocketry, EMP, explosive's technology, and radar.	
Stand-off Neutralization of Weapons of Mass		Ability to render WMD unusable or ineffective from a distance.	Bacteriology, chemistry, rocketry, nuclear physics, and high-voltage	
See-through Capability for Buildings and Structures	Priority 3 C4I	Determine content and positioning of people, furniture, and equipment in structures without penetration or access to walls, roofs, etc. Optimally, real-time video of persons and items inside building.	X-ray and millimeter wavelength.	
Strategic/Discriminating Remote Sensors		Emplaced by air, artillery, or ground. Interchangeable sensors used in multiple configurations. Includes IR imagery, seismic, audio, electronic emission, compressed imaging, low-light TV, neutron and other nuclear detection system.	Multi-media sensors, long-life power sources, LPI, spread spectrum (Morse) comms, interactive display consoles (receive, record, direct sensor activity, multi-spectral camouflage (concealment), and space-based or airborne communications relay.	
Universal Long-Life/Light-Weight Power	Priority 3 Force Projection & Sustainment	Individual power source to provide power to various types of equipment (radios,	Batteries, miniaturization, solar power (chemical photo voltaic), electrical	

Technology Type	Priority	Technology Effect	Related Technologies	Impact (assigned by decision-maker)
Universal Long-Life/Light- Weight Power cont.		position/navigation, mini-computer) within wide range of terrain and climatic medical conditions.	generation, electrical insulation, and human engineering and	
Strategic Airlift		All-weather, low-cost strategic airlift platforms requiring minimum fixed-forward, based to rapidly transport multi-purpose vehicles.	Composite tech, STOL, heavy-lift/specially designed helos, aerial refueling, navigation/defensive electronic equip, serial port tech, radar, IR, night vision, satellite/other comms, navig/posit devices locating devices, aerial/land/sea sensor.	
Floating Sea Base Capability		Receives intra-theater airlift sealift. Tailored for specific operations to preclude/minimize US presence on-shore. Sustain all-weather support of on-shore operations, receive replenishment by air/sea. Relocatable within 90 days.	STOL, heavy-lift rotary/fixed wing aircraft, Sea Delivery Vehicle, deep submersible recovery vehicles, amphibious/maritime tech (incl. offshore habitats/hydrospace platforms), materiel handling, load-master simulation model	

Geopolitics [Ref. 53]

Action	Type	Effect	Impact (assigned by decision-maker)
Government	Democratic	Free speech, free market economy	
	Democratic Isolationist	Poor economy	
	Democratic Participative (United Nations)	Deterrence and containment, sanctions, keep peace	
	Communist	No free speech, money on military power	
	Socialist	No free speech, money on military power	
	Fascist	No free speech, money on military power	
	Totalitarian	No free speech, money on military power	
Change in Government	Dictatorship	No free speech, money on military power	
	Coup	Military enforcement	
Climate	Election (popular support)	Generally peaceful	
	War (Mission of troops)	Destroy/Neutralize enemy	
	Peace	Peacekeepers/Peacemakers	
Expansion of NATO		International community take action or impose peace	

Economics [Ref. 54]

Type	Effect	Impact (assigned by decision-maker)
Interest Rates	Adjusts for inflation.	
Shrinking Deficit	Spending cuts (Defense).	
Value of dollar	Can indicate inflation.	
Inflation	Weakens currency's buying	
Industry Prices	Affects prices on defense	
Imports	Can affect prices on equipment parts included in Defense budget.	

[THIS PAGE LEFT INTENTIONALLY BLANK]

APPENDIX B. EXPERT SYSTEMS

This appendix contains a brief discussion on expert systems. Included in the discussion is the definition, the components, and the value added of expert systems. Also included are examples of how this technology is being used in the civilian sector.

The field of expert systems, in particular, deals with modeling the knowledge of experts. An expert system is a group of rules that outline a reasoning process which can draw deductions, producing new information, and modifying rules if necessary. [Ref. 62: p. 68] Basically, the knowledge consists of facts and heuristics. The "facts" constitutes a body of information that is widely shared and publicly available from experts in the field. The "heuristics" are mostly private rules of good judgment that are characteristic of the decision-making process of experts. [Ref. 63: p. 5] With expert systems, the computer is programmed with a group of rules in such a way that it can draw deductions or provide an outcome based upon a given set of circumstances. The expert system works using the basic components contained in Figure 17.

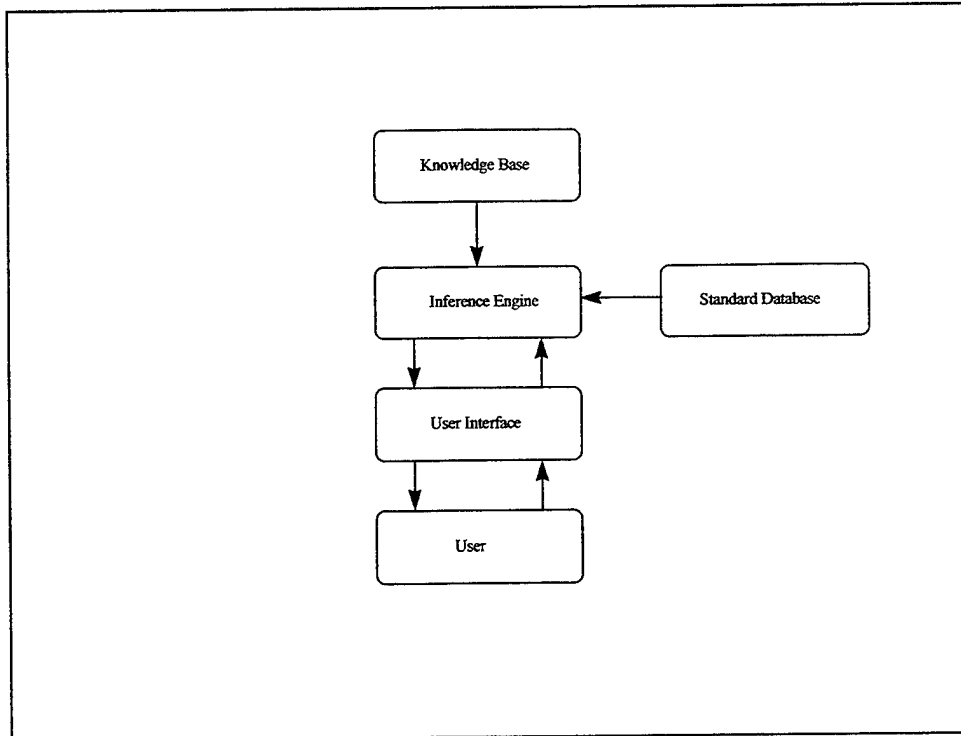


Figure 17. Expert System Components

An Inference Engine integrates the input data, the goals specified by the user, and information from the standard database with the expert knowledge contained within the knowledge base. A person can see that this technology may be applied in two different ways. The first way is to provide decision support, reminding the expert of options he or she may have forgotten. The other application is in decision-making, so that in the absence of a scarce resource (i.e., an expert), a less qualified or even unqualified person can make a decision beyond his or her level of expertise. [Ref. 64: p. 1]

The primary goal of an expert system is to improve the quality of decision-making. The computer can accomplish this goal by performing some of the complex or laborious tasks usually done by people. The time-consuming and sometimes tedious job of scheduling work on a manufacturing plant floor, analyzing business trends, or even diagnosing an illness are some examples of tasks that expert systems are currently

handling in several civilian industrial fields. In short, by taking the knowledge of an expert in a given field and encapsulating that knowledge as a group of facts and heuristics for the computer, less experienced people can invoke the same level of knowledge as an expert.

An organization would use expert system technology in cases where human experts are in high demand and short supply. Expert systems provide a measure of permanence and can repeat mundane decisions faithfully, allowing the human being to focus on his/her strong points – spontaneous thought or adding to the knowledge base. Once this knowledge is in the memory banks, the computer does not forget and can actually “learn” from the new information. Therefore, reproducibility is another key advantage. Also, computers are not as expensive as training human experts, since the computer cannot “walk” out the door once the knowledge is learned. The third factor is consistency, whereby similar transactions are handled in the same manner. Permanent documentation of the decision process is the fourth factor. Depth is the last benefit. Combining the knowledge of many experts provides more depth of knowledge than one person could ever hope to amass. Expert systems can also be designed with feedback mechanisms to expand their own knowledge base, increasing the amount of expert knowledge available. These are just a few of the many advantages realized by employing expert systems. [Ref. 65: p. 11]

As with any technology, disadvantages accompany advantages. Expert systems can not duplicate that critical human capacity of common sense. Therefore it is important that expert systems be viewed as one tool in the decision maker’s arsenal. Creativity is another area in which expert systems are deficient. If the rules applying to

situations are not present in the knowledge base, the expert system can deduce them but cannot perform spontaneous association or subjective cross-referencing, i.e., one person mentions a word or phrase and it reminds another person of a childhood memory. The rules in expert systems must be continually updated. Also, human beings have a variety of senses to assist in making decisions. Expert systems rely solely on the user's input, the coded heuristic, and knowledge contained in the knowledge base. [Ref. 65: p. 11] In short, as long as a human being interfaces with the computer or machine, even with the disadvantages, expert systems can provide a valuable added dimension to the decision-making process.

Expert systems are prevalent in the civilian sector, with approximately seventy percent of the top 500 companies in the United States using expert systems. [Ref. 62: p. 68] Industries such as manufacturing are using these systems for scheduling work on the plant floor. [Ref. 62: p. 68] During the 1988 Olympics, police schedules and paychecks in Lillehammer, Norway were generated by knowledge-based systems. [Ref. 66: p. 72] Within the field of medicine, expert systems help prevent adverse interactions among drugs prescribed to patients, check 50 million electrocardiograms per year, and diagnose illnesses based upon symptoms and patient information. [Ref. 62: p. 71] The financial industry is using expert systems to detect and stop credit-card fraud. During the last 18 months, these applications of expert systems have prevented the loss of fifty million dollars by spotting anomalies in the purchasing patterns of customers. [Ref. 62: p. 70] Within the engineering industry, expert systems embedded within Computer Assisted Design systems help the user analyze and optimize the design. [Ref. 67: p. 18] These are just a few of the civilian areas in which expert systems are flourishing.

Products and practices which perform well within the civilian industries often end up being used in the government, and expert systems are no exception. Screening welfare recipients and assisting U.S. Customs agents to identify illegal cargo are two of the ways in which expert systems are being used. [Ref. 62: p. 70] The military is researching the use of expert systems in limited cases. Currently undergoing evaluation at Fleet Training Center San Diego is the MK92 Fire Control System Maintenance Advisor Expert System, which is designed to help the maintenance technicians in repairing the MK92 Fire Control System. Optimizing maneuvers in aerial combat is another area in which research is ongoing.

With this technology becoming prevalent in today's business and government, education has been a logical expansion. Researchers are investigating the use of advisory agent software, which is an integration of artificial intelligence principles and embedded knowledge. In short, it is expert system technology. This type of software offers instruction and advice to help someone complete a task. At the first use of this software, the agent's knowledge is very basic, but the more often the software is used, the expert system adds to its knowledge base, and the more it learns about the user and how to best assist the person. Most software use wizards to assist the user. This intelligent agent software, named "Coach", will be able to build and maintain information about a user's proficiency, the mistakes made and what method the user chose to correct the mistake, and in terms of "coaching", what worked and did not work. An added benefit is that the "Coach" can be made available to the teacher to assist in understanding where a student might be having difficulty. [Ref. 57: p. 98] Software companies are beginning to use this kind of technology to improve user support and user satisfaction. As a matter of fact,

Microsoft® is planning to use expert systems technology in the self-help portion of future releases of its Windows software. [Ref. 66: p. 72]

Expert systems are working successfully in many areas of industry. The military has invested money in developing a limited number of expert systems for operational use. As the success of these experts systems becomes widely known, more people will be willing to invest in and use them. The underlying premise of expert systems is that now less experienced personnel can have access to and use the knowledge of experts, benefiting everyone.

APPENDIX C. EDUCATIONAL SKILLS REQUIREMENTS

A. INFORMATION WARFARE (Curriculum 595, subspecialty code XX46P)

- The officer will have an in-depth understanding of IW/C2W and the disciplines needed to support them.
- The officer will have in-depth understanding of the capabilities, limitations, design and operation of communications, computers and information networks.
- The officer will have a systems level understanding of information systems and their vulnerabilities as well as capabilities.
- The officer will understand the organizational decision process, as well as the structure and other processes of organizations with emphasis on their vulnerabilities and capabilities.
- The officer will understand the concepts, principles, methods and capabilities of joint operational intelligence, with emphasis on the operational requirements levied upon the intelligence community to support IW/C2W.
- The officer will understand the integration of IW as a weapon and its role in modern warfare; understand the integral roles of EW, psychological operations, military deception, OPSEC, and physical destruction; understand INFOSEC and nodal attack in this warfare area; employ real-time intelligence, tactics and EW systems; understand the physical principles of generation, transmission, propagation, reception, processing and suppression of detection and surveillance information.
- The officer will demonstrate the ability to conduct independent analysis in IW/C2W and proficiency in presenting the results in writing and orally by means of a thesis and command oriented briefings.
- The officer will have an understanding of the American and world military history and joint maritime planning including the origins and evolution of national and allied strategy. [Ref. 68]

B. COMPUTER SCIENCE (Curriculum 368, subspecialty code XX91P)

- The officer will have a thorough knowledge of software engineering to include:
 - An understanding of the software development process, including specification of requirements, design, implementation, testing and maintenance. Military real time software projects, such as control software for a ship's boiler. Design on systems that emulate requirements in real time embedded systems used by DOD.
 - The ability to plan and implement a major programming project and develop the appropriate documentation.
 - The ability to incorporate modern software engineering techniques in Ada based systems.
- The officer must have a thorough knowledge of software technology to include:
 - The formal definition of programming languages covering specifications of syntax and semantics, properties of block structured languages, programming techniques and evaluation of languages.
 - The relations that hold among the elements of data involved in problems, the structure of storage media and machines, the methods useful in representing structured data in storage, and techniques of operating upon data structures.
 - Operating systems used in various environments relative to addressing techniques, memory management, file system design and management, system accountability and security, all built around DOD ADP security instructions.
 - The techniques used in the design and implementation of programming languages.
 - Design and implementation of database systems including hierarchy, network and relational models, and the language extensions required to support such systems.
 - Computer graphics covering human-computer interaction and methods for computer-assisted problem solving.
 - Artificial intelligence techniques including heuristic search, artificial intelligence languages, knowledge representation, expert systems and means-end analysis.
 - Formal methods for the design and analysis of software systems.

- The officer must have a thorough knowledge of computer system design to include:
 - System analysis and design theory encompassing the basics of analysis, design and testing.
 - Empirical and analytical methods for determining the efficiency and performance of computer systems.
 - An understanding of the design issues of hardware/software compatibility, operating system compatibility and information system requirements.
 - Computer science theory relevant to the capabilities and limitation of hardware and software systems.
 - Computer security of DOD and other hardware systems, software systems and networks.
- The officer must have a thorough knowledge of computer architecture to include:
 - Basic components of computer systems and their patterns of configuration and communication covering the range of large scale mainframes to microcomputers.
 - The organization, logic design, and components of military and other digital computing systems relating to multiprocessing, multiprogramming, distributed processing and networking.
- The officer shall possess skills that perform a realistic perspective on solving military and real world problems.
 - Completing a significant project applying academic skills outside the classroom.
 - The graduate will demonstrate the ability to conduct independent analysis in computer science and proficiency in presenting the results in writing and orally by means of a thesis and command-oriented briefing.
- American and world military history and joint and maritime planning including the origins and evolution of national and allied strategy; current American and allied military strategies which address the entire spectrum of conflict; the U.S. maritime component of national military strategy; the organizational structure of the U.S. defense establishment; the role of the commanders of unified and specified commands in strategic planning, the process of strategic planning; joint and service doctrine, and the roles and missions of each in meeting national strategy. [Ref. 69: pp. 62-3]

C. INFORMATION TECHNOLOGY MANAGEMENT (Curriculum 370, subspecialty code XX89P)

- American and world military history and joint and maritime planning including the origins and evolution of national and allied strategy; current American and allied military strategies which address the entire spectrum of conflict; the U.S. maritime component of the National Military Strategy; the organizational structure of the U.S. defense establishment; the role of the Commanders of the Unified and Specified Commands in strategic planning; the process of strategic planning; joint and service doctrine, and the roles and missions of each in meeting national requirements.
- The officer must have a thorough knowledge of information systems technology to include:
 - Computer Systems: Components of computer systems including central processing units, input/output devices, storage devices, operating systems, programming languages, distributed computer systems and computer security.
 - Communication Systems and Networks: PCM systems, AM, FM, TV, modulation, SATCOM, fiber optics, HF, microwave systems, error control coding, antijam communications, low probability of intercept communications, GPS, data encryption, wide- and local-area network hardware, software, components and systems, physical layer interfaces and protocols, communications software, network management and control, and communications security.
 - Software Engineering: Methodologies for the analysis, design, development, prototyping, testing, implementation and maintenance of software; software metrics and reliability; productivity analysis and software cost estimation and planning; man-machine interfaces and system ergonomics; CASE and ICASE tools.
 - Database Management Systems: Database technologies (including object oriented) and technical and administrative issues involved in the design, implementation and maintenance of database management systems.
 - Decision Support and Expert Systems: Problem identification, formulation, and design of systems to support decision making; application of artificial intelligence technology to preserve perishable expertise and enhance distributed expertise; understanding the design of executive information systems, office automation, group decision support systems and crisis management systems, and their potential impacts on organizations and missions.

- The must officer must master the following concepts to effectively manage information system assets:
 - Managerial Concepts: Decision-making theory, microeconomics, operations analysis, financial management, organization development, and research methodologies.
 - Evaluation of Information Systems: cost and operational effectiveness (benefit) analysis; selection, evaluation, acquisition, installation and effective utilization of information systems hardware and software; risk assessment; information system architectures involving alternative system concepts.
 - Systems Analysis and Design: Information systems feasibility studies and life cycle management including fact-finding techniques for determining systems requirements and specifications, system performance evaluation, conversion and maintenance of legacy systems and post-implementation evaluation and security analysis of information systems.
 - Management of Information Systems: Information systems facilities planning, production planning and control, requirements determination of information systems personnel, human resource management, budgeting and financial control of computer centers, design of effective organization structure and information systems, and control and security (INFOSEC) policies.
 - Adapting to Technological, Organizational, and Economic Changes: Evaluation of potential impacts of new technology on information systems planning and development and on organization strategy; appraisal of evolving responsibilities of information systems managers.
- The officer must be able to combine analytical methods and technical expertise with operational experience for effective military applications to include:
 - DOD Decision Making Process on Information Systems: DOD, DON, OMB and congressional decision making on information systems matters.
 - Acquisition Management: Acquisition policies and procedures of the DOD, including the planning, programming, and budgeting system; project management.
 - DOD Computer and Telecommunications: Architectures and specifications of Navy and DOD systems, computers, telecommunications networks and services, including the Defense Communication System (DCS); Navy fleet communications system, including satellite communications, WWMCCS,

MIN, JMCIS, GCCS, and the Navy Telecommunications System (NTS);
Decision Support Systems.

- C4I and C2W: Concepts and application to strategic, operational and tactical level operations including support. [Ref. 69: pp. 139-141]

LIST OF REFERENCES

1. Chief of Naval Operations, ADM M. Boorda during the commissioning ceremony for the Fleet Information Warfare Center, Norfolk, Va., October 24, 1995.
2. Joint Publication 3-13, Joint Doctrine for Command and Control (C2W) Warfare: Battlefield Application of Information Warfare, Draft, March 1995.
3. Chairman, Joint Chiefs of Staff, Memorandum of Policy No. 30, 1st revision, 8 March, 1993.
4. Paret, Peter, *Makers of Modern Strategy from Machiavelli to the Nuclear Age*, Princeton University Press, Princeton, N. J., 1986.
5. Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 1 December, 1989.
6. Armed Forces Staff College Pub 1, *The Joint Staff Officers Guide* 1993.
7. Hutcherson, N., Lt. Col., *Command and Control Warfare: Putting Another Tool in the Warfighter's Database*, Air University Press, Maxwell AFB, Alabama, September 1994.
8. *A Historical Survey of Counter-C3*, BDM Corporation, McClean, Va., 27 April, 1979.
9. *Conduct of the Persian Gulf War Conflict: An Interim Report to Congress*, U.S. Department of Defense, Government Printing Office, Washington, D.C., July 1991.
10. Joint Publication 3-53, *Doctrine for Joint Psychological Operations*, 30 July, 1993.
11. Joint Command and Control Warfare Staff Officer Course, National Defense University, Armed Forces Staff College, Norfolk, Va., April 1993.
12. Joint Publication 3-0, *Doctrine for Joint Operations*, 9 September, 1993.
13. Radvanyi, Janos, ed., *Psychological Operations and Political Warfare in Long-term Strategic Planning*, Praeger, New York, 1990.
14. FM 90-24, *Multi-Service Procedures for Command, Control, and Communications Countermeasures*, 17 May, 1991.

15. Joint Command and Control Warfare Staff and Operations Course Student Text, Armed Forces Staff College, Norfolk, Va., January 1996.
16. Laffey, Thomas J., "The Real-Time Expert," Byte, Vol. 16, Issue 1, January 1991.
17. Abell, John M., Lisa K. Roach, and Michael W. Starks, Degraded States Vulnerability Analysis, Army Ballistic Research Lab, Aberdeen Proving Ground, Maryland, June, 1989.
18. Anderson, Randy and Penny Guglielmoni, Effectiveness Vulnerability Assessment Post Processor (EVAPP) Version 1, User's Manual, Sverdrup Technology, Inc., Eglin AFB, Florida, Technical and Engineering Acquisition Support Group, June, 1995.
19. Bailey, Charles, James M. Bates, Jr., Eugene J. Bednarz, Scott J. Smith, and Howard C. Wilson, A Procedure to Evaluate Survivability Methodologies for Aircraft Design, Volume I, Air Force Institute of Tech Wright-Patterson AFB, OH School of Engineering, December, 1982.
20. Ballance, Robert A., Anthony J Giancola, and Jeff Van Dyke, An Object-Oriented Approach for Vulnerability Assessments. Phase I, Kachina Technologies, Inc. Albuquerque, New Mexico, February, 1994.
21. Bennett, Gerald B., Jr., Vulnerability Predictors for US Aircraft and Two Large Threat Weapons, Aeronautical Systems Division, Wright-Patterson AFB, OH Directorate of Mission Analysis, August, 1982.
22. Bennett, Gerald B., Jr., Vulnerability Estimators for Conceptual Aircraft, Aeronautical Systems Division, Wright-Patterson AFB, Ohio, August, 1981.
23. Beverly, William, A Tutorial for Using the Monte Carlo Method in Vehicle Ballistic Vulnerability Calculations, Army Ballistic Research Lab, Aberdeen Proving Ground, Maryland, August, 1981.
24. Bowers, Ronald A., Application of the Battle Damage Repair Methodology to the M1A1 Abrams Main Battle Tank, Army Research Lab, Aberdeen Proving Ground, Maryland, August, 1994.
25. Buckland, Michael E., Mark Webster, and Frank J. Tkalcevic, GRAFTED - Graphical Fault Tree Editor: A Fault Tree Description Program for Target Vulnerability/Survivability Analysis. User Manual, Materials Research Labs, Ascot Vale (Australia), December, 1993.
26. Burdeshaw, Mark D. John M. Abell, Scott K. Price, and Lisa K. Roach, Degraded States Vulnerability Analysis of a Foreign Armored Fighting Vehicle, Army Research Lab, Aberdeen Proving Ground, Maryland, November, 1993.

27. Celmins, Aivars, Accuracy of Vulnerability Integrals, Army Ballistic Research Lab Aberdeen Proving Ground, Maryland, April, 1990.
28. Crawford, Kent S. and Michael J. Bosshardt, Assessment of Position Factors that Increase Vulnerability to Espionage, Defense Personnel Security Research Center, Monterey, California, October, 1993.
29. Erdmann, David, Foreign Asset Management Methodology, Alliant Techsystems, Inc., Edina, Minnesota, January, 1993.
30. Finn, Gregory G., Reducing the Vulnerability of Dynamic Computer Networks, University of Southern California, Marina Del Rey Information Sciences Institute, June, 1988.
31. Fleming, Richard W., Vulnerability Assessment Using a Fuzzy Logic Based Method, Air Force Institute of Tech Wright-Patterson AFB, OH School of Engineering, Master's Thesis, December, 1993.
32. Hafer, T., D. Brassard, K Brendley, and D. Garfinkle, Vulnerability Methodology Upgrade, System Planning Corp., Arlington, Va., July, 1985.
33. Happ, Henry, Charles Royer, George Radke, and Joseph Krainak, The Satellite Assessment Center Modeling Tool, Kaman Sciences Group, Albuquerque, New Mexico, June, 1994.
34. Kiger, S. A., T. R. Slawson, and D. W. Hyde, Vulnerability of Shallow-Buried Flat-Roof Structures. Report 6, A Computational Procedure, Army Engineer Waterways Experiment Station, Vicksburg, MS Structures Lab, September, 1984.
35. Krauthammer, Theodor, A Computational Approach for Vulnerability and Response Assessment of Buried Reinforced Concrete Arches, Pennsylvania State University, University Park Dept. of Civil Engineering, January, 1992.
36. Moch, D. A., W. J. Vogt, and L. S. Wolfarth, Cruise Missile Vulnerability Study, Volume 1, Historical Vulnerability Review, Analytic Sciences Corp., Fort Walton Beach, Florida, December, 1993.
37. Notwothy, M. W., Cruise Missile Vulnerability Study, Volume 2, 3 DOF Engagement Analysis, Analytic Sciences Corp., Fort Walton Beach, Florida, December, 1993.
38. Radke, G. E. Jr. and J. Evanoff, A Fast Recursive Algorithm to Compute the Probability of M-out-of-N Events, Phillips Lab, Kirtland AFB, New Mexico, May, 1994.

39. Robinson, Alan R., Assessing the Vulnerability of Multi-Commodity Networks with Failing Components, Air Force Institute of Tech Wright-Patterson AFB, OH School of Engineering, Master's Thesis, March, 1994.
40. Schlegel, Palmer R., Ralph E. Shear, and Malcolm S. Taylor, A Fuzzy Set Approach to Vulnerability Analysis, Army Ballistic Research Lab, Aberdeen Proving Ground, Maryland, December, 1985.
41. Shavers, Victor R., Command Control, Communications (C3) as a Tactical Force Multiplier - Myth or Reality, Army War College, Carlisle Barracks, Pennsylvania, April, 1982.
42. Speers, John J., Ron L. Hinrichsee, R. M. Marshall, C.N. Heightland, and Clark E. Wallace, Structural Assessment and Vulnerability Evaluation - Aircraft Vulnerability to High Energy Lasers, Science Applications International Corp., Dayton, Ohio, March, 1994.
43. Walbert, James N., The Mathematical Structure of Vulnerability Spaces, Army Research Lab, Aberdeen Proving Ground, Maryland, November, 1994.
44. Ward, Beth S., John M. Abell, and Mark D. Burdeshaw, Degraded States Vulnerability Analysis of a Self-Propelled Howitzer, Army Research Lab, Aberdeen Proving Ground, Maryland, November, 1994.
45. Wolfe, J. W., Data Link Vulnerability Analysis (DVAL) Methodology. Electronic Warfare and Intelligence Support (EWIS) Process, Data Link Vulnerability Joint Test Force, Kirtland AFB, New Mexico, November, 1984.
46. Howard, Michael Eliot and Peter Paret, On War/Carl von Clausewitz, Princeton University Press, Princeton, N. J., 1976..
47. Podell, Harold J. and Marshall D. Abrahms, "A Computer Glossary for the Advanced Practitioner," Computer Security Journal, Vol. IV, No. 1, Northborough, Ma: Computer Security Institute, 1986.
48. Interview with CDR G. Lott, Naval Postgraduate School, Department of Electronics and Engineering, Monterey, Ca., 24 May, 1996.
49. Arquilla, John and David Ronfeldt, "CyberWar Is Coming!," Comparative Strategy, Vol. 12, no. 2, 1993, pp. 141-165.
50. Margolis, Philip E., Personal Computer Dictionary, Random House, New York, 1991.
51. "Most Common Viruses By Name," McAfee Virus, <http://www.mcafee.com/support/techdocs/vinfo/comnames.html>.

52. "Advanced Capability Requirements,"
http://www.arpa.mil/asto/MOOTW_Folder/chapter3.html.
53. Talbot, Brent, Former Secretary of State, "The New Geopolitics: Defending Democracy in the Post-Cold War Era," Oxford University Address, October 1994.
54. Interview with Professor David Henderson, Naval Postgraduate School, Department of Systems Management, Monterey, Ca., May 21, 1996.
55. Spegele, Joseph B., A Framework for Evaluating Application of Smart Cards and Related Technology Within the DOD, Master's Thesis, Naval Postgraduate School, Monterey, Ca., 1995.
56. Criterium Decision Plus User's Guide, Sygenex Corp. 1994-1995.
57. Indermaur, Kurt, "Baby Steps," Byte, Vol. 20, Issue 3, March 1995, pp. 97-104.
58. Hanson, Rickey L., CPT, USA, "The Evolution of Artificial Intelligence and Expert Computer Systems in the Army," Master's Thesis, U.S. Army Command and General Staff College, Ft. Leavenworth, Kansas, 1992.
59. Alexander, Robert S., "Intelligent Application of Artificial Intelligence," Phalanx, Vol. 24, No. 4, December 1991.
60. "Going Beyond Real-Time, The Next Step in Simulation," Aviation Week & Space Technology, Vol. 141, Issue 11, September 12, 1994, p. 71.
61. Dunlap, Charles J., Jr., "How We Lost the High-Tech War of 2007," The Weekly Standard, January 29, 1996, pp. 22-28.
62. Port, Otis, "Computers That Think are Almost Here," Business Week, n3433, July 17, 1995, pp. 68-71.
63. Feigenbaum, Handbook of Artificial Intelligence, Harmon & King, 1985.
64. Widman, Lawrence E., "Expert Systems in Medicine,"
<http://amplatz.uokhsc.edu/acc95-expert-systems.html>, 1995.
65. Brown, Carol E. and Daniel E. O'Leary, "Introduction to Artificial Intelligence and Expert Systems," http://www.bus.orst.edu/faculty/brown/es_tutor/es_tutor.htm, 1994.
66. Hedberg, Sara, "Artificial Ingredients," CIO, Vol. 7, Issue 16, June 1, 1994, pp. 72-79.

67. Highland, Fred, ed., "Embedded AI," IEEE Expert, Vol. 9, No. 3, June 1994, pp. 18-20.
68. Superintendent, Naval Postgraduate School Memorandum dtd 15 September 1995, Educational Skill Requirements for Information Warfare Curriculum (595) XX46P, Deputy Director for Operations (Current Ops) (J38) and Director, Command and Control Warfare Division (N-64).
69. The Naval Postgraduate School Catalog, Academic Year 1996.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center2
 8725 John J. Kingman Road., Ste 0944
 Ft. Belvoir, VA., 22060-6218

2. Dudley Knox Library.....2
 Naval Postgraduate School
 411 Dyer Rd.
 Monterey, California 93943-5101

3. Office of the Deputy Assistant Secretary of the Navy1
 Navy 1000
 Pentagon Room 5E715
 Washington, DC 20350-1000
 DASN C4I
 Attn.: CDR S. Vetter

4. Dr. Gerry Baumgartner1
 NCCOSC RDTE DIV / Code 841
 53570 Silvergate Ave.
 San Diego, California 92152-5274

5. LT David Jacobson1
 1317 Neck Rd.
 Burlington, N.J. 08016

6. Capt. Vern Huber1
 U.S. Atlantic Command
 1562 Mitscher Ave., Suite 200
 Norfolk, VA. 23551-2488

7. Professor Vicente Garcia10
 816 Sherman Ct.
 Marina, CA., 93933

8. Professor Carl R. Jones Code SM/Js.....2
 Naval Postgraduate School
 Monterey, CA. 93943

9. Professor Fred Levien1
Chairman, Electronic Warfare Department
Naval Postgraduate School
Monterey, CA. 93943-5000
10. Professor Dan Boger Code SM/Bo1
Systems Management Academic Group
Naval Postgraduate School
Monterey, CA. 93943-5000
11. Professor John Arquilla Code NS/Ar1
SOLIC Department
Naval Postgraduate School
Monterey, CA. 93943-5000
12. Professor Cynthia Irvine Code CS/Ic1
Computer Science Academic Group
Naval Postgraduate School
Monterey, CA. 93943-5000
13. LCDR Steve Iatrau1
IW Academic Group
Naval Postgraduate School
Monterey, CA. 93943-5000
14. Professor John Gibon Code CC/Gj.....1
C4I Academic Group
Naval Postgraduate School
Monterey, CA. 93943-5000
15. LT Debra A. Lankhorst3
P. O. Box 33
Chest Springs, PA. 16624