
1998 THESIS ABSTRACTS IW

DETERMINATION OF A METHODOLOGY FOR CONDUCTING A COST EFFECTIVENESS ANALYSIS STUDY OF THE INTEGRATION OF LOW OBSERVABLES (LO) AND ELECTRONIC WARFARE (EW) IN AIR VEHICLE (AV) DESIGN (U)

Oscar L. Alvarado-Civilian

B.S., Texas A&M University, 1986

Master of Science in Electrical Engineering-September 1998

Advisors: F.H. Levien, Department of Electrical and Computer Engineering

R. Clark Robertson, Department of Electrical and Computer Engineering

CAPT James R. Powell, Information Warfare Academic Group

The advent of decreasing defense budgets coupled with acquisition reform efforts and the high cost of advanced technology applications has produced a definitive need for a methodology to assess the cost benefit of aircraft performance specifications. This methodology must be an iterative process that allows the user to perform design tradeoffs and assess their respective impacts to military utility and cost. This thesis details the approach for conducting an Analysis of Alternatives (AoA), a.k.a. Cost and Operational Effectiveness Analysis (COEA), study to assess the cost-performance tradeoffs of applying Low Observable (LO) technology and Electronic Warfare (EW), either exclusively or mutually, to an aircraft design. The methodology recommends the use of engagement level models and simulations (M&S) coupled with mission level M&S in the absence of a single integrated M&S product. The engagement level analysis is necessary to support high fidelity data requirements that are used by the mission level program to gather relevant measures of effectiveness (MOE) required for the mission effectiveness evaluation. These MOE's are then integrated with corresponding cost data in an effort to examine cost-performance characteristics. Iterative performance modifications can be similarly evaluated in an effort to establish trends, which will assist the user in assessing cost-performance tradeoffs.

DoD KEY TECHNOLOGY AREAS: Modeling and Simulation, Other (Low Observables, Electronic Warfare, Electronic Counter-Measures)

KEYWORDS: Low Observables, Radar Cross Section Reduction, RCS, Electronic Counter-Measures, ECM, Modeling and Simulation, M&S, Mission Level Modeling and Simulation, Enhanced Surface-To-Air Missile Simulation, ESAMS

ORGANIZATIONAL INNOVATION AND REDESIGN IN THE INFORMATION AGE: THE DRUG WAR, NETWAR, AND OTHER LOWER-END CONFLICT

Alexander Berger, Captain, United States Air Force

B.A., University of New Hampshire, 1990

M.S., Troy State University, 1996

Master of Arts in National Security Affairs-March 1998

Advisors: John Arquilla, Information Warfare Academic Group

Scott D. Tollefson, Department of National Security Affairs

The end of the Cold War and the rise of the Information Age have fostered an uncertain security environment which the United States is struggling to master. The purpose of this thesis is to explore the factors that lead complex organizations to initiate large-scale structural change in the face of environmental uncertainty; and more specifically to determine how the rise of the Information Age may change the organizational requirements of the U.S. national security structure. This thesis creates a unique framework for analysis, blending principles of organization and innovation theory with the theory of information-based "netwar."

This study analyzes the organizational structures adopted by several transnational drug cartels and compares them to that of U.S. counternarcotics forces. Next, this thesis reviews a series of recent occurrences pertaining to national security to test whether there are manifestations of netwar threats emerging and whether new and old organizational actors are learning to adapt their structures to gain an advantage over the United States.

1998 THESIS ABSTRACTS IW

Finally, this thesis is both predictive and prescriptive with regard to the issues of organizational redesign. It argues that structural changes are necessary for the United States to ensure the national security in an Information Age. Then it makes recommendations that would help the U.S. security structure redesign itself to become more agile in the face of Information Age threats.

DoD KEY TECHNOLOGY AREAS: Battlespace Environments, Command, Control, and Communications

KEYWORDS: Organizational Redesign, Information Warfare, Drug War, Innovation, Inter-Service Coordination, Netwar

ARTIFICIAL INTELLIGENCE AND FOREIGN POLICY DECISION-MAKING

Russ H. Berkoff-Major, United States Army

B.S., United States Military Academy, 1981

Master of Science in Defense Analysis-December 1997

Advisors: John Arquilla, Information Warfare Academic Group

Christopher Layne, Command, Control, and Communications Academic Group

With the advent of a global information society, the U.S. will seek to tap the potential of advanced computing capability to enhance its ability to conduct foreign policy decision-making. This thesis explores the potential for improving individual and organizational decision-making capabilities by means of artificial intelligence (AI). The use of AI will allow us to take advantage of the plethora of information available to obtain an edge over potential adversaries. Another purpose of this thesis is to give guidance to the software community as to what policymakers will need in order to improve future decision-making processes. The third purpose is to encourage government and private sector decision-makers to allocate adequate resources to actualize the potential of AI. The method of analysis this thesis uses is to examine U.S. foreign policy decision-making on the cognitive or individual, group, and organizational levels. Using the Cuban Missile Crisis and the Yom Kippur War as test beds for critical analysis, identification of both decision enhancing and impeding functions is accomplished. Finally, a counterfactual analytic framework, using an AI model, tests the likely influence of AI on decision-making. The results substantiate the value of AI as both a decision-making enhancer and an impediment reducer for the policymaker. Additional conclusions are derived that improve the decision-making system and its processes by means of introducing an AI capability.

KEYWORDS: Artificial Intelligence, Foreign Policy, Cuban Missile Crisis, Yom Kippur War, Decision-Making, Cognitive Theory, Group Dynamics, Organizational Theory, Bureaucratic Politics, Decision Modeling, Decision-Making

DoD KEY TECHNOLOGY AREAS: Command, Control, and Communications, Computing and Software, Modeling and Simulation

SINGLE-FREQUENCY MEASUREMENTS USING UNDERSAMPLING METHODS

Eng S. Chia-Major, Republic of Singapore Air Force

B.S., National University of Singapore, 1989

Master of Science in Electrical Engineering-March 1998

Advisor: Phillip E. Pace, Department of Electrical and Computer Engineering

Second Reader: Curtis D. Schleher, Information Warfare Academic Group

The objective of this study is to verify the Symmetrical Number System (SNS) undersampling receiver architecture using software and to investigate implementation issues using digital signal processing (DSP) hardware. In the software design, a MATLAB program is written to determine a single sinusoidal input frequency using this receiver architecture. Each channel of the SNS undersampling receiver consists of a low speed ADC, a discrete Fourier transform followed by a constant threshold device to detect the signal's frequency bin. The detected frequency bins are then recombined in an SNS-to-decimal algorithm to recover the frequency of the signal. Error rate performance in a Gaussian noise environment at the input stage is evaluated. In the hardware design, a sinusoidal waveform is digitized, discrete Fourier transformed and

1998 THESIS ABSTRACTS IW

converted from the SNS format to a decimal value using a single channel digital signal processor. Implementation difficulties and design issues are discussed.

DoD KEY TECHNOLOGY AREA: Electronic Warfare

KEYWORDS: Symmetrical Number System, Symmetrical Folding, Undersampling, Discrete Fourier Transform

21ST CENTURY SUBMARINE INFORMATION OPERATIONS (U)

Scott R. Coughlin-Lieutenant, United States Navy

B.S., United States Naval Academy, 1992

Master of Science in Systems Engineering-September 1998

Advisor: Vicente C. Garcia, Jr., National Security Agency Cryptologic Chair

Second Reader: CAPT James R. Powell, Information Warfare Academic Group

The United States Submarine Force has a long and distinguished history of providing national decision makers with Intelligence, Surveillance, and Reconnaissance services allowed by the unique access granted by the submarine's attribute of stealth. To maximize the effectiveness of our submarine fleet to continue to perform tomorrow's Information Operations (IO) missions requires evolution. This thesis will explore how to best prepare our submarine fleet to perform Information Operations.

DoD KEY TECHNOLOGY AREAS: Battlespace Environments, Command, Control and Communications, Conventional Weapons, Electronic Warfare, Surface/Under Surface Vehicles – Ships and Watercraft, Sensors, Directed Energy Weapons, Air Vehicles, Space Vehicles, Computing and Software

KEYWORDS: Submarine, Information Operations, Information Warfare, Intelligence, Reconnaissance, Surveillance

DEVELOPMENT OF HIGH POWER MICROWAVE (HPM) ADVANCED CONCEPT TECHNOLOGY DEMONSTRATION (ACTD) FOR ASCM DEFENSE OF THE ARG (U)

Brian P. Dulla-Lieutenant, United States Navy

B.S., United States Naval Academy, 1991

Master of Science in Applied Physics-December 1997

Advisor: Captain James R. Powell, Information Warfare Academic Group

CLASSIFIED ABSTRACT

KEYWORDS: High Power Microwaves (HPM), Directed Energy Weapon, Anti-Ship Cruise Missile Defense, Microwave Coupling

DoD KEY TECHNOLOGY AREAS: Electronic Warfare, Directed Energy Weapons

1998 THESIS ABSTRACTS IW

AN ASSESSMENT OF WIRELESS LOCAL AREA NETWORKS: VULNERABILITIES AND POTENTIAL MILITARY IMPLEMENTATION (U)

Cynthia M. Fulmer-Lieutenant Junior Grade, United States Navy

B.S., United States Naval Academy, 1995

Master of Science in Systems Engineering-September 1998

Advisors: CAPT James R. Powell, Information Warfare Academic Group

Vicente Garcia, National Security Agency Cryptologic Chair

Wireless network technology provides improved services such as flexibility and high data rates at the promise of full mobility. The emergence of wireless local area networks (WLANs) has changed the role of wired communications in the face of this lower-cost, easy to implement, flexible technology. Wireless networks have mainly been implemented for civilian use. However, there is tremendous potential for WLANs in the military, from everyday administrative to operational shipboard implementation, to use by the Marine Corps during amphibious assaults and other ground maneuvers. The widespread use of WLANs, however, has occurred without certain key issues such as the security and vulnerabilities of WLANs being addressed. The objective of this thesis is to provide the Department of Defense with critical information on WLANs, a tutorial on how WLANs work, and to address the issue of vulnerabilities. This thesis provides a background of WLANs, looking at wireless communication, wired LANs, and the IEEE 802.11 standard for WLANs. It discusses vulnerabilities of WLANs and provides an initial vulnerability assessment and provides an overview of how WLANs have been implemented in the military, its potential for future use, and the security issues involved with military implementation.

DoD KEY TECHNOLOGY AREAS: Command, Control, and Communications, Computing and Software

KEYWORDS: Wireless Local Area Networks, Local Area Networks, Wireless Communication, IEEE 802.11, Wireless Security

LOW-END SOLUTIONS TO THE UNDERGROUND DILEMMA

Brian M. Hayes-Captain, United States Army

B.S., Suffolk University, 1986

Master of Science in Defense Analysis-December 1997

and

David A. Roddenberry Jr.-Major, United States Army

B.S., Western Carolina University, 1986

Master of Science in Defense Analysis-December 1997

Advisors: John Arquilla, Information Warfare Academic Group

Gordon H. McCormick, Command, Control, and Communications Academic Group

Both the 1981 Israeli Raid on the Osirak nuclear reactor in Iraq and the Gulf War, served notice to would-be proliferators that, in order to survive in the face of the conventional superiority of the United States and its allies, means must be developed to protect those assets deemed valuable or strategic in nature. Many would-be proliferators have chosen to develop underground structures, referred to as hardened and deeply buried targets (HDBT), as the preferred means to protect and hide their efforts to obtain weapons of mass destruction (WMD). To counter this trend, the U.S. relies almost entirely upon a policy of negotiated peacetime elimination or reduction of WMD/HDBT through diplomatic channels. Yet, if these efforts fail and the necessity for preemption or prevention emerges, instead of immediately relying on direct force alternatives, an indirect low-level interdiction method may be both more appropriate and available.

This thesis explores an alternative means by which the vulnerabilities of HDBT/WMD sites may be exploited through the use of low-level, indirect, counter-force strategies. This exploration of alternative HDBT interdiction approaches concludes that low-level counterforce strategies can complement existing counterproliferation initiatives, when employed as components of an overall campaign designed to deny and disrupt a would-be proliferator's progress.

1998 THESIS ABSTRACTS IW

KEYWORDS: Counterproliferation, Hardened and Deeply Buried Targets (HDBT)

DoD KEY TECHNOLOGY AREA: Other (Weapons of Mass Destruction)

WINDOWS NT 4.0 SECURITY FOR IT-21

Kevin S. Hinton-Lieutenant, United States Navy

B.S., United States Naval Academy, 1991

Master of Science in Systems Engineering-September 1998

Advisors: CAPT James R. Powell, Information Warfare Academic Group

Vicente C. Garcia, National Security Agency Cryptologic Chair

The Navy is jumping into the information technology revolution by procuring commercial off-the-shelf computer networking hardware and software. This strategy is termed IT-21 and revolves around minimum standards set in January 1997. These standards designate Microsoft Windows NT 4.0 as the computer network operating system for tactical and administrative networks. Windows NT is inexpensive and easy to install and maintain, but it is a young operating system and has proved to be full of vulnerabilities. This may make the Navy's exchange of administrative and tactical information highly vulnerable to a determined and technical foe as well as the teenage hacker. There are methods to reduce the risk, however. Windows NT can be configured and implemented to significantly reduce the number of vulnerabilities. There are also a number of commercial security products that monitor the configuration of Windows NT, scan for security vulnerabilities, and detect near real time intrusions into Windows NT networks. The application of a combination of these techniques can drastically improve the security of our information exchange systems in the 21st Century.

GREAT POWERS, WEAK STATES, AND ASYMMETRIC STRATEGIES

Michael R. Lwin-Captain, United States Army

B.S., Georgetown University, 1989

Master of Science in Defense Analysis-December 1997

Advisors: John Arquilla, Information Warfare Academic Group

Christopher Layne, Command, Control, and Communications Academic Group

On the verge of the twenty-first century, America finds itself in the position of a great power with dominant military technology. This thesis examines the possibility that weaker states may be able to strategically innovate and defeat us in war despite our technological advantages. The purpose of the thesis is to survey what type of strategic innovations, also known as asymmetric strategies, are possible and to examine the conditions under which they may be successful.

This thesis begins by defining asymmetric strategies using a comprehensive model of strategy developed by Rear Admiral J.C. Wylie. The thesis also examines four variables which may explain the success or failure of asymmetric strategies. To illustrate possible asymmetric strategies and examine the contextual conditions under which they work, the thesis considers the cases of the Italo-Ethiopian war of 1935-36, the Russo-Finnish War of 1939-40, and the American-North Vietnamese War of 1965-73. The thesis finds that the four variables have significant explanatory power for the success or failure of these strategies. The thesis concludes by examining strategic implications for the United States, both as a possible opponent of weak states and as a supporter of a weak state faced by a great power threat.

KEYWORDS: Strategy, Strategic Innovation, Asymmetric Conflict and Military Technology, Future Wars, Italo-Ethiopian War, Russo-Finnish War, Vietnam

DoD KEY TECHNOLOGY AREAS: Battlespace Environments, Conventional Weapons, Other (Strategy)

1998 THESIS ABSTRACTS IW

INFLUENCE MODELING STATE-TERRORISM FOR INFORMATION OPERATIONS (U)

Russell L. Marsh-Lieutenant, United States Navy

B.S., Oregon State University, 1994

Master of Science in Systems Engineering-September 1998

Advisor: CAPT James R. Powell, Information Warfare Academic Group

Second Reader: Gordon McCormick, Special Operation Low Intensity Conflict (SOLIC) Curriculum Committee

The purpose of this research is to use Situational Influence Assessment (SIAM) Module created by SAIC to model a terrorist organization that is attempting to disrupt negotiations between two state actors. The SIAM model was used to analyze the causal relationships and to look for the various leverage points at which to apply Information Operations (IO) that will minimize the effects of terrorist action, and influence the terrorists decision making process. The actors in a specific scenario were modeled as to how leadership could be influenced. After analysis with SIAM, possible IO options were created, incorporated into the model and tested to see how effective the IO options were at influencing the decision-making process. Once the IO options had been tested, a suggested plan of action results. Both a preventative approach and reactive approach are proposed. The preventative approach is intended to reduce the effectiveness of terrorism and impede the conduct of the terrorist organization. The reactive approach provides options for responding to terrorist activities without alienating the surrounding populace.

DoD KEY TECHNOLOGY AREA: Modeling and Simulation

KEYWORDS: SIAM, Terrorism, Information Operations, Peace Negotiations

AN OPERATIONAL HIGH POWER MICROWAVE APPLICATION FOR INFORMATION OPERATIONS (U)

Daniel J. Miller-Lieutenant, United States Navy

B.S., University of Colorado, 1992

Master of Science in Systems Engineering-September 1998

and

David P. Shewfelt-Captain, United States Marine Corps

B.S., United States Naval Academy, 1991

Master of Science in Systems Engineering-September 1998

Advisor: CAPT James R. Powell, Information Warfare Academic Group

Second Reader: Michael A. Morgan, Department of Electrical and Computer Engineering

This thesis documents the results of a feasibility demonstration of a high power microwave application for Information Operations and recommends future improvements to the system. Success in the Information Operations (IO) and Information Warfare (IW) arena requires advanced capabilities. This thesis describes one such capability that would provide commanders with courses of action previously unavailable.

DoD KEY TECHNOLOGY AREA: Directed Energy Weapons

KEYWORDS: Information Operations, High Power Microwave

1998 THESIS ABSTRACTS IW

COMPUTER NETWORK ATTACK (U)

David C. Rice-Lieutenant, United States Navy

B.S., United States Naval Academy, 1994

Master of Science in Systems Engineering-September 1998

Advisors: CAPT James R. Powell, Information Warfare Academic Group

Vicente C. Garcia, National Security Agency Cryptologic Chair

The convergence of computing and telecommunications places new and complex demands on U.S. intelligence agencies. Techniques in Computer Network Attack are discussed as a means to cope with the new communications environment.

DoD KEY TECHNOLOGY AREAS: Computing and Software, Command, Control, Communications, Other (Computers and Intelligence)

KEYWORDS: Information Operations, Information Warfare, Computer Network Attack

MODELING THE EFFECTS OF INFORMATION OPERATIONS ON AN ADVERSARY DECISION-MAKER (U)

Walter E. Rogers, II-Lieutenant, United States Navy

B.A., Virginia Military Institute, 1991

Master of Science in Systems Engineering-September 1998

Advisor: CAPT James R. Powell, Information Warfare Academic Group

Second Reader: R. Mitchell Brown, Department of National Security Affairs

The potential for crisis and conflict exists in almost every region of the globe in today's unstable world. In this fiscally constrained time, however, the United States cannot afford to expend resources and lives by employing forces in every crisis. This makes the use of Information Operations as an instrument to deter conflict increasingly desirable. Information Operations have the potential to accomplish U.S. strategic goals more effectively, with reduced political risk, and with comparatively less physical risk to our armed forces. Few commanders, however, willingly commit to a course of action before they have a firm grasp of the expected results. Unlike the use of physical means, whose effectiveness can be measured in terms of CEP and PK, the effects of Information Operations on an adversary's decision process cannot be quantified in the same way because the outcome of this process does not display physical phenomena. This thesis applies a software tool entitled Situational Influence Assessment Module (SIAM) to examine how a specific adversary's decision process can be modeled and what effects Information Operations may have on influencing that process.

DoD KEY TECHNOLOGY AREAS: Modeling and Simulation, Other (Information Warfare)

KEYWORDS: IO Modeling and Simulation, SIAM

COMPUTER NETWORK RESEARCH IN THE WINDOWS NT ENVIRONMENT (U)

Bruce G. Ward-Lieutenant, United States Navy

B.S., State University of New York (Albany), 1991

Master of Science in Systems Engineering-September 1998

Advisors: Vicente C. Garcia, National Security Agency Cryptologic Chair

CAPT James R. Powell, Information Warfare Academic Group

The world is witnessing an explosion of computer networking that is quickly changing the way that the United States Armed Forces and Department of Defense (DoD) agencies, such as the National Security Agency (NSA), need to focus their resources. U.S. adversaries and rogue nations as a venue of aggression can easily attain attacks on the United States National Information Infrastructure (NII).

1998 THESIS ABSTRACTS IW

This research documents the development of the Naval Postgraduate School's Computer Network Research Lab and discusses at the classified level different techniques toward educating the warfighters and increasing the technical knowledge base of our military leadership, which will assuredly be required in future conflict and the cyber battle field.

DoD KEY TECHNOLOGY AREA: Computer and Software

KEYWORDS: Computer, Network Research, Windows NT