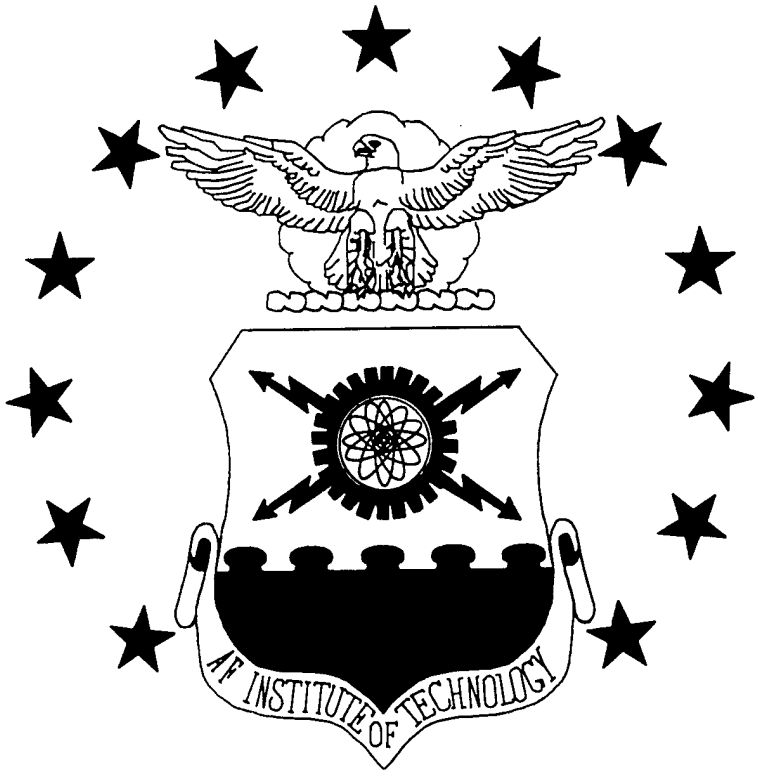

DEVELOPMENT OF A NATIONAL INFORMATION WARFARE STRATEGY: A REENGINEERING APPROACH

THESIS

Christina M. Anderson
Capt, USAF

AFIT/GIR/LAS/97D-1

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY
AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/GIR/LAS/97D-1

DEVELOPMENT OF A NATIONAL INFORMATION WARFARE STRATEGY: A REENGINEERING APPROACH

THESIS

Christina M. Anderson
Capt, USAF

AFIT/GIR/LAS/97D-1

Approved for public release; distribution unlimited

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.

AFIT/GIR/LAS/97D-1

DEVELOPMENT OF A NATIONAL INFORMATION WARFARE STRATEGY: A REENGINEERING APPROACH

THESIS

Presented to the Faculty of the Graduate School of Logistics

and Acquisition Management of the Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the

Requirements for the Degree of

Master of Science in Information Resource Management

Christina M. Anderson

Captain, USAF

December 1997

Acknowledgments

I first offer special thanks to my thesis committee for their support and assistance. As my advisor, Major Mike Morris provided an immeasurable amount of his valuable time editing and refining my work. His incredible patience and quiet professionalism taught me a well-learned lesson on officership and leadership. Thank you for trusting me and not micromanaging me even when time was running short. As my reader and advisor for Sigma Iota Epsilon (SIE), of which I was president, Dr. Tony D'Angelo too proved invaluable. Our discussions often provided needed respite from the stress at AFIT. His guidance as SIE advisor, coupled with wonderful fellow SIE officers who assisted with both initiations and the three tours we offered, made the job enjoyable and fun.

Second, I thank my family and friends for their love and support. My parents are truly my best friends, and they never fail to be there when I need them. Their pride in me has gotten me through occasional bouts of self-doubt and their unconditional love is what some children only dream about. To my friends (you know who you are), I offer my thanks for providing love and humor when I most needed it. The money didn't hurt either. Finally, I thank my new church family at Knollwood Church of Christ for their teaching of the Word and wonderful Christian example. I will miss you most of all.

Most importantly, I thank my personal Lord and Savior, Jesus Christ. On 13 April 1997, I became a committed Christian. I repented of my sins, professed my faith, and was born again under the watery grave of baptism for the remission of my sins. I had heard the Gospel for years but always felt something was missing. Now I know that I was missing Him in my life. Words cannot express my gratitude for His patience during my gradual understanding of, and final obedience to, the Gospel. It amazes me how very much He loves us. I am also thankful for the incredible gift of His Word, which gives all the guidance we need. I just hope all don't wait until it is too late to recognize Him and obey His commandments.

Christina M. Anderson

Table of Contents

Abstract

This thesis presents an analysis of the United States' national strategy for defensive against information warfare (IW). Vast improvements in technology. have created new problem areas regarding U.S national security and strategy. National security is now threatened by potential attacks on our national infrastructure. The need for defense against such attacks continues to grow as a national security problem. However, there is currently no national direction in this increasingly critical area of national security.

Regarding this need for a national IW policy, the following questions are investigated: 1) How and by whom is the U.S. ensuring reliability and security of its information?, 2) Are current key organizations in IW, and their associated strategies, adequately defending the U.S. against the threat of IW?, 3) Is there a need for a national IW strategy to successfully defend against information warfare threats?, 4) What recommendations have been made regarding organizational means to address national IW strategic objectives?, and 5) How might business process reengineering be applied to accomplishing a national IW strategy?

To answer the above questions, this study discusses the roles and responsibilities of organizations currently involved in IW. The research then evaluates the problems areas associated with these current efforts and experts' recommended solutions. The thesis then recommends business process reengineering as an effective methodology for developing and implementing the needed national policy. Specifically, the research provides a step-by-step process, based predominantly on Hyde's (1995) process management model, to utilize when pursuing this new national policy.

DEVELOPMENT OF A NATIONAL INFORMATION WARFARE STRATEGY:

A REENGINEERING APPROACH

I. Introduction

Failure to develop a strategy for both defensive and offensive information warfare could put the U.S. and the U.S. military into the situation of being on the receiving end of an 'Electronic Pearl Harbor'. --George J. Stein (1995)

Chapter Overview

This thesis presents an analysis of the United States' national strategy for defensive information warfare (IW). This chapter introduces general issues such as the advent of IW and its implications. The chapter then discusses the problem statements which will be addressed by this study. Finally, the chapter concludes with a description of its scope and limitations and a brief summary of the methodology employed.

General Issue

"Military weapons and military strategy usually reflect the politics, economy, and--most especially—the technology of a given society" (Berkowitz, 1995, 60). The advent of the current information age away from the industrial age has occurred precisely because of vast improvements in technology. Such advances in technology have drastically changed both military strategy and the weapons it employs to effectively pursue that strategy. However, "information technologies have expanded faster than the nation's understanding of the inherent vulnerabilities of the networks and systems that bind the more advanced nations" (Harley, 1997, 72). This dramatic and changing course of events creates new problem areas regarding U.S national security and strategy.

Due to such advances in information technologies, warfare has taken a new dimension in the form of IW. National security is now not only threatened by an invasion on our soils; our security is threatened by potential attacks on our national infrastructure such as telecommunications lines, banking information systems, and the national power grid (Berkowitz, 1995, 62; Fredericks, 1996, 2-3; Harley, 1997, 72: Molander et al, 1996, 85; O'Malley, 1997, 74; PCCIP, 1997, 1-2: Scott, Oct. 28, 1996, 60; Thomas, 1997, 90; Wells, 1996, 2; Whisenhunt, 1996, 6). The need for defense against such attacks continues to grow as a national security problem (Whisenhunt, 1996, 1; PCCIP, 1997, 2). "The more dependent the adversary is on information systems, the more vulnerable he is to hostile manipulations of those systems" (Szafranski, 1995, 61).

The military, in particular, has become more technologically dependent and thus more vulnerable (Harley, 1997, 72; Signal, February 1997, 21) The combination of the Department of Defense's reliance on civilian information systems and the fact that civilian information systems are prime candidates for attack create the need for a new defensive strategy (Berkowitz, 1995, 64; Campen, July 1995, 67; Grier, 1997, 22; PCCIP, 1997, 1: Scott, Oct. 28, 1996, 60). On the other end of the battle spectrum, the U. S. must fully recognize the use of information for offensive reasons. "Establishing information dominance will likely be crucial to effective military operations in most future conflicts" (Krepinevich, 1996, 13).

Coupled with the ever-growing global network, exponential advances in technology have significantly increased the potential harm of information attacks inflicted from any direction by even the smallest of America's adversaries (Berkowitz, 1995, 63;

PCCIP, 1997, 4). Due to the pervasive nature of IW, the United States may not even know exactly who their adversaries are (Covault, 1997, 21; Molander et al, 1996, 88). Whether politically or economically motivated, enemies have a much wider range of information tools available during the information age (PCCIP, 1997, 3). This reality "is an uncovered and unprotected source of great power and [is] perhaps [the U.S.'s] greatest vulnerability" (Coroalles, 1996, 32).

The United States, "in civilian as well as military matters, is more dependent on electronic information systems than is anyone else in the World" (Berkowitz, 1995, 59; Whisenhunt, 1996, 6). Thus, the United States is the most information-dependent country in the world, which significantly increases its vulnerability (Scott, 1995, 85; Aldrich, 1996, 100). "In a technologically advanced military, 'information is the heart and soul of everything we do' says Colonel James Massaro, commander of the Air Force's Information Warfare Center" (O'Malley, 1997, 74). Likewise, for the Army, "information can be considered the hub of a modern army's operational power and strength...in destroying an opponent's ability to gain, process, and transmit information may be the surest way to destroy that enemy" (Coroalles, 1996, 34).

Problem Statement

The problems addressed by this thesis provide an analysis of the roles and responsibilities associated with current key organizations involved in IW and an identification of an approach which may be valuable for developing an overarching national IW strategy. In particular, this research analyzes business process reengineering

(BPR) techniques as a potential application when such a national policy is developed. The following questions will be investigated:

1. How and by whom is the U.S. ensuring reliability and security of its information?
2. Are current key organizations in IW, and their associated strategies, adequately defending the U.S. against the threat of IW?
3. Is there a need for a national IW strategy to successfully defend against IW threats?
4. What recommendations have been made regarding organizational means to address national IW strategic objectives?
5. How might BPR be applied to accomplishing a national IW strategy?

Importance of Research

"It is critically important to ...the entire military that the national information environment be reliable and secure" (Wells, 1996, 10). What exactly is the U.S. doing to ensure reliability and security of its information environment? There are many entities currently engaging in both offensive and defensive IW, to include the U.S. Air Force. Along with other governmental agencies, each branch of the service has committed resources to IW (Jensen, 1994, 35). However, "the current course of each service developing their own capability will not suffice to meet this threat" (Wells, 1996, 25). Likewise, the military services are not in the position to defend the information infrastructure upon which they rely (Grier, 1997, 24). The Defense Science Board found that "current intelligence resources and processes that apply to IW are deemed insufficient to provide and understanding of the threats and potential adversary

capabilities" (Signal, March 1997, 70). Because such a system is failing to properly defend our information resources, what must the U.S. do?

There has yet to be a national direction in this increasingly critical area of national security (PCCIP, 1997, 5; Wells, 1996, 22; Whisenhunt, 1996, 2). "Information assets are now strategic assets and should be so reflected in our national security policy" (Thomas, 1997, 88). In addition, there has been little cooperation among both the private and public sector, both of whom will be integrally involved in IW (Scott, 1995, 88). "We need to strengthen our government-civilian partnership to protect the national information infrastructure" (Munro, 1996, 15; PCCIP, 1997, 1; Whisenhunt, 1996, 12). A 1991 National Research Council report "suggests the brokering and enhancement of communications between commercial and national security interests" (Signal, March 1997, 70). How will the U. S. create a team composed of members from both sectors to effectively manage IW?

Finally, what will happen if the United States does not provide overall direction and leadership in IW? The military alone is extremely vulnerable; it has more than 2 million computers and more than 10,000 local area networks that could be attacked by a determined aggressor (O'Malley, 1997, 74). How will the U.S. military be affected by such a failure to provide an overarching national IW strategy? "The American military is the most information-dependent force in the world...(it) is also the most networked force in the world, a combination which, absent adequate defenses, makes the American military extremely vulnerable to attack" (Aldrich, 1996, 100). The Defense Science Board predicts that "by 2005, attacks on U.S. information systems by terrorists and

foreign espionage agents will be widespread" (O'Malley, 1997, 72). In 1996, then CIA-director confirmed this when he "called the risk of cyberspace attack one of the top threats to U.S. national security" (Covault, 1997, 20). Is the United States adequately prepared to meet the increasing threat of IW? If not, what must be done to successfully meet this threat? This thesis provides a blueprint for addressing the above critical questions regarding national IW strategy.

Scope/Limitations

This research has a very broad scope in its application. IW has two sides: offensive and defensive. Offensive measures such as hacking, chipping, and electronic warfare are already used (Schwartau, 1996). Relative to defensive measures, these various offensive actions are better understood by the government, the private sector, and enemies of both; "the development of security measures is lagging significantly behind methods of attack, as offensive measures tend to be easier to develop and are outpacing efforts to counter them" (Signal, February 1997, 21). Offensive IW is included as a significant part of the overall national strategy. However, this thesis focuses only on the defensive front in information protection. The U. S. is seriously threatened by attacks against vital infrastructures and, thus, defensive measures are a central issue. Likewise, defensive IW is where the U. S. is most lacking in guidance and direction. Therefore, focusing on defensive issues is a reasonable research objective. The communications career field is charged with the defensive, information protection side of IW. Thus, it would behoove the field if this research provided a limited, defensive-oriented scope.

Research Approach and Overview

Chapter I introduced this thesis effort by providing the importance of this research, the problem statements to be addressed by this effort, and the thesis' scope and limitations. Chapter II presents an examination of current literature regarding the advent of IW, the current key organizations involved in the arena, the need for an overall national IW strategy, current recommendations on potential organizational methods for implementing that strategy, and an analysis of the benefits of the BPR approach. Chapter III then outlines the research history and methodology utilized in this thesis. Next, Chapter IV applies a step-by-step BPR approach to the current problem area of national IW strategy. In conclusion, Chapter V presents the limitations and potential future research topics applicable to this study.

II. Literature Review

As far as many experts in the U.S. government are concerned, IW is already here—and it is time to start planning serious defenses.– Peter Grier

Chapter Overview

Much has been published regarding the various social, political, and economic implications of information warfare (IW) in the United States. First, this thesis examines the advent of IW as a critical problem area for protection of vital national interests and security. Second, the research discusses the roles and responsibilities of the public and private sector organizations involved in IW. This study then reviews experts' arguments about the need for a national IW strategy. Business process reengineering (BPR) is then offered as a possible methodology for implementing these ideas regarding a national IW strategy. The study then covers BPR basics and determinants for using BPR. The discussion identifies problem areas in the current IW environment and offers BPR as a possible solution. Coupled with experts' current recommendations, the thesis discusses several implementation issues that need to be evaluated before BPR is used. Finally, the chapter concludes with an analysis of the first four problem statements.

New Role of IW

Without a doubt, the U. S. is more dependent than any other nation in the World on information and the systems that support and create it (Berkowitz, 1995, 59; Whisenhunt, 1996, 4). IW poses a particular threat because over 90 percent of military communications are on commercial lines, commercial vendors from foreign countries

develop software for use by the military, and modern military aircraft are designed solely by computer aided design programs. (Berkowitz, 1995, 60-61; Signal, February 1997, 22). The move from proprietary military systems "to commercial off-the-shelf, open architecture systems...could have a variety of vulnerabilities or security holes" (Ackerman, 1996, 58). All these realities present unique national security concerns. The "evolving battlefield involves friendly and enemy information systems that use military and commercial technologies and systems" (Robinson, February 1997, 17). IW could do serious damage via attacks on either military, other public sector systems, or private sector systems such as the national power grid or telecommunications lines (PCCIP, 1997, 1). A November 1997 report by the President's Commission on Critical Information Protection recommends the U.S. "build an IW nerve center to warn of electronic attack against not only U. S. military targets but the entire federal government and key private sector information sources" (Seffers and Walsh, 1997, 27). General Michael V. Hayden, USAF, former Air Intelligence Agency commander, states "Information now in its own right has become a place to do battle—[it can be used as] a weapon and a target" (Signal, July 1997, 60). Despite this recognition, however, the services are still in the early stages of incorporating IW in their strategies. "Although U.S. national security leaders agree IW is fast becoming a critical, integral element of military operations, they continue to wrestle with defining what IW is, what agency should be its focal point, and how it fits into overall defense policy" (Scott, 1996, 60).

Current Key Organizations Involved in United States IW

Currently, there are many U.S. organizations who have a role in the IW.

> The national security bureaucracy is currently very active in (IW) arena, with all of the military services and various civilian agencies and their supporting analytical organizations establishing centers for IW, writing position papers, and generally grappling with the problem of how to cope with the information revolution and its consequences. (Buchan, 1996, 1)

Some roles are very small while others constitute a large, vital part of our nation's current defense against IW attack. This study now looks at some of these key agencies.

Department of Defense (DoD). From the Office of the Secretary of Defense to the military services, the DoD is key in defensive IW strategy. DoD agencies are integral to successful IW. Each of the services has its own IW doctrine, strategy, and organization (Berkowitz, 1995, 64; Fredericks, 1996, 9; Jensen, 1994, 35; Wells, 1996, 1).

Office of the Secretary of Defense (OSD). In 1995, the Secretary of Defense formed the IW Executive Board to "facilitate the development and achievement of national IW goals" (Molander, 1996, 82). The Deputy Secretary of Defense is the Chairman and the board consists of senior DoD officials, including the Vice Chairman of the Joint Chiefs of Staff (Fredericks, 1996, 4). The Board "address(es) IW roles and responsibilities and serve(s) as a DoD focal point for IW discussion at the national level" (Fredericks, 1996, 4). An IW council chaired by the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)) supports the board and, as "the senior IW advisor to the Secretary of Defense, has organized a small IW directorate...to help him execute his responsibilities" (Fredericks, 1996, 4).

The OSD also has two directorates involved in IW. The IW directorate has a variety of roles, to include "centralized planning, coordination, and oversight for IW and conducts program reviews of selected Service and defense agency IW efforts...also focused on initiating a DoD 'Red Team' effort" (Fredericks, 1996, 4). The Infrastructure Policy Directorate (USD(P)) shapes "the role of DoD in the protection of infrastructures, including coordination between DoD and non-DoD government, and civilian/corporate owned infrastructures" (Fredericks, 1996, 5). Both the IW Executive Board and IW Council help deconflict the activities of ASD(C3I) and USD(P) (Fredericks, 1996, 5).

Joint Staff. Within the Joint Staff, the IW/Special Technical Operations Division (IW/STOD) is responsible for "coordinating compartmented planning between the Services, Combatant Commands, and DoD agencies...[it] provides the linchpin for ensuring the integration of all dimensions of joint IW" (Fredericks, 1996, 6). The Joint Command and Control Warfare Center (JC2WC) supports Combatant Commanders and "is fully engaged in the warfighting application of IW...[by] dispatch[ing] tailored teams to augment CINC and Joint Task Force staffs and provide C2W expertise in all joint exercises and contingency operations" (Fredericks, 1996, 7). Ultimately, JC2W2 serves "as executive agent to support the OSD Red Team effort" (Fredericks, 1996, 5). The Joint Communications Security (COMSEC) Monitoring Activity identifies "vulnerabilities exploitable by potential adversaries and recommend countermeasures and corrective actions" and the Joint Spectrum Center which "serves as the DoD focal point for supporting spectrum supremacy aspects of IW" (Fredericks, 1996, 8).

Defense Advanced Projects Research Agency (DARPA). DARPA's mission is to "perform research and development that helps the DoD to maintain U.S. technological superiority over potential adversaries" (MoA, 1995). Their work is often performed in unclassified, university settings (MoA, 1995). Regarding dual-use technologies, DARPA is the lead agency for development, dissemination, and training (Dunn, 1996, 34: Lepkowski, 1993, 22). Pertinent to this research, specific technologies emphasize information infrastructure (MoA, 1995). Given the dual nature of DARPA's research efforts and their massive funding --$2 billion in 1996 alone (Dunn, 1996, 34)--they "work hand in hand with industry on technologies that would be critical not just to defense but to U.S. competitiveness in civilian markets as well" (Corcoran, 1993, 20).

Defense Information Systems Agency (DISA). DISA has ultimate responsibility for protecting DoD's information infrastructure (Fredericks, 1996, 13). DISA both protects the DoD 'infosphere' from unauthorized access and assesses network vulnerabilities (Robinson, October 1995, 15; Whisenhunt, 1996, 5). According to a Joint Memorandum of Agreement between DISA, ARPA, and NSA, "DISA is the first line of defense for IW" (MoA, 1995). DISA provides "global automated systems security incident support team...to respond to security incidents" (Fredericks, 19965: Robinson, October 1995, 18). DISA's Countermeasures Department

> coordinates incident responses between 3 federal law enforcement agencies, 5 Defense Department counterintelligence/law enforcement agencies, 44 incident response teams, 20 vendors and manufacturers, 26 members of the national security information exchange, and 9 federal/national working groups. (Robinson, October 1996, 18)

DISA's Global Operations and Security Center (GOSC) "monitors the health and status of (DISA's) defense information systems network...[it] also functions as the DoD's CERT through its automated systems security incident support team, ASSIST" (Signal, March 1997, 69). ASSIST works closely with the other CERTs; however, "the military does not have a focal point to coordinate defensive efforts" (Signal, March 1997, 69).

United States Air Force (USAF). The USAF has several units dedicated to IW. There are some redundant efforts within the USAF because "organizationally, [it] has not come to grips with all of IW's ramifications. Some real leaps of faith have to made at the organizational level before [it] can exploit all capabilities" of IW (Braunberg, 1996, 65).

The Air Intelligence Agency (AIA) at Kelly Air Force Base, Texas, "investigates incidents of computer 'break-ins' at USAF facilities and sends teams out regularly to help with computer security" (Buchan, 1996, 9). The AIA employs defensive measures to bases around the world, including a automated security incident measurement system that detects unauthorized entry (Signal, July 1997, 60). The agency's IW Battlelab is tasked to "explore new ideas and foster innovative technologies to improve capabilities" in core competencies such as IW (Airman, May 1997).

The USAF IW Center (AFIWC), also at Kelly, is charged to "investigate and develop offensive and defensive information-based warfare and IW techniques" (Braunberg, 1996, 63). As a subordinate to AIA, AFIWC is "closely align(ed) with the intelligence community" (Fredericks, 1996, 9). It surveys bases to determine systems' vulnerabilities and supports the Computer Emergency Response Team (CERT) who "perform an on-line assessment to determine whether or not a site has been violated"

(Braunberg, 1996, 64; Fredericks, 1996, 9). The Team also provides on-site expertise to develop proactive countermeasures (Fredericks, 1996, 9). Ultimately, AFIWC is "charged with developing and maintaining general IW capabilities" (Grier, 1997, 24).

The 609th IW Squadron, at Shaw AFB, South Carolina, protects "vital computer networks in U.S. Central Command Air Operations Centers" (McKenna, 1996, 67). The squadron protects base information systems from attacks; in particular, they look more thoroughly at unclassified systems because "the classified networks are fairly secure" (O'Malley, 1997, 73). Even though it focuses mostly on defensive IW measures, it also studies offensive techniques" (Grier, 1997, 24; O'Malley, 1997, 73).

Finally, there are other Air Force organizations and personnel peripherally involved in areas affecting IW protection, to include operations, plans and programs, intelligence, and communications at both the headquarters and major command levels. They establish IW policy and guidance, e.g., Air Combat Command (ACC) is designated the major lead organization for USAF's command and control. The Air and Space Command and Control Agency reports directly to the ACC commander and is structured to integrate functions and to eliminate duplication of effort" (Signal, July 1997, 62).

United States Army. The primary Army IW unit is the Land IW Activity (LIWA) in Fort Belvoir, Virginia. LIWA "is a totally new organization" (Fredericks, 1996, 11) that "seeks to preserve and institutionalize the use of information operations in the Army's modernization plan" (Signal, July 1996, 51). LIWA focuses on team effort rather than a rigid, stove-piped organization to determine whether an enemy's IW efforts succeeds (Signal, July 1996, 52). LIWA coordinates its activities and monitors other

service/agency progress via an electronic network. "It is connected electronically with the national intelligence community, the Defense Department and joint and service IW centers and activities" (Signal, July 1996, 54). This connection enables the Army, like the Air Force and Navy, to "closely align its IW effort with the intelligence community" (Fredericks, 1996, 11). The LIWA also leads the IW-based Red Team that performs information attacks "to assess system vulnerabilities, to perform risk assessments, and to recommend solutions" (Robinson, July 1996, 47). The team has a Command and Control Protect Program that "identifies elements of IW as force multipliers, synchronizes current and planned IW activities, and supports education" (Robinson, July 1996, 48). Like the USAF, the Army has a CERT with very similar duties. Ultimately, LIWA is the Army's "organizational focal point for the integration of command and control into the table of organization and equipment Army" (Blount, 1996, 14).

United States Marine Corps. "Rather than create a separate IW organization, the Marines assign liaison officers to the other services' IW centers to benefit from their efforts" (Fredericks, 1996, 11). This joint approach ensures its defensive IW programs "operate in tight cooperation with the U.S. Navy" (Signal, July 1996, 61). It relies on the Army for psychological operations information and works closely with the LIWA for land-based operations (Signal, July 1996, 54) and there is a Marine Liaison Officer at the AFIWC (Signal, July 1996, 62). Finally, the Corps does have a new Commandant's Warfighting Laboratory that incorporates IW in its field actions (Signal, July 1996, 62).

United States Navy. The Navy has several organizations involved with IW. The Navy's IW Activity (NIWA) operates at the National Security Agency, the Office of

Naval Intelligence, and the Naval Research Lab, conducting research and development to support IW (Ackerman, 1996, 57). The Fleet IW Center (FIWC) is an "operational organization for supporting IW activities to include network security tests (Ackerman, 1996, 57; Whisenhunt, 1996, 6). The FIWC "serves as the link between the NIWA and the Atlantic and Pacific fleets" (Fredericks, 1996, 10). Ultimately, the Navy's FIWC focuses on short-term requirements while the NIWA focuses on the long-term (Fredericks, 1996, 10). The Navy also has both an IW council made up of high-level officials and a information and an electronic warfare systems program directorate that focuses on acquisition (Ackerman, 1996, 58).

Other Governmental Agencies. Not only the military is involved in IW activities. There are a plethora of other governmental agencies involved in IW, ranging from Presidentially-appointed commissions to the National Security Agency .

Commission on Critical Infrastructure Protection. Established in July 1996, the Commission on Critical Infrastructure Protection "weighs the implications of the (IW) threat. Members are considering whether it is a truly imminent danger or possibly an overhyped annoyance" (Grier, 1997, 22). The commission included "broad representation from federal departments and agencies and from the private sector" (PCCIP, 1997, 2). The commission looks "at vulnerabilities in broad commercial systems, including telecommunications nets, electrical power systems, supply systems, banking, and transportation" (Grier, 1997, 24). The commission published an extremely

thorough report in November 1997 on infrastructure protection that is cited throughout this study.

Information Warfare Commission. In July 1996, the President also established an IW commission to "sketch out a national IW or cyberwar defense plan against hackers by 1997" (Munro, 1996, 15). Recognizing that "formation of any nationwide defense plan will require an unprecedented degree of government-industry partnership", the commission includes both industry and governmental leaders.

The National Communication System. The National Communication System (NCS) coordinates national security and emergency preparedness communications planning for the whole federal government under direction from the National Security Council (Fredericks, 1996, 13). Working closely with the NCS, the National Security Telecommunications Advisory Committee (NSTAC) is comprised of industry leaders who advise the president on national security issues involving the information infrastructure (Fredericks, 1996, 13; Signal, March 1997, 70) and is "one of the single most important groups created to advise the President" (Whisenhunt, 1996, 18). Such a pool of industry leaders proves beneficial in future policy development and applications.

National Security Agency (NSA). The NSA is a critical expert in IW which "acts as the U.S. Government's focal point for cryptography, telecommunications security, and information systems security for national security systems" (MoA, 1995). It provides equipment such as the multilevel information system security initiative and firewalls to the military services (Robinson, July 1996, 49; Ackerman, 1996, 58). NSA

develops "'standards, techniques, systems and equipment' for classified information" (Fredericks, 1996, 12). The Computer Security Act of 1987 gave it responsibility for

> the protection of the National Information Infrastructure...to the National Institute of Standards and Technology and to the National Computer Center, which is part of NSA. (However) neither has the budget, power or expertise to effect real changes in the manner that computer systems vital to the national interest are protected, most importantly, they do not have the legal right to do so when those systems are owned and operated by private companies. (Buchan, 1996, 18)

Finally, the President's Commission on Critical Infrastructure Protection recommended that the NSA, along with the National Institute of Standards and Technology, provide "technical skills and expertise required to identify and evaluate vulnerabilities in the associated information networks and control systems" (PCCIP, 1997, 7).

U.S. Government Research Organizations. Research organizations also support IW efforts, especially for the military. A part of the Air Force Research Laboratory, Rome Laboratory "is investigating software and technologies that can better protect critical military and civil information systems and data from the growing threat of attacks" (McKenna, 1996, 65). The lab also works on 110 IW-related projects funded by such organizations as NSA and AFIWC (McKenna, 1996, 65). Rome Lab primarily focuses on integrity and availability of information, risk analysis and management, recovery, indications and warning, and intrusion (McKenna, 1996, 65-67). The National Defense University (NDU) is also integrally involved in IW research. Its Institute for Strategic Studies has published several key writings by experts such as Martin Libicki and David Alberts, and has developed an IW-based discipline for its Information

Resources Management College. In addition, the College has a School of IW and Strategy catered primarily for senior DoD officials (Cerjan & Clarke, 1994, 19). Finally, research is done by students at the services' intermediate and senior service schools, and at both the Air Force Institute of Technology and the Naval Post-Graduate School.

The Intelligence Community. The Intelligence Community is made up of numerous organizations, to include the Defense Investigative Agency, Federal Bureau of Investigation (FBI), National Security Agency, and the Central Intelligence Agency. Within this community, "there exists an acute appreciation of the enormous impact IW has on their efforts" (Fredericks, 1996, 12). Each has an office "to orchestrate IW related activities and satisfy the needs of their customer" (Fredericks, 1996, 12). The President's Commission on Critical Information Protection recently recommended a needed future IW nerve center that warns of electronic attack against both military and commercial targets fall under the auspices of the FBI (Seffers and Walsh, 1997, 27).

Indirect Governmental Organizations. There are other governmental agencies that have an indirect role in IW defensive measures. ARPA, DISA, and NSA have started a joint undertaking in the formation of the Information Systems Security Research Joint Technology Office (ISSR-JTO). Its functions include coordinating research efforts to avoid duplication, maintaining an exchange of technical expertise, and long range strategic planning for information systems security research (MoA, 1995). In 1994, the President established, via Presidential Decision Directive 29, the Security Policy Board to recommend security policies, procedures and practices. This directive also established the Security Policy Advisory Board to include civilian and non-governmental agencies in

security policy recommendations. However, the boards only advise and do not establish policy (Whisenhunt, 1996, 17-18). Finally, the U.S. National Intelligence Council studied IW and "has produced a classified report on known foreign efforts or plans to attack national data networks, such as the Defense Switched Network" (Grier, 1997, 23).

Private Sector. Many organizations in the private sector are involved in IW and national security. For example, there are several private sector research organizations involved in the IW effort. The Science Applications International Corporation created a Center for Information Strategy and Policy that "runs seminars and writes papers" on IW (Grier, 1997, 23). In addition, Rand Corporation "has carried out groundbreaking IW work" (Grier, 1997, 23). Without a doubt, "planning for IW requires cooperation between the defense sector and the commercial sector" (Berkowitz, 1995, 64). Attacks against organizations such as telecommunications and electric companies could seriously degrade our security. "Civilian information systems are prime candidates for attack" (Berkowitz, 1995, 64; PCCIP, 1997, 1). Private companies are working their own security problems, often replicating others' efforts. While some industry leaders have joined advisory boards, there is little coordination between the two sectors. Since both could be affected by IW, both must be integrally involved in the formulation of an overall national IW policy.

Arguments about the Need for an Overall National Strategy

Many experts in IW are recommending that America's leaders take a firm stand on IW. "The U.S. military still has no comprehensive and coordinated plan for

addressing security concerns or forging an overall defensive strategy" (O'Malley, 1997, 74). They argue the need to develop a coherent national policy and organizational structure to protect national interests from IW (Fredericks, 1996, 14; Wells, 1996, 7; Scott, October 28, 1996, 64). With so many organizations working separately on IW, it is clear America's leadership must formulate a coherent, total IW policy (Wells, 1996, 25).

> There is currently no national policy assigning responsibility for protecting the U.S. civilian sector from 'information attacks', defining the national interest in this area, or establishing priorities and resolving conflicts among potentially competing objectives. Absent such a national policy and a mechanism for implementing it, major problems will remain unsolved. (Buchan, 1996, 19)

Failing to provide this overall policy could have dire consequences for all, especially the military. "The United States must implement a national command and control (C2) protect policy for the national information infrastructure if any portion of the defense information infrastructure is to be considered reliable" (Robinson, July 1996, 50).

Another contributing factor to the need for a national policy is the U. S.' increased dependence on information technology. "National defense is becoming more dependent on complex information systems, which control civil finance and telecommunications networks and electricity-distribution grids as well as weapons systems, and the threat to these systems is growing" (McKenna, 1996, 65). The huge increase in military computer networks and information systems "has far outpaced the ability of the Defense Dept. and intelligence community to protect the integrity of many key systems, leaving the U.S. increasingly vulnerable" (Covault, 1997, 20). In addition, planning for defensive

IW is vital to national security. The failure of the nation to effectively develop a national IW strategy is due to a lack of precedent regarding this rapidly evolving area.

> [The] quest for a new military strategy is impeded by a lack of historical precedent, common definitions, joint and combined doctrine and guiding principles. Missing is a national-level policy that integrates and synchronizes military initiatives with complimentary actions of non-defense activities that also...play a role in IW. (Campen, July 1995, 67)

Finally, the "development of defensive (IW) strategies must be a broad and open government-industry effort" and partnership (Covault, 1997, 21). There is no doubt on the part of IW experts that the time has come for a national IW policy.

Business Process Reengineering (BPR) Basics

This review presented various organizations involved in IW and arguments for a national strategy. "IW requires new concepts within DoD because traditional approaches to military planning and command and control will not work for it" (Berkowitz, 1995). Is there a methodology that could solve the problems associated with current efforts in this untraditional way, while also developing an organizational means to effectively implement such solutions? BPR provides a unique methodology to generate solutions.

Definition of BPR. In their seminal work, Hammer and Champy define BPR as "the fundamental rethinking and radical redesign of business processes to achieve dramatic improvements in critical, contemporary measures of performance, such as cost, quality, service, and speed" (Hammer and Champy, 1994, 32). There is a need to start over, from scratch, "abandoning long-established procedures and looking afresh at work required" (Hammer & Champy, 1994, 31; Chang, 1994, 54; Moad, 1993, 22). Ultimately, the

organization must break rules and old traditions and abandon old assumptions of things like specialization (Hammer & Champy, 1994, 47). What exactly does this mean?

BPR is fundamental because it looks at the foundation of why an organization exists. By asking why they do what they do, a company looks at future capabilities: it "first determines what a company must do, then how to do it...It ignores what is and concentrates on what should be." (Hammer & Champy, 1994 33). BPR analyzes the business without constraints or a pre-determined mind set; it creates "new processes without the constraints of existing methods, people, technology, management systems, or organizational structures" (Chang, 1994, 54). It is a systematic methodology that enables businesses to completely reexamine its processes. "It is not a quick fix. Rather, it is a fundamentally new way to think about and structure organizations" (Linden, 1993, 10).

BPR delves down to the roots to achieve "massive improvement by radically redesigning the way a process operates, without regard to how things were done previously" (Chang, 1994, 55). Davenport argues it is "a radical strategy for change that must carefully consider complex implementation issues involving the workforce, technology, and organizational culture" (Hyde, 1995, 55). Leaders "think outside the box" when analyzing processes. BPR "aims at the total rethinking and redesign of organizations along processes, not functional lines" (Linden, 1993, 10). Starting with a clean sheet, it attacks paradigms to establish more efficient, effective processes (Dixon et al., 1994, 95; Halachmi, 1996, 12). "'Nothing is sacred' is the rule. Reengineering tears apart an organization, producing a new and different enterprise top to bottom and destroying notions of tasks, hierarchy, and business functions" (Ettorre, 1995, 13-14).

If successfully implemented, BPR results in dramatic improvements. It "demands blowing up the old and replacing it with something new." (Hammer &Champy, 1994, 34). BPR demands dramatic results of ten-fold increases in productivity versus ten percent as seen in total quality management: "new processes should ...move the organization from one performance curve to a higher one" (Halachmi, 1996, 12).

The key focus of BPR is on processes versus functions. "Organizations have been using reengineering to dramatically speed up work processes" (Mechling, 1994, 190). Looking at processes, "it is critical to select a broad, cross-functional process" or perspective (Chang, 1994, 56; Halachmi, 1996, 12). Ultimately, BPR questions if a "process is necessary and what it is intended to achieve" (Halachmi, 1996, 12). It provides a way to change organizational processes "from vertical/hierarchical or functional management to horizontal or process management" (Hyde, 1995, 57).

Principles of BPR. According to Hammer and Champy, the four principles of reengineering are: process orientation, ambition, rule-breaking, and creative use of information technology (Kim, 1994, 31). Other authors have added some principles to Hammer and Champy's simple list. Linden (1993) offers the following:

1. Substitute parallel for sequential process.
2. Bring 'downstream' information 'upstream'.
3. Provide a ngle point of contact to customers/suppliers when possible.
4. Capture information once, at the source.
5. Ensure a continuous flow of the 'main sequence: that chain of activities that adds value for the end user.
6. Organize around outcomes, not functions.
7. Don't 'pave cow paths'. First, redeign the process, then automate.
8. Every time a piece of paper enters the system, demand to know why. (Linden, 1993, 11-12)

Mechling (1994) reinforces Hammer and Champy's approach, but from a different angle.

> The order of magnitude goals of reengineering (tenfold not ten percent) require that the horizontal flow of work through the organization be redesigned, not just the vertical flow of management reporting. Work steps are typically eliminated, steps are executed in parallel rather than sequentially, jobs are broadened, and accountability is shifted from following the rules to producing results. (Mechling, 1994, 190)

Advantages of BPR. If developed and implemented properly, BPR offers numerous advantages to those willing to dedicate the necessary resources. Managers see "drastic increases in productivity after they redesign processes, and subsequently, the organization structure" (Kim, 1994, 34; Kim and Wolf, 1994, 82). BPR "eliminates unnecessary functions and control systems, introduces multi-disciplinary approaches to work, creates cross-boundary partnerships, reduces the number of managerial layers, and realigns the human resources systems to support the change" (Burstein, 1995, 53). It forces better problem-solving and enforces accountability; it "untangle(s) the confusing skeins of accountability and set(s) up processes for problem-solving" (Ettorre, 1995, 17). BPR de-layers bureaucracy and "collapses long, tedious sequences of sign-offs and hand-offs, shrinking the time it takes to make decisions and deliver services" (Linden, 1993, 10). This occurs regardless of the methodology used; "process analysis techniques vary, but generally result in the identification of repetitive, bureaucratic, and little value-added work tasks" (Spina, 1994, 27). Finally, "when successfully reengineered, the new processes eliminate constraints of geography and time" (Mechling, 1994, 190).

Disadvantages of BPR. Despite BPR's tremendous benefits, there are a few risks and/or disadvantages. BPR requires a process with breadth, which is often hard to determine. "Some reengineering efforts will fail if the process being reengineered does not have enough breadth" (Chang, 1994, 56). Ultimately, the main disadvantage is that they often fail. "Most reengineering projects are fraught with problems. In fact, Hammer estimates that "as many as 70% of so-called reengineering projects fail" (Moad, 1993, 22) while others guess a two-thirds failure rate (Horney and Koonce, 1995, 38). Such failure has alot to do with poor support from upper management sponsors (Horney and Koonce, 1995, 38). Spina (1994) offers the following reasons for BPR failure:

1. A structured methodology for BPR is not established and adhered to.
2. Consultants unfamiliar with commercial nuclear power business processes are retained to lead utility BPR efforts.
3. Process and information management are treated separately.
4. BPR changes are not implemented to full fruition.
(Spina, 1994, 26)

Most importantly, BPR often does not succeed because leaders fail to start from scratch. Huff (1992), Hammer (1990) and: Martin (1993) all agree that

> restructuring, reorganizing, and automation have not yielded the improvements that organizations had previously anticipated. In short, organizations must stop paving the cowpaths by using IT to mechanize old ways of doing business—they must obliterate processes and start over. (Kim and Wolf, 1994, 82)

In addition to the above, BPR is very difficult to implement. Grover et al. (1995) accomplished a meta-analysis to determine the determinants of BPR implementation problems. They grouped their problem areas into the following: management support problems, technological competence problems, process delineation problems, project

planning problems, project management problems, and change management problems. They found the "need for managing change was not recognized" ranked at the top of the list in terms of severity (Grover et al., 1995, 124). Second came management's short-term view and quick-fix mentality, with third place attributed to rigid hierarchical structures (Grover et al., 1995, 124). Ultimately, the most striking result of this research was that "four of the five (and six of the top ten) most severe implementation problems concern change management" (Grover et al., 1995, 124). Thus, "inability to manage organizational change...will most likely lead to project failure" (Grover at al., 1995, 136).

Successful Use of BPR in the Public Sector. Several authors point out that government organizations can successfully use BPR to dramatically improve their processes while others are more skeptical. They first argue the need for drastic change. "Unless government changes, it can no longer solve or meet the needs of today's America" (Kim and Wolf, 1994, 73). Likewise, "the potential rewards for reengineering are huge in any organization, but are especially so in the federal government with hundreds of millions of taxpayer dollars at stake" (Taylor, 1995, 96).

There are tremendous advantages for the public sector organization that uses BPR effectively. "Properly used, (BPR) offers public sector managers a new and formidable instrument for bringing fundamental, radical change to government" (Burstein, 1995, 54). Since most governmental organizations are familiar with total quality management, they may be at an advantage when using BPR. "Organizations that have already implemented quality improvement may be in a better position to introduce reengineering, which is a

more radical approach" (Chang, 1994, 55). BPR is necessary in some governmental endeavors. "Despite its risks, reengineering will at times be important, even essential, for the success of American government and society" (Mechling, 1994, 195).

Many aspects of government are being reengineered successfully (Linden, 1993, 12). The U.S. Customs Service "is now in the process of ...'managing by process', the heart of reengineering, that reduces management layers and emphasizes horizontal integration, breaking down barriers that have developed among functional components and different disciplines" (Burstein, 1995, 54). The U.S. Patent and Trade Office, "perhaps the largest repository of technical literature in the entire world", has successfully reengineered both their patent and trade, mark application processes (Taylor, 1995, 85-86). The U.S. Passport Service "has streamlined its processes; it used to take up to six weeks to get a passport renewed and now it can be done in a matter of hours" (Linden, 1993, 12). The former Bush administration DoD CIO is cited as "one of the best examples of reengineering" (Mechling, 1994, 192). Other examples of successful BPR efforts include the U.S. Navy Shipyards, welfare eligibility process in Merced, California, New York City, Ontario Ministry of Revenue ESPRIT Project, Iowa Communications Network, and Child Support in Massachusetts (Mechling, 1994, 190-191).

Despite the above advantages to public sector use of BPR, some factors inhibit its use. Many do not believe BPR can truly be used in the public sector. "For public sector leaders, there is more than a little concern that reengineering (or reinvention with technology, as it is called) may be a mirage, not a reachable reality" (Mechling, 1994, 189). Part of the problem inherent in public sector work is its political nature. "Existing

practices are politically sensitive" and may be unable to be reengineered (Manganelli and Klein, 1994, 45). Public agencies have difficulty identifying customers and "outside stakeholders whose support, consent, or noninterference are necessary for the success of BPR" (Halachmi, 1996, 16). In addition, the clean sheet of paper approach "ignores the existence of a business process' surrounding context" and environment (Manganelli and Klein, 1994, 46). The public sector's culture can deny the effective use of BPR.

"In the public sector, reengineering poses an approach versus avoidance dilemma: although public sector work flows cry out for radical redesign, public sector cultures (with checks and balances, limited powers, and executive oversight) make radical change risky" (Mechling, 1994, 190). The U.S. government, and its attendant bureaucracy, may be incapable of taking the dramatic steps necessary. "Some well-performing agencies are not going to get the permission to go through a radical reengineering either, even though ...their performance curve could greatly benefit from the effort" (Halachmi, 1996, 13).

> In changing government, the most successful approach is likely to involve lots of stakeholder participation to secure small but swift steps that, taken together, can accomplish significant change. The view of most practitioners is that pursuing the revolutionary ends of reengineering is almost always valuable, but pursuing the revolutionary means of reengineering is rarely so. (Mechling, 1994, 194)

Determinants for Using BPR to Develop National IW Strategy

There are several determinants to see if BPR is appropriate in the current IW environment. According to Chang (1994), the following should be considered

1. If the particular area is changing rapidly
2. If a process affects people in many different locations
3. If key suppliers and customers need to be involved
4. If there is a sense of urgency

5. If lengthy processes are involved.

As described above, there is dramatic and continuing change occurring in information technology of which IW itself is an outgrowth. Given the pervasive nature of IW and the numerous locations of organizations involved, the large geographical areas involved in IW clearly promote the use of BPR. Many experts argue above that the need for an overarching national IW strategy is critical. Using BPR can assist strategists in this very necessary development of a national policy. Lengthy processes are also prime candidates for realizing BPR's tremendous benefits. Defending against IW attacks seems to get more complex each day, as do the organizations charged to do so. The final determinant lies in the supplier-customer relationship. It is difficult to clearly define exactly who "the customer is" in IW, and thus it is difficult to include them in the BPR process. However, the suppliers who defend against IW are identified above, and their involvement is fundamentally necessary in order for the BPR process to be effective.

BPR as a Solution to Problems Occurring from a Lack of a National IW Policy

BPR can solve the problems, as described by several authors below, associated with the lack of a national IW policy. In particular, specialized initiatives, fragmented and redundant efforts, the lack of consensus on who is responsible for national IW strategy, and the lack of top level control of IW strategy have occurred as a result of the lack of a coherent plan. By developing a coherent plan to solve these problems, BPR can alleviate these problems. In addition, various recommendations ranging from single organizational responsibility to developing an interagency consortium have pointed to the need for a new way of doing business, which BPR can promote.

Need for a Coherent Plan. Regarding national IW policy, "there appears to be much fragmentation and a lack of a coherent integrated plan" (Whisenhunt, 1996, 21). With so many agencies with varying skills involved in the protection of national security, "sorting all this out should be a part of the national-level debate on the roles and missions of the military, the intelligence community, and the rest of the defense community" (Buchan, 1996, 14). Campen (1996) argues "missing is a national-level policy that integrates and synchronizes military initiatives with complementary actions of non-defense activities that also would play key roles in IW" (Campen, July 1996, 67). Particularly for the DoD, "no formal mechanism is yet in place to ensure the warfighters obtain a coordinated IW support package" (Fredericks, 1996, 8). Finally, a RAND study revealed "a badly needed multi-dimensional framework for sharpening near-term executive branch focus on the development of strategic IW policy" (Molander, 1996, 83). Solutions are beyond the control of any single service and, thus, a national-level plan is needed (Buchan, 1996, 2; Scott, 1996, 64). Because of increased dependence on many agencies and the private sector for information systems, security "will require a more integrated approach than the U.S. national security community has displayed so far" (Buchan, 1996, 10).

This lack of a coherent plan has caused several problems. There are specialized initiatives in which many governmental organizations have their own measures, policies, and organizational structures to defend against IW attacks. "Efforts appear specialized and non-complementary. There...(is) an absence of over-arching focus" (Scott, 1996, 60). Such separate policies/strategies are fragmented and not large enough in scope and application. "Some pieces of this strategy are currently in place, but they are fragmented

and there is no overarching directive from the Executive Branch which could serve as national policy" (Whisenhunt, 1996, 2). Military piecemeal efforts, while honorable, fail to successfully tackle the broad implications inherent in IW . "The current course of each service developing their own capability will not suffice to meet this threat" (Wells, 1996, 25). This fragmentation of current IW initiatives creates unnecessary redundancy.

> Efforts remain fragmented with little or no interaction between various factions. A national policy on IW would bring order out of chaos by establishing an accepted definition and assigning responsibilities for merging these efforts into coherent...national objectives and direction. (Whisenhunt, 1996, 15)

The lack of a national security strategy has also failed to produce an organization responsible for IW strategy and protection of national security. "Only crude assessments have been made of the risks and benefits of (IW). There is no consensus on which agency should lead...Further there are only hints of the top-level guidance that must pilot this unprecedented shift in national security policy" (Campen, June 1996, 47; Fredericks, 1996, 14; Wells, 1996, 7). Such a failure to cover all pertinent issues will seriously degrade our defensive abilities. "Defense against attacks on our information systems is a growing national security problem which will not be solved without an executive decision on what is to be done and who is in charge" (Whisenhunt, 1996, 1).

Finally, the lack of a coherent plan results directly from lack of senior leadership in the IW arena. Initiatives to create a national policy must come from the highest level of government; "absent strong emphasis from the Executive Branch and without an authoritative body to direct these multiple fragmented efforts into a complementary program, our abilities to carry out any strategy are severely degraded" (Whisenhunt,

1996, 22). By empowering an office or commission to address IW's complicated issues, the president provides oversight, guidance, and the necessary resources to succeed. "IW must be institutionalized and firmly, continually controlled from the very highest political authority" (Campen, June 1996, 48). Regarding the DoD's IW leadership, "a need exists for direct flag officer sponsorship to orchestrate joint IW policy" (Fredericks, 1996, 6).

There is no doubt from the above that a national, coherent plan is now critical to thwarting the various outcomes that have resulted from no national IW policy.

> What is desired by private citizens, private industry, and the government is an information network that is credible, available, secure, and survivable. This will only be achieved through the development of a national policy or program that has the mandated authority to integrate the multiple fragmented efforts that are on-going today. (Whisenhunt, 1996, 13)

When developing this plan, use of BPR looks at the complex processes to determine what is and is not value added. The focus on processes rather than the current organizational focus enables IW strategists to develop an effective national plan that negates the specialized and redundant efforts currently occurring. By focusing on processes, the BPR team equipped to formulate the national strategy can address who ideally needs to be in charge and what organizational needs are required to support a national approach.

Need for New Way of Doing and Organizing Business. Many of the experts cited throughout this chapter recognize the need for a new way of doing business regarding IW. "The new IW security paradigm requires functioning in nontraditional ways" (Robinson, 1995; Burstein, 1995, 52). A recent report by the President's Commission on Critical Infrastructure Protection stated that questions are arising on which agency should be in

charge and, "in particular, some in Congress wonder how the program should be coordinated with ongoing security operations" (Seffers and Walsh, 1997, 27). Current recommendations for organizing the IW business are presented below. However, these recommendations fail to address unique requirements of defending against IW. The old, functional way no longer applies. "Information warfare is a new way of doing business" (Whisenhunt, 1996, 3).

Authors have speculated on the kind of organizational structure needed for the U. S. to maintain its edge in IW. There is an evident need for the very top levels of the government to be integrally involved.

> An immediate and badly needed first step is the assignment of a focal point for federal government leadership in support of a coordinated U.S. response... (it) should be located in the Executive Office of the President, since only this level can the necessary interagency coordination of the large number of governmental organizations involved in such matters--and the necessary interactions with Congress—be carried out effectively...(it) should have responsibility for close coordination with industry, since the nation's information infrastructure is being developed almost exclusively by the (private) sector. Once established, this high-level leadership should immediately...initiat(e) and manag(e) a comprehensive review of national-level IW issues. (Molander, 1996, 90-91)

It is clear that leadership should come from the White House (Fredericks, 1996, 16). Some have recommended the private sector solution of a Chief Information Officer for the U.S. whose responsibilities would include information security (Anthes, 1995, 55).

There have also been recommendations to create a single organization dedicated solely to IW efforts. The Defense Science Board recommended that the ASD(C3I) pilot a new IW organization with its own chain of command (Signal, March 1997, 69-70). To decrease current redundant efforts, "the complexity of information operations may require

that service operations and/or agency operations be fully integrated to meet the challenges of (sophisticated) adversaries" (Wells, 1996, 11). Likewise, the U.S. could "produce a more specialized, differentiated set of skills and responsibilities (rather) than lumping quite disparate specialties together into an umbrella 'IW' organization" (Buchan, 1996, 14). We have a ready pool of IW experts, to include men and women from both the public and private sector, that could serve in an overall IW organization. Committees such as the "Security Policy Board, the NSTAC, and the Information Systems Security Committee have the requisite composition of government and private industry leaders to serve as a pool from which to establish a single authority to implement such a policy" (Whisenhunt, 1996, 22). Both the DSB and NSTAC have called for "organizing a special group to prepare government and commercial entities better for IW and to develop standards and policies" (Signal, March 1997, 69). Colonel Brain Fredericks, USA, recommends creating an organization similar to the National Communication System that works directly for the Vice President; the NCS should act as a "blueprint" for an integrated IW effort because it has links to all governmental agencies and is a "model for government-industry cooperation" (Fredericks, 1996, 14). Some authors have focused more directly on military organizational requirements. Clodfelter and Fawcett (1995) recommend a separate branch of the military. "If, indeed warfare does now consist of five mediums, one if which is information, then a rationale exists to create a branch of the military devoted to IW, much as the Air Force exists to conduct military operations in the air" (Clodfelter and Fawcett, 1995, 28). Rather than create a separate force, there could

be a joint command in which one service has overall oversight, similar to the current set-up at North American Aerospace Defense Command (Scott, 1996, 64; Wells, 1996, 24).

Because so many governmental agencies are involved in IW, some recommend an interagency approach. Since organizations such as NSA have a core of experts on information security while others such as the Federal Bureau of Investigation have the legal muscle to defend against IW, Buchan argues "some sort of interagency approach or even a public-private consortium that enlists the skills of industry experts might eventually prove adequate" (Buchan, 1996, 18). Such an interagency approach focuses on the overall governmental process, whereas others recommend leadership by a DoD agency over the services. "Designate a defense agency as the lead agency and define supporting roles for each service. [However] This would leave a void with respect to the non-defense portion of the national information environment" (Wells, 1996, 23-24). However, the President's Commission on Critical Infrastructure Protection recently stated that "no one person or organization can be in charge" (PCCIP, 1997, 5).

The use of BPR can help develop a new way of doing business by transforming an organization from a hierarchical to a vertical.

> In the case of IW, greater definitional rigor may be achieved by recognizing that what is truly distinctive about the Information age (and potentially revolutionary) is the emergence of a new form of organization. The functional hierarchy and centralized decision-making of the bureaucratic organization,... may be giving way to the shared global and situational awareness of...the information technology network. (Harknett, 1996, 94)

Thus, the emergence of information technology enables new ways of doing business, creating the need for new organizational structures "that parallel new ways of doing

business" (Chang, 1994, 55-56). By making the most effective use information technology's potential, BPR can address problems that traditional organizations are incapable of handling. "The pyramidal or triangular organizational concept is anachronistic and does not take advantage of current technology" (Gregory, 1994, 38).

For the military in particular, experts call for the kind of dramatic results only found when using and implementing BPR to change processes and organizational structures. "It is possible that the mission and organization of the U.S. military will need to change dramatically." (Wells, 1996, 13). A RAND study states, "traditional intelligence-gathering and analysis methods may be of limited use in meeting the strategic IW challenge" (Covault, 1997, 21; Molander, 1996, 88). Today's military is as pyramidal as in the 1950's; "armies must surely follow companies in 'delayering'" (Economist, June 10, 1995, 24). The DoD "cannot use traditional-style directives...to improve the ability to defend...against the IW threat" (Berkowitz, 1995, 65).

> With BPR, the government can effectively create a new organizational structure. BPR would assess and put aside non-value added activities and some of the redundant efforts described above. "A rank-, protocol- and process-conscious military must make significant structural changes to its doctrine, organization, and procedures and eliminate those echelons that contribute no added value to the flow of information" (Campen, July 1995, 69). BPR can ensure that the military is effectively organized to meet the ever-increasing threat of IW. Major Thomas E. Gregory proposes "a complete dismissal of the old pyramidal hierarchy. We should be organized, trained, equipped, and maintained exactly as we intend to fight". (Gregory, 39)

Using BPR, the military can totally revamp their existing organizational structure dedicated to current defense against IW in favor of a lean fighting force.

Implementation Issues when Using BPR in the Public Sector for IW National Policy

If the public sector hopes to take advantage of the tremendous opportunities afforded by BPR, the U.S. government's leaders must support some things necessary for BPR's successful implementation. They must ensure senior-level leaders are involved, effectively utilize technologies, take organizational culture into account, promote public and private sector cooperation, and, most importantly, develop a step-by-step process.

Involve Senior Management. Most of the BPR experts argue that "the most important factor is leadership, especially the ability to champion and protect risk-taskers dedicated to change within the organization" (Kim and Wolf, 83; Ettorre, 1995, 13-14; Taylor, 1995, 87). Radical innovation, a key concept behind BPR, "generally requires an initial openness to change by top management" (Dixon et al., 1994, 101). Such executive involvement must be present throughout the whole BPR process.

> With reengineering, senior executives must drive the effort from start to finish in order to achieve radical change in a short time. Reengineering involves sensitive structural change, job redesign, and sometimes job elimination. So senior management must be involved in the process and totally committed to it. (Chang, 1994, 55)

The importance of senior-level involvement cannot be overstated; "managerial attitude toward change is a critical factor in facilitating innovations" (Grover et al., 1995, 114; Hyde, 1995, 60; Leth, 1994, 559). William G. Stoddard, reengineering director at Andersen consulting, states,

> We won't take on a job if a prospective client doesn't have top management support in place that recognizes the need for reengineering, sees the opportunity for major benefits outweighing the cost and pain, and, lastly, has the will to do it. (Ettorre, 1995, 14)

With hands-on involvement, the senior manager ensures BPR is effectively implemented. For example, by dedicating necessary resources, he/she can "conduct a thorough pilot of the improved process before moving into full implementation" (Chang, 1994, 58).

In the IW environment, from the President all the way down to squadron commanders, leadership must be committed to the BPR-focused national policy development effort. Top management support is necessary to ensure required resources to the effort are committed.

> [Those currently] responsible for National Information Infrastructure security don't have necessary resource or expertise. Requires a top-down establishment of a national strategy and governing policies. In effect, it must have focused leadership and assigned responsibility for end-to-end consideration of all the needed and integrated components of a most complex national scheme. (Scott, 1996, 64)

For such a large process as defending against IW, the public sector in particular must accept a lengthy, costly process in order to correctly apply BPR principles. For example, the Air Force will need top management support to implement whatever role they acquire after the national strategy is implemented. "The Air Force will need inspired, innovative leaders , who are willing to renounce a 'business as usual' approach to strategic planning, if it is to sustain its competitive advantages over the long term" (Krepinevich, 1996, 19).

Effectively Utilize Information Technologies (IT). Coupled with Hammer and Champy, many authors argue the need for leaders to effectively use IT when harnessing the tremendous opportunities inherent in BPR. "IT is assuming the role of catalyst for shaping and restructuring the organization...(and) is an enabler of BPR" (Kim, 1994, 31). Thus, organizations must know how to take advantage of IT in order to truly benefit from

BPR. "Organizations that are successfully reengineering...use information resources well" (Caudle, 1995, 39). However, Grover et al. (1995) point out that

> information technology is an important enabler, but the reengineering project itself involves significant changes in areas such as roles and responsibilities, organizational structure, and shared values, and none of these can take place in an orderly fashion without careful planning and conscientious efforts to communicate with, educate, and motivate the affected employees. (Grover et al., 1995, 129)

Dixon et al. (1994) confirmed IT plays a role but it "was not the most critical enabler of reengineering efforts (they) studied" (Dixon et al., 1994, 105).

In the IW arena, the use of BPR can afford the government an opportunity to totally re-think its procurement and use of IT. "If the information revolution really is to have the impact on military affairs that its most ardent proponents suggest, fundamental changes will have to occur in the way the U. S. designs and acquires new systems" (Buchan, 1996, 6). General Ronald R. Fogelman, former USAF Chief of Staff, states, "Information systems have become strategic centers of gravity" (Covault, 1997, 20). He also believes that "dominating this information spectrum is going to be critical to military success in the future" (Davis, 1996, 31). As seen previously, IT also encourages new organizational structures. "Hierarchy is not a requirement of an effective high-tech command and control system" (Gregory, 1994, 40). By effectively managing IT, the U. S. can reduce the current redundant efforts already described.

> The system of systems might, eventually, save a lot of money by revealing and removing redundancies among the many systems...It will cross traditional service lines and require a willingness on the part of senior staff to face up to details normally left to techno-nerds (with which the American military is well-endowed). And it will mean changing the

organization of the military, and its doctrine and tactics. (Economist, June 10, 1995)

Take Organizational Culture into Account. When looking to develop and implement BPR, public sector leaders must recognize the importance of effectively managing both change and its effect on the organizational culture. "BPR requires a break with the organization's previous culture" (Halachmi, 1996, 14) which is often hard to initiate. Reengineering fails when "work places have dealt inadequately with the 'people variables' that are always at play in organizations in times of rapid change" (Horney and Koonce, 1995, 38). For the public sector, in particular, managing employees through the organizational and cultural change is unique. "The culture of one government agency must be synchronized with the culture of the civil service as a whole. A culture change... limited to one agency may not be possible or may jeopardize the ability of the agency to deal with counterpart units at other levels of government, (etc.)" (Halachmi, 1996, 15).

Training is a vital component of managing the organizational change inherent in BPR. "The requirement for training in new methods or general reskilling should not be underestimated" (Dixon et al., 1994, 105; Burstein, 1995, 54). Training was one of the reasons Texas Instruments (TI) was successful in several of its reengineering projects. "Besides creating classes that focused on new technologies, TI started internally marketing the benefits of reengineering to all concerned" (Moad, 1993, 23).

Need for Public/Private Sector Cooperation. A BPR assessment of organizations involved in IW would soon recognize the necessity for public/private sector cooperation. "To be successful, defensive IW must have the support of private industry" (Fredericks,

1996, 14; PCCIP, 1997, 7). Senator Bob Kerry states, "We need to strengthen our government-civil partnership to protect the national information infrastructure" (Munro, 1996, 15). A BPR analysis would see that "the separate world of the public and private sector have blurred as each has entered the service delivery environment of the other (Osborne and Gaebler, 1992)" (Kim and Wolf, 1994, 80; PCCIP, 1997, 7). However, both sectors have not fully grasped these blurred responsibilities. As described previously, both perform independent defensive IW measures. However, arising out of necessity, there has been increasing cooperation between the two. "Planning for IW requires cooperation between...(both) sectors" (Berkowitz, 1995, 64; PCCIP, 1997, 1).

While a necessity in the IW arena, such cooperation is relatively new for both sectors. "Operating in a partnership environment is not natural for government or industry. Many traditional attitudes do not work well here...for those willing to accept the challenge, however, working in such an environment is particularly rewarding" (Dunn, 1996, 37). Such an unnatural relationship may occur because, among other things, each has its own standards regarding success. "The private sector has a higher threshold of pain... The military wants 100 percent assurance that the communications it needs will get through. The private sector is perfectly willing to accept 90 percent" (Signal, February 1997, 23). In addition, both sectors will be held accountable for defensive IW measures. "Although 'protect and attack' actions will involve and impact the private sector, a national security, rather than private/commercial, perspective must dominate strategy and policy formulation" (Scott, 1996, 64).

Develop a Step-by-Step Process. When implementing BPR, the public sector must use a step-by-step process to guide its efforts toward effecting organizational change. "Systems and people resist change unless an organization addresses barriers methodically and systematically" (Horney and Koonce, 1995, 38). One can use various methodologies when reengineering processes. Most important is that "the reengineering effort must be straightforward and practical and feature simple implementation steps" (Leth, 1994, 564). The decision of which methodology you use "will have a great impact on whether or not you achieve your reengineering goals" (Manganelli and Klein, 1994, 47). A process management model developed for the public sector in particular will be introduced in Chapter III as a model for the analysis in Chapter IV. Below are other methodologies that offer some pertinent areas to consider which will be used to fill-in holes and provide support and reinforcement for the process management model.

Burstein (1995) offers five distinct phases: "readiness, planning, process redesign, transition, and implementation" in which "each phase, indeed every step, of reengineering (must be) carefully planned and sequenced" (Burstein, 1995, 54). Spina (1994), on the otherhand, offers a different five-phase approach: 1) Team formation and approach, 2) Documenting the existing process, 3) Analyzing the existing process, 4) Designing the improved process, and 5) Implementing the improved process (Spina, 1994, 26). Manganelli and Klein (1994) have their own take; the methodology should incorporate several important ingredients.

> First, it should develop a clear statement of corporate goals and strategies focused on satisfying the customer. Second, it should be process-oriented instead of function-oriented...Third, it should facilitate the identification

> of value-added and non-value added activities. Fourth, the methodology should lead to process visions that are performance breakthroughs implemented through radical, not incremental change. Fifth, it should develop an actionable implementation plan specifying tasks, resources, and timing of events. (Manganelli and Klein, 1994, 46-47)

Another model is the Competency-Alignment Process (CAP). Aligning the people and culture along the lines of BPR, Horney and Koonce (1995) proffer that

> competency alignment is a critical underpinning of successful BPR initiatives...reengineering should be targeted toward the specific goals of changing employee behaviors, processes, and systems at the 'transactional' level in an organization (the level at which day-to-day business is actually done. (Horney and Koonce, 1995, 38)

CAP, first developed by Coopers and Lybrand, "focuses on analyzing, understanding, and optimally deploying people in the reengineered organization, ensuring the best job fit for everyone" (Horney and Koonce, 1995, 38). CAP is in four stages, as shown:

1. Assess Stage
    A. Assess your people.
    B. Assess your Process.
    C. Determine necessary tasks.
    D. Determine necessary skills, abilities, and competencies.
    E. Create a Gap Analysis Matrix.
2. Deploy Stage
    A. Develop skill, ability, and competency profiles.
    B. Use the profiles to deploy people into reengineered jobs, to redeploy them else where in the organization, or to outplace them.
3. Learning Stage
    A. Create training and career development plans for employees.
    B. Explore the use of different approaches, formats, and methods.
    C. Outsource non-core functions.
4. Align Stage
    A. Align human resource systems, including recognition, compensation, and performance appraisal.
    B. Conduct pilot test.
    C. Review, assess, and revise as appropriate.

Coupled with the above processes (Burstein, 1995; Spina, 1994; Manganelli and Klein. 1994; and Horney and Koonce, 1995), Hyde's process management model described in Chapter III and applied in Chapter IV will provide a thorough framework by which the nation can use BPR to develop and implement a national IW strategy.

Answers to the problem statements

This chapter provided an extensive literature review that covered current organizations involved in IW, arguments about the need for national IW guidance, problems associated with the lack of such a policy, current expert solutions to such problems, and an introduction to the use of BPR. With the above information, Problem Statements 1-4 can be addressed. Given the BPR information discussed above, Problem Statement 5 will be analyzed when a step-by-step BPR-oriented methodology is applied to the development of a national IW strategy in Chapter IV.

1. How and by whom is the U.S. ensuring reliability and security of its information?

There are a variety of both governmental and non-governmental organizations involved in ensuring the reliability and security of information in the U. S. (e.g., see Berkowitz (1995), Buchan (1996), Fredericks (1996)). While there is communication among some of these entities, there are often specialized initiatives and redundant efforts on the their parts (e.g., see Scott (1996), Whisenhunt (1996)). These organizations are doing an effective job of defending against IW attacks. However, most experts agreed that in the near future much still needs to be done (e.g., see Molander (1996), Wells, (1996)).

2. Are current key organizations in IW, and their associated strategies, adequately defending the U.S. against the threat of IW? Current organizations involved in the defensive IW effort are adequately defending the U. S. against the current threat. However, most experts agreed that such defense has been more reactionary than proactive, and many of the current security efforts are minimal (e.g. see Buchan (1996), Whisenhunt 1996)). With the proliferation of IT occurring throughout the world at an unheard of pace, the threat will increase substantially as more and more countries and individuals have access (e.g., see Harley (1997), Szafranski (1995), Whisenhunt (1996)).

3. Is there a need for a national IW strategy to successfully defend against IW threats? The vast majority of experts recommend a national IW policy to guide efforts so the U. S. can be adequately prepared to successfully defend against the threat of IW in the near and far future (e.g., see Fredericks (1996), O'Malley (1997), Scott (1996), Wells (1996)). The original focus of this research effort was on the Air Force's role in IW. After reviewing the available literature on this topic, it quickly became apparent that most writers noted the lack of a national policy. For this very reason, the scope of this research broadened to include this critical area of a need for a national strategy.

4. What recommendations have been made regarding organizational means to address national IW strategic objectives? Numerous authors cited above have recommended various means to address and solve current problems associated with organizations involved in IW. Most have recognized the need for starting with commitment from the top leadership in primarily the public sector, but also the private

sector (e.g., see Anthes (1995), Molander (1996)) . Some have looked at creating a separate organization to tackle IW issues while others have recommended a separate branch of the military specifically (e.g., see Clodfelter and Faucett (1995), Wells (1996)). Others take a more realistic approach of creating a Joint Military Command or the development of an Interagency approach (e.g., see Buchan (1996), Scott (1996), Wells (1996)). Finally, some only see problems with the lack of legal precedent regarding IW and, thus, see legal reforms as a possible alternative (e.g., see Anthes (1995), Thomas (1997), Whisenhunt (1996)).

Summary

This chapter provided the background information needed to understand the importance and relevance of this research. A national policy, to include directives and organizational guidelines, regarding IW is imperative. Top leaders must be involved in this critical area in order for these individual, yet important, efforts to truly be totally effective toward defending the nation's security. The following chapter provides the methodology behind this research effort.

III. Methodology

Chapter Overview

This chapter describes the methodology and research design employed by this research effort. The research design seeks to answer the investigative questions presented in Chapter I. In general, this thesis uses qualitative research techniques, via an extensive literature review, to examine the first 4 questions. To address Question 5, the study then analyzes how the nation, utilizing a business process reengineering (BPR) approach, might develop an overall national information warfare (IW) strategy.

History of the Research Effort

This research originally began with a data collection of literature regarding the various Air Force roles and organizations involved in IW. It quickly became obvious that the other services, along with other governmental agencies, were also extensively involved in IW. In order to fully comprehend the nature of organizational activity in the IW realm, the data collection was expanded to include these additional organizations. Thus, the focus of the research changed dramatically and became much broader in scope.

After collecting and reading the articles about all of the organizations involved in IW, it became apparent that each of the organizations was operating without benefit of an overarching national policy and strategy. Several of the authors recommended various ways to remedy such disjointed efforts. However, the researcher concluded that, given the amount of redundant and sometimes inefficient efforts, coupled with the pervasive nature of IW, a more dramatic approach would be needed to effectively address this new

realm of warfare. Given the recent, and dramatic, success of recent BPR efforts, BPR was then evaluated to determine its applicability to the problem of a lack of national IW policy, strategy, and organizational structure. Based on the surveyed literature, a step-by-step process was developed to address this lack of a national strategy.

Research Design. An initial, preliminary search was conducted using the World Wide Web to see what information was available regarding information warfare. The World Wide Web provided good general information and there were several sites that had good bibliographies. In addition, the Web was an excellent medium to search Air University's catalog of research efforts regarding IW. In addition to Air University's articles, the researcher found additional scholarly articles via two on-line databases. The First Search database, which surveys over 12,500 journals in over 40 databases, was used for the initial search; in particular, ArticleFirst was used. A secondary search using OhioLink's Periodical Abstracts was then accomplished, which covers over 1,600 periodicals. Finally, the Air University Library published an invaluable and extensive bibliography over 60 pages long that included Internet sites, books, governmental documents, and periodical articles about information warfare which was also used.

The initial literature review was initially conducted only with the ArticlesFirst database but was later reinforced by another search using Periodicals Abstracts. Both searches were based on the following word and Boolean search terms: *information warfare, Air Force and information warfare, Air Force roles,* and *Air Force roles and information warfare.*

In addition to looking for additional information on Air Force units involved in IW, the second review broadened to include the other organizations and again searched both databases. The search was conducted based on the following words and Boolean searches: *Air Force Information Warfare Center, 609th Information Warfare Squadron, National Air Intelligence Center, Army and information warfare, Navy and information warfare, Marine Corps and information warfare, Information Warfare Executive Board, Defense Advanced Projects Research Agency, Defense Information Systems Agency, ISSR-JTO, Security Policy Board, Security Policy Advisory Board, National Security Agency, NSTAC, and the Information Warfare Commission.* In the hopes of finding as much information as possible on IW-based issues and the various organizations involved, word searches were also further expanded to include the following: *information terrorism, electronic terrorism, information security,* and *information protection.*

The third, and final, review focused on BPR. For this area, searches were again conducted using both databases. Word and Boolean searches included the following: *business process reengineering, process reengineering, reengineering,* and *business process reengineering and government.* With this final review, all data collection for the literature review in Chapter II was complete.

Analysis of BPR as a Tool for Developing National IW Strategy

An analysis that develops national IW strategies by incorporating ideas from both Hammer and Champy's reengineering process and other surveyed literature from Chapter II is analyzed in Chapter IV. The analysis provides a step-by-step process for the United States to effectively define a national IW strategy, policy, and the organizational structure

required to successfully implement such policies and strategies. Thus, the analysis answers the last research objective/question found in Chapter I: How might BPR be applied to accomplishing a national IW strategy? The analysis applies the step-by-step process described below, specifically using BPR to develop a national IW strategy.

Development and Use of a Step-by-Step Process. The analysis uses a step-by-step process based on Hyde's process management model (Hyde, 1995) to develop and plan for implementing national IW strategy. Various methodologies have already been described in Chapter II. Each has its own value but is generic in its application; thus, each will be used to fill-in some holes and support Hyde's model. However, as seen below, Hyde's model has several benefits regarding the use of BPR in developing and implementing national strategy. Hyde's process management model is much more extensive than the previously described models. It has been developed specifically for reengineering projects initiated by the government, and can thus be applied to the area of IW where the government is the main entity.

Hyde argues that "several phases or stages are generally discernible" in reengineering efforts:

1. Pre-planning Assessment: Is the organization ready?
    A. Assessing the Need for Change
        1) Political environment
        2) Organizational climate
        3) Labor management relations
        4) Is there a "window for change"?
    B. Pre-planning activities
        1) Commitment (and continuity) of top management
        2) Line up needed resources (internal and external)
        3) Does the organization understand the process (and pain) of change?

2. Strategic Plan: Is there a vision and clear targets?
    A. Select Steering Group/Body to Coordinate Change Efforts
    B. Selecting the Change Targets
        1) Link change targets to organization's strategic plan
        2) What are the change objectives?
        3) Has a "compelling case for change" been communicated?
    C. Preparing the Foundation
        1) Has a baseline or benchmark been set?
        2) Have "core" processes been identified?
        3) Have customers and stakeholders been targeted?
        4) Has a cross-functional team been established?
3. Process Re-design: Is there a change agent and a methodology?
    A. Internal Process Assessment
        1) Sub-Process Definition and Documentation
        2) Process Mapping/Flowcharting
        3) Identify Current Process and Performance Measurements
    B. Customer/Stakeholder Assessment
        1) Customer Value-Added Analysis
        2) Concept Engineering of Expectations
        3) Identify Customer Performance Measurements
    C. Process Visioning and Modeling
        1) Ideal Models
        2) Process Attributes and enablers
        3) Verification and Prototyping
4. Conversion and Integration: Is there an adequate transition strategy?
    A. "Conversion Requirements
        1) Business Process Changes
        2) Workforce and Job Changes
        3) Work Systems and Technology Changes
        4) Facilities and Communication Changes
    B. "Upskilling" of Workforce
        1) Converting Work Group into a Team
        2) Workforce Planning
        3) Training and Development for Process Work
    C. Develop Implementation Plan
5. Implementation: Is there a real commitment and an intelligent effort to change?
    A. Cultural Change
        1) Politics
        2) Communications
        3) Human Resources
        4) Labor Relations
        5) Technology
    B. Sustaining Management by Process. (Hyde, 1995, 61-68)

Each stage and its components will be addressed in detail during the analysis in Chapter IV. The analysis will use and refine Hyde's model in order to address and answer the particular focus of this research: the use BPR in developing and implementing national IW strategy. However, the reader must recognize that managing by process, is difficult in both the public and private sectors because 1) processes often cross functions, 2) processes often lie outside management systems, 3) managers aren't assigned to particular processes, 4) customers see differently from "insiders" in the organization, and 5) most communication is vertical rather than horizontal (Hyde, 1995, 58). Despite these difficulties, the process management model for reengineering will prove valuable in the development of a national IW strategy. "Process management lies at the core of what reengineering seeks to change most in bureaucratic organizations" (Hyde, 1995, 59).

Summary

This chapter provided the methodology by which this thesis addressed the problem statements introduced in Chapter I. A brief history of the research effort was described and the research design was detailed. The research design included a step-by-step process that was used in the analysis stage of this research. Specifically, Hyde's process management model served as the foundation for using BPR to develop the national IW policy. The application of this model to the IW arena is presented in Chapter IV.

IV. Results and Analysis

Developing a strategy of IW starts with serious, creative, and "color-outside-the-lines" thinking about current information technologies and ways in which they might be turned to strategic purpose to serve the national command authorities and military use.—George J. Stein (1995)

Chapter Overview

This chapter provides an analysis regarding the role of business process reengineering (BPR) in developing a national information warfare (IW) strategy. In particular, this chapter directly answers problem statement number five introduced in Chapter I: specifically, "How might BPR be applied to accomplishing a national IW strategy?". The first four problem statements were thoroughly addressed and answered in the literature review in Chapter II. Utilizing the process management model discussed in Chapter III, this chapter applies a step-by-step approach on how to use BPR when developing and implementing national IW strategy.

Use of BPR in Developing National IW Policy—A Step-by-Step Analysis

When developing the critically needed national IW strategy, the United States must look at the processes involved. The effort must first reengineer the current specialized, and often redundant, efforts described in Chapter II into whole processes. This lessens the need for a more bureaucratic approach which would require reconnecting fragmented activities (Hammer and Champy, 1994, 48). BPR enables the strategist to take a new look at what is currently being done and, with a "clean sheet of paper", design a whole new, improved process from scratch.

Given this unique approach, how exactly does one go about using the BPR process? The process management model described in Chapter III provides a valuable shell upon which to use BPR in the public sector. With the other methodologies described in Chapter II provide additional support, this analysis looks at and modifies this process management model. The analysis will use the following refined version of Hyde's process management model;

1. Form Teams
2. Determine Pre-planning Activities/Requirements
3. Assess Organization's Readiness
4. Develop Strategic Plan
5. Prepare the Foundation
6. Document the Existing Process
7. Re-design the Process
8. Develop a Conversion and Integration Strategy
9. Implement the Improved Process

For each stage of the process, the analysis first re-introduces the steps involved, as seem in Chapter III, and then examines those steps as applied toward the development of a national IW policy.

1. Form Teams. Hyde begins his methodology with a pre-planning assessment. However, this research focuses first on the formation of teams to start the process. Without teams to do the assessment, who will do it? Dedicated, full time teams must be established (e.g., see Chang (1994) and Spina (1994)). Hyde places the selection of a steering group/body to coordinate change efforts and the use of a cross-functional team under his second main activity, strategic planning, after the assessment phase. However, this analysis believes the team-building effort must occur at the very beginning.

When developing these teams for evaluating the current IW environment, the United States government, under the direction of a top leader such as the Vice President or Secretary of Defense, should choose both top leaders from the key organizations currently involved and experts in process reengineering as members of the Steering Committee. Recognizing that the BPR process is a lengthy one, members of the Steering Committee ideally should maintain their position throughout the process. As such, ideal members would probably be senior-level civilians in the DoD and other agencies, in addition to Vice Presidents of key industries such as telecommunications and banking.

The Steering Committee provides focus and direction for the Working Group. The Working Group should be composed of personnel directly involved in the current IW environment and, as much as possible, should represent each organization involved in the defensive IW effort. However, this could prove difficult given the transitory nature of most, especially military, employees. While members of the Working Group should be associated full-time with the BPR project, they should also continue to be fully aware of their organization's current IW efforts. When choosing members of the Working Group, it is critical to select individuals who can both "think outside the box" and put aside sensitivities about their organizations' involvement. Doing so will allow them to effectively analyze value-added and non-value added activities later on in the process. Finally, members of both the Steering Committee and Working Group must be well respected in their respective organizations so that, when the BPR process is complete, they can go back to the organization and sell the new process/organizational structure.

2. Determine Pre-planning Activities/Requirements. The newly formed teams should first determine pre-planning requirements. For Hyde, this was the second half of the pre-planning assessment, with assessing the need for change placed first in the section. However, this study believes the pre-planning activities should precede assessing the need for change. Particularly with the need for top management commitment, teams should ensure the pre-planning activities are present before proceeding any further with the process.

The United States has drastically reduced its budget over the past few years. Due to the politically popular goal of maintaining a balanced budget, funds will be scarce. Due to the critical need of an overall IW policy, top leaders in the government must be willing to dedicate the necessary time and resources necessary to tackle this unique challenge. Congressional and Presidential support is needed to ensure the necessary funds are committed so the teams can properly utilize BPR for developing a national IW strategy. External support from industry is also needed since it too will be affected by future change requirements. Finally, pre-planning activities must address the organizations' capability to change. Both the military and civil service of the government understand the pain of process change. The government as a whole has seen drastic funds cuts and dramatic personnel drawdowns since the late 1980's. Thus, given the current organizational culture, the United States government would be capable of adopting the necessary changes that result from the BPR-developed national IW policy.

3. Assess Organization's Readiness. After garnering top management commitment and the necessary resources, the team must assess whether or not the organization is ready and capable of change. The assessment primarily looks at the need for change in the political environment, organizational climate, labor management relations, and the "window for change". Included in this assessment of the organization's readiness is a portion of the Competency Alignment Process: 1) assess your people by determining their current skills, abilities and competencies, and 2) assess your processes to determine if there is a need for change by determining current tasks. However, before fully assessing your processes, the strategist must follow two other steps described later: develop a strategic plan and prepare the foundation.

For the IW realm, the criticality of assessing the readiness of the organizations currently involved in defensive IW cannot be overestimated. The political sensitivities and desire of the organizations to be involved in IW must be recognized. Regarding the military organizational climate, in particular, the services have been fighting over roles and responsibilities for years and IW will be no different. Because IW involves both the public and private sector, one must also analyze how potential change might affect labor management relations. Since most BPR efforts result in downsizing, labor-management relations may become strained if the change process is not effectively managed. Given the vast and ever-expanding capabilities of information technology, constant change has become commonplace and pervasive. Such a reality creates an almost permanent "window for change" when dealing with IW issues.

During the assessment of the United States' readiness for change in defensive IW measures, the teams must also look at the people involved in the processes. For example, they need to study the capabilities of the Army and Air Force Red Teams to see similarities and differences in abilities. They need to discern the growth and continuing advances in technology to decide what future personnel skills are necessary. Evaluating this will allow team members to see if personnel currently have the skills necessary for the future defense of the country against IW. They must also determine how information technology may supplant the need for manpower. Finally, the team must accomplish an initial assessment of exactly what current processes and their associated tasks are involved in the defense against IW. More will follow on this most critical part of the puzzle in Step 6 below.

4. Develop Strategic Plan. Next comes the strategic plan in which the teams determine if there is a vision and clear targets. The strategic plan should develop a clear statement of corporate goals and strategies which focuses on satisfying the customer (Manganelli and Klein, 1994, 46-47). Starting the development of this strategic plan is the selection of change targets. Next, the teams should link the change targets to the organization's overall strategic plan. When evaluating the change targets, the teams must also determine the change objectives. When analyzing the processes, the teams, along with top management, must ensure that a "compelling case for change" has been communicated. Finally, Hyde places the target of stakeholders and customers below under the heading "prepare the foundation". However, this analysis recommends that this

be placed under strategic planning, along with determining the change targets. This recommendation stems from the reality that the majority of change targets often relate to the organization's desire to improve its relationship with customers and stakeholders.

Chapter II provided an in-depth review of organizations currently involved in IW. The first change targets selected for analysis should be these organizations and how they currently affect the nation's defense against IW attacks. By focusing on the organizations involved, the United States can reduce redundancies and functional, independent efforts. Change targets should also include discerning the need for an effective means of ensuring public/private sector cooperation. A look at these particular change targets would analyze existing technologies and the process by which the country can ensure compatibilities.

Chapter II also showed a compelling case for the need of an overarching national policy regarding IW. The strategic plan formally initiates the development of such a policy by developing clear goals and objectives on national defensive IW policy measures. The strategic plan would provide a vision of where the United States wants to go with its current BPR initiative regarding IW. Such a vision might include a reference to ensuring the security of communications systems against IW attacks. Objectives to achieve such a vision/goal might include cutting redundant efforts and, thus personnel required, by 25%. The strategic plan would also address for the first time what and who exactly will be involved in the change process, e.g., what organizations and what leadership support. Finally, this study proposes that identifying the stakeholders, namely the American citizen and both the public and private sectors, who, in this case, also become the customers, as a necessary step in strategic planning. By identifying the

stakeholders as the American public, team members now have accountability not only for ensuring that the future IW policy is effective but also that taxpayers moneys are effectively managed.

5. Prepare the Foundation. Hyde includes this step in the strategic planning phase, along with selecting the change targets. However, while this may be a part of the strategic planning, preparing the foundation involves certain actions such as obtaining the necessary resources while strategic planning is not as tangible until implemented later. The start of the preparation is determining a baseline or benchmark. Next one must further delve into the processes discovered previously to discern whether "core" processes have been identified. Manganelli and Klein (1994) reinforce this perspective by placing emphasis on how the BPR analysis should be process-oriented instead of function-oriented. Hyde's last two sections of this phase include targeting customers and stakeholders and establishing a cross-functional team, which have already been incorporated in earlier stages.

Concerning defensive IW, it would be difficult to set clear, distinct baselines or benchmarks because the field expands and changes rapidly. IW is a new, evolving area and performance measurements still need to be developed. However, benchmarks can be established regarding the development of organizational structures and responses to attacks. For example, the team could develop benchmarks around the implementation of the newly developed processes. They could use Gantt charts to monitor progress of the plan's implementation. In addition, a benchmark concerning decreased redundancies and

specialized initiatives could be set; the team could cut the redundancies and then evaluate the cost savings associated with the changes. Finally, the teams need to take another look at the core processes involved before going to the next, and perhaps most complex, lengthy phase. They would ensure they have fully captured existing processes before delving into the fine detail of the process analysis in the next stage.

6. Document and Analyze the Existing Process. Hyde's next phase is "Process Re-Design". However, for this study, the analysis prefers Spina's stage of "Documenting and Analyzing the Existing Process". This stage should primarily facilitate the identification of value-added and non-value added activities. (Manganelli and Klein, 1994, 46-47). It should also conduct Hyde's Internal Process Assessment, which includes sub-process definition/documentation, process mapping/flowcharting, and current process and performance measurements identification. Since customers and stakeholders have been identified and targeted above, next comes Hyde's customer/stakeholder assessment, to include customer value-added analysis, concept engineering of expectations, and identification of customer performance measurements. Hyde then places process visioning and modeling in this phase. However, this research places this critical portion of process review and re-design in Spina's "Re-Design the Processes" below.

When analyzing current IW processes, the teams should first review available literature to determine exactly who is involved and how. The review in Chapter II, along with several cited references, provides a good starting point. The teams must also look in-depth at the exact role of each organization and its charge regarding IW. During this

stage, the teams should quickly recognize value-added and non-value added processes, especially where the military services are involved. For example, during the research for this study, it quickly became apparent that there are several redundant efforts regarding the military's use of CERTs. An analysis of these CERTS would prove valuable in determining what is and is not value-added. The same could be said regarding an analysis of current intelligence efforts in the IW arena.

During this analysis, the teams should also look at all the sub-processes involved and map/flowchart them to see relationships among current processes. For example, how are operational and exercise plans affected by potentially changed processes for defensive IW. Because IW is such a broad category encompassing everything from COMSEC to network security, changing how the United States defends against IW can have pervasive effects on various plans and programs. Given the core and sub-processes, the team must then map or flowchart the "big picture". Doing so will enable the team to analyze and later reengineer processes.

The teams should also document current performance measurements and determine if they are an accurate reflection of defensive needs. For example, the team could use the number of computer intrusions detected as a measure; if more detections are found after the improved process, the BPR effort was not in vain. The team could also look at moneys saved as a result of streamlined efforts developed during the BPR initiative. Finally, the team could look at response times of the CERTS to see if they've improved after the new processes and organizations are implemented.

During this stage, the teams should further evaluate the customer/stakeholder. Will taxpayers allow Congress to commit the funds necessary to support the lengthy and politically sensitive BPR process? Do American citizens appreciate the need for a totally new way of doing business when developing national IW strategy? What does the public, along with both sectors, expect as an outcome of such an extensive, expensive, time-intensive effort? Finally, how will the teams measure their satisfaction with the outcome?

7. Re-design the Process. After documenting the existing processes, Spina's next step involves designing the improved process (Spina, 1994, 26). Incorporated into this part of the process is Hyde's "Process Visioning and Modeling" phase. The goal of this step is for the methodology to lead to process visions that are performance breakthroughs implemented through radical, not incremental change. (Manganelli and Klein, 1994, 46-47). During the redesign stage, the teams provide a process visioning by thinking outside the box for alternative, more value-added processes. They model these ideal processes and look at process attributes and enablers. During this stage, the teams also implement the two steps of the Competency Alignment Process: first, assess your people by determining the necessary (versus current from step 3) skills, abilities and competencies, and, second, assess your process by also determining necessary (again, versus current as seen in step 3) tasks.

After redesigning existing processes and revamping the personnel attributes necessary to implement them, the teams then verify the pragmatism of the new processes and test out the new system through prototyping. This stage is the most complex and difficult.

As seen in Chapter II, current defensive IW efforts cross numerous functional areas and there are perhaps "too-many-to-count" processes. In assessing these processes, the teams should look at value-added versus nonvalue-added efforts under the charge of significantly streamlining current efforts. For example, the teams would evaluate current intelligence gathering methods used by the intelligence community. Are the FBI, CIA, and the various military services' special investigations units fighting the same battles on the same turf? Are the military Computer Emergency Response Teams (CERTs) necessarily divided according to each service? Could these processes be streamlined to avoid redundant or specialized initiatives? Redesigning the core and sub-processes involved in defense against IW will be lengthy. Thinking "outside the box" is often difficult and it would be hard to completely understand the personnel skill changers that will be required with the change.

After re-designing the defensive IW processes and organizational structure to support them, the teams need to verify their new processes via a prototype. They would need to test the new system on one particular organization, for example the Air Force. The teams, for instance, may take away all service-specific CERTs but wouldn't accomplish such an overwhelming task immediately; such an effort would need to occur gradually. Perhaps they would form a DoD CERT and then disband the Air Force's CERT first, and so on. By evaluating how the Air force adjusts to the change, the teams

could better manage other organizational change requirements. The same prototyping process could be used to decrease redundant intelligence gathering efforts.

8. Develop a Conversion and Integration Strategy. After redesigning the process and testing a few of the areas via prototypes, the teams must develop an adequate transition strategy, to include conversion and integration. The teams must evaluate such conversion requirements as business process changes, workforce and job changes, work systems and technology changes, and facilities and communication changes. They must also address how to effect the necessary changes in personnel skills. This "upskilling" of the workforce, as Hyde calls it, involves workforce planning, to include "changing work assignments, retraining employees, and realigning organizational structures" (Hyde, 1995, 67).

Incorporated into this stage is the Competency Alignment Process (CAP) model's recommendation to develop worker skills, abilities, and competency profiles. In addition, the teams will need to create the training and career-development plan for employees and align recognition, compensation, and performance appraisals, as again recommended by CAP. Hyde also realizes the necessity for training and development plans for process work. By realigning such skills, teams look at what skills are necessary to keep within the government and can thus outsource non-core functions, as recommended by CAP.

Finally, after addressing the conversion and integration needs, the teams must develop an extensive implementation plan. Teams "should develop an actionable implementation plan specifying tasks, resources, and timing of events" (Manganelli and

Klein, 1994, 46-47). Hyde points out the necessity for starting the implementation plan early during the redesign phase: "the biggest problem is starting the implementation process too late. The larger the change implications, the greater the necessity to form an implementation team that overlaps the redesign phase" (Hyde, 1995, 68).

The conversion and integration of the redesigned defensive IW strategic processes into the public sector will be extremely difficult and lengthy. There are many "institutional problems [that] extend to career paths within the military as well as to basic organizational structure" (Buchan, 1996, 7). The implementation of the national IW strategy must first look at how the business itself has changed. The policy must be flexible enough to adapt to the ever changing and increasing threat of IW. Given the use of BPR in developing the national strategy, the business processes for defending against IW will likely become more horizontal and flat versus the taller, vertical organizational traditional structure. Locations of organizations to implement the process will have to be decided, which obviously has political implications due to the potential increase in jobs and local income for the locations chosen. The teams will also have to look toward more compatible information systems not just within the Department of Defense but across both the public and private sectors. Likewise, converting to the new national focus will cause changes in how organizations currently communicate and, probably, the chain of command itself.

The most important part of this phase will be how successful the United States is in handling the personnel requirements for implementing the new national IW strategy. The conversion and integration plan will have to address the drastic change in personnel

requirements. There will be new skills and abilities in understanding the new, better processes. Such new skills will need to be taught to either personnel from existing organizations or personnel from a completely new organization, depending on how the teams organize the new effort. After addressing the above issues regarding conversion and integration, the teams must develop a thorough implementation plan that addresses how exactly they will implement the desired, necessary personnel, location, and organizational changes.

9. Implement the Improved Process. All of the experts end their BPR methodologies with the implementation of the improved process (Spina, 1994, 26). Regarding implementation of the improved process, Hyde asks, "Is there a real commitment and an intelligent effort to change?" (Hyde, 1995, 61). During implementation, the teams must look at the cultural changes that will occur as a necessary result of the improved processes, to include areas such as politics, communications, and human resources. As CAP suggests, during implementation, the United States will need to deploy people into reengineered jobs or redeploy them elsewhere. The teams must also recognize the value of good labor relations and the reality that many employees will be initially resistant to change. Likewise, as discussed in Chapter II, the teams must ensure the newly implemented process takes advantage of the tremendous potential seen in effectively utilizing information technology. Finally, Hyde recommends sustaining the management by process mentality when dealing with future issues. During this final

phase, CAP recommends that the leadership must continually review, assess, and revise the strategy as appropriate.

During the implementation phase, the United States government, along with the private sector, must monitor and react to several issues. The most pervasive issue will be promoting cultural change as necessary to successfully implement the new policy. The implementation of the new policy will cause disruption to organizations currently involved in defensive IW measures. For example, if the reengineered processes disbanded the service-specific IW centers in favor of a large DoD IW center, the services would have to either separate personnel at their centers or find new jobs for them. Thus, as the inevitable streamlining occurs, politicians will face angry constituents who have lost their jobs as a result of the new plan. There may be continued fighting among the services on who should have gotten the job. While one of the goals of the initiative is to increase communications, some personnel may, in an effort to thwart the change, fail to share vital information. As seen above, the changed process will drastically affect the use of human resources and even the best laid out plans cannot alleviate the potential pain of such a tremendous change effort. Thus, labor relations will be affected and personnel involved may demand more compensation for having to cooperate.

In addition to managing personnel changes, organizations involved will have to accept some kind of standard regarding the use of information technology in order to promote compatibility among separate systems. For example, the FBI system may not be compatible with the DoD system. Such continued incompatibility reduces data sharing and inhibits the improved processes from being fully realized. Finally, implementation of

the BPR-improved process needs to ensure that the processes are re-addressed as needed so that the nation continues to be prepared to effectively defend against IW attacks.

Summary

This chapter provided an analysis of the use of BPR against the current problem of the need for an overarching national defensive IW policy. The chapter refined and analyzed Hyde's process management model described in Chapter III, coupled with various steps of other methodologies discussed in Chapter II. These steps were developed and defended as necessary to successfully use BPR for developing a national IW strategy and the organizational structure required to implement it. The next, and final, chapter evaluates answers to the five problem statements introduced in Chapter I.

V. Conclusion

Chapter Overview

This thesis has analyzed the need for an overarching national information warfare (IW) policy in the United States and offered business process reengineering (BPR) as a method by which to develop that policy and implement it. This chapter concludes the analysis with a discussion of the study's significance and limitations. Finally, the chapter ends recommendations on possible areas for further research and concluding remarks.

Significance of This Research Effort

Currently, there is no national policy or guideline regarding the extremely critical area of defensive IW. While many experts in the field have argued the need for such an overall policy, most have only offered a cursory glance at a potential national policy and its subsequent organizational requirements. In today's cost-reducing environment, the U. S. can no longer afford current redundant efforts where the military services and other governmental agencies are, for the most part, pursuing their own answers to IW threats.

Ultimately, this research has demonstrated the need for an overall national focus and public/private sector cooperation to successfully defend against IW. The recent report by the President's Commission on Critical Infrastructure Protection confirms this study's conclusions. The problems associated with the lack of a national IW policy must be addressed as soon as possible. The lack of a coherent plan to thwart IW attacks will create significant problems in the near future (see PCCIP, 1997). Coupled with the PCCIP's recommendations, the recent visibility of IW's potential harm leaves no room

for ignorance on both the government and private sector's parts. Both sectors know that IW poses a significant problem for national security and that the threat is going to grow exponentially as technology expands enemy capabilities. The lack of a national plan to address these issues will only encourage future attacks since there is no effective, planned deterrent. Even if BPR is not used in this area and no subsequent changes to organizational structures occur, as recommended by this study, a national policy is still needed to provide general guidance to those organizations involved in IW. Failure to develop a national policy will ultimately be a failure successfully defend the nation against IW attacks.

United States leaders must focus on changing current organizational structures given the problems found during this study. The current organizational set up will not successfully meet the future demands of IW. Unlike conventional warfare, IW demands a new means of defense. Current organizations are doing an effective job, but the threat continues to grow and organizations are currently ill-equipped to handle future threats (see PCCIP, 1997). By changing from a stove-piped horizontal organizational structure to a more flexible, vertical, information-sharing structure, both the government and private sector can better prepare against IW attacks. Failure to properly structure organizations involved in IW may result in future inability to effectively deter IW threats.

Many experts have recommended solutions to the various problems occurring in the IW arena. Unlike these previous studies, this study applies an actual methodology for the first time to thoroughly develop a national policy and deal with such issues as personnel requirements. As such, it offers a unique perspective to a large, complex

problem area that must be solved if the country is to successfully thwart IW attacks in the future. In addition, these expert recommendations fail to recognize the unique environment within which IW operates. This research points to the need for a shift of paradigms toward a process focus, rather than the functional views offered by the experts. A completely new, unconventional way of waging warfare, IW demands a totally new way of doing business. While there are certainly other methodologies available such as total quality management, BPR offers a proven methodology to dramatically alter current processes. While the recommended methodology can be vastly improved, it does provide a good starting point where none currently exists. If implemented correctly according to true, process-oriented BPR concepts, the pursuit of a national IW policy will have lasting, positive effects on the future defense of the country.

However, while BPR is indeed a valuable methodology for vastly improving broken processes, its use in the IW realm will be limited at best. This is due to the political reality and sensitivities of the current environment. Each branch of the service, along with the other agencies described in Chapter 2, has its own piece of the IW pie and is unlikely give it up. Likewise, the ability of the government to actually create an effective steering committee and full-time working group is doubtful due to limited, continually decreasing funding. Finally, the President's Commission on Critical Infrastructure recommends a less radical approach than what BPR offers. In their 5 November 1997 report, the Commission states that "protection of our infrastructures will not be accomplished by a big federal project. It will require continuous attention and incremental improvement for the foreseeable future" (PCCIP, 1997, 5). While this

approach is more realistic than the one offered by this thesis, some key elements of BPR such as a process focus and value-added versus non-value-added should not be ignored.

Limitations of this Research

Due to the subjective nature of this research, there are many limitations. Because this study focused only on defensive measures, the analysis only covered half of the IW equation. The research was purposely limited to defensive problem areas and, thus, failed to thoroughly address offensive IW. Because the research was qualitative, there is no empirical data (i.e. on redundant efforts) to back up the application of BPR to the IW arena. The rapidly changing environment inherent in IW limits the applicability of this research to near-term application. In addition, due to the incredible complexity involved in defending against IW attacks, it is difficult to fully investigate every defensive effort in detail; failure to fully understand every process may preclude the effective use of BPR. Finally, both defensive and offensive IW involves some highly classified information that prohibits full knowledge of the extent of the problem and its attendant solutions.

Recommendations for Further Research

This study was an exploration of the organizations involved and the problems associated with the current means by which the United States defends against information warfare attacks. After proving the need for an overarching national defensive policy, this thesis effort recommended utilizing a business process reengineering approach to effect this change. The analysis of a step-by-step approach was only cursory. Therefore, a more thorough discussion and subsequent research to support such a methodology is

needed. In addition, a more in-depth study and comparison of exactly what current organizations do in defensive IW operations would provide valuable, specific evidence of redundancies. Finally, business process reengineering is not the only method by which the United States can effectively develop a national strategy, although this study certainly pointed to its viable use. There are additional management theories such a quality management that could be studied. Finally, an analysis of business process reengineering efforts in the Department of Defense could either prove or disprove its usefulness in the military environment.

Conclusions

This research paved the way for the United States to successfully develop and implement a national defensive information warfare strategy. Business process reengineering can effect positive change toward a better, less wasteful way of defending the United States against information warfare attacks. The United States must take the need for a national IW strategy seriously before it is too late. The President's Commission on Critical Infrastructure Protection is "quite convinced that our vulnerabilities are increasing steadily while the costs associated with an effective attack continue to drop...We should attend to our critical foundations before the storm arrives, not after" (PCCIP, 1997, 6).

Bibliography

Ackerman, Robert K. "Navy Doctrine, Systems Face Information Warfare Makeover." Signal, July 1996, 57-60.

Aldrich, Richard W. "The International Legal Implications of Information Warfare." Airpower Journal, Fall 1996, X, No. 3, 99-110.

Anthes, Gary H. "New Laws Sought for Info Warfare." Computerworld, June 5, 1995, 55.

Berkowitz, Bruce D. "Warfare in the Information Age." Issues in Science and Technology, Fall 1995, 59-66.

Blount, Kerry A. "Wrestling With Information Warfare's 'Dark Side'." Army, February 1996, 9-15.

Braunberg, Andrew C. "Air Force Pursues Two-Sided Information Warfare Strategy." Signal, July 1996, 63-65.

Buchan, Glenn. "Information War and the Air Force: Wave of the Future? Current Fad?" Rand Corporation, March 1996, 1-20.

Burstein, Carolyn. "Introducing Reengineering to Government" The Public Manager, Spring 1995, 52-54.

Campen, Alan D. "Rush to Information-Based Warfare Gambles With National Security." Signal, July 1995, pp. 67-69.

Campen, Alan D. "Assessments Necessary in Coming to Terms With Information Warfare." Signal, June 1996, 47-49.

Caudle, Sharon. "Reengineering and Information Resources Management." The Public Manager, Winter 1994/1995, 39-42.

Cerjan, Paul G. and Robert B. Clark. "NDU Develops a Discipline in Information-Based Warfare." Army, May 1994, 18-19.

Chang, Richard Y. "Improve Processes, Reengineer Them, or Both?" Training and Development, March 1994, 54-58.

Clodfelter, Mark and John M. Fawcett, Jr. "The RMA and Air Force Roles, Missions, and Doctrine." Parameters, Summer 1995, 23-29.

Corcoran, Elizabeth. "Computing's Controversial Patron." Science, 260, 2 April 1993, 20-22.

Coroalles, Anthony M. "On War in the Information Age: A Conversation with Carl von Clausewitz." Army, May 1996, 24-34.

Covalt, Craig. "Cyber Threat Challenges Intelligence Capability." Aviation Week & Space Technology, February 10, 1997, 20-21.

Davis, Harry J. "Developing Air Force Information Warfare Operational Doctrine: The Crawl-Walk-Run Approach." Air War College, Air University Press, 1 April 1996, 1-41.

Defense Science Board. "Report of the Defense Science Board Task Force on Information Warfare-Defense." Office of the Under Secretary of Defense for Acquisition and Technology, November 1996, 1-16.

"Digital Formats Complicate Information Security Tasks." Signal, February 1997, 21-23.

Dixon, J. Robb, Peter Arnold, Janelle Heineke, Jay S. Kim and Paul Mulligan. "Business Process Reengineering: Improving in New Strategic Directions." California Management Review, Summer 1994, 93-108.

Dunn, Richard L. "DARPA turns to 'other transactions'." Aerospace America, October 1996, 33-37.

Earl, Michael J., Jeffrey L. Sampler and James E. Short. "Strategies for Business Process Reengineering: Evidence From Field Studies." Journal of Management Information Systems, 12, No. 1, Summer 1995, 31-56.

Ettore, Barbara. "Reengineering Tales From the Front." Management Review, January 1995, 13-18.

Franks, Frederick M., Jr. "Winning the Information War: Evolution and Revolution." Vital Speeches of the Day, 453-458.

Fredericks, Brian and Robert F. Minehart, Jr. "Information Warfare: the Organizational Dimension." U.S. Army War College, 7 February 1996, 1-26.

Gregory, Thomas E. "The Cybernetic Design: Maneuver Warfare Organization for the Information Age." Marine Corps Gazette, December 1994, 38-40.

Grier, Peter. "At War With Sweepers, Sniffers, Trapdoors, and Worms." Air Force Magazine, March 1997, 21-24.

Grover, Varun, Seung Ryul Jeong, William J. Kettinger, and James T. C. Teng. "The Implementation of Business Process Reengineering." Journal of Management Information Systems, 12, No. 1, Summer 1995, 109-144.

Halachmi, Arie. "Business Process Reengineering in the Public Sector: Trying to Get Another Frog to Fly?" National Productivity Review, Summer 1996, 9-18.

Hammer, Michael and James Champy. Reengineering the Corporation: A Manifesto for Business Revolution. Harper Business, New York, 1994.

Harknett, Richard J. "Information Warfare and Deterrence." Parameters, Autumn 1996, 93-107.

Harley, Jeffrey A. "Information, Technology, and the Center of Gravity." Naval War College Review, Winter 1997, L, No. 1, 66-87.

Horney, Nicholas F. and Richard Koonce. "The Missing Piece in Reengineering." Training and Development, December 1995, 37-43.

Hyde, A. C. "A Primer on Process Reengineering." The Public Manager, Spring 1995, 55-68.

"Industry, Government Pursue Data Security Clearinghouse: Alleviating Information Warfare Threats Spins Up Innovative Organizational Plan." Signal, March 1997, 69-71.

"Information Officers Disseminate, Protect Intelligence Data." Signal, July 1997, 59-62.

"Information Warfare Battlelab Stands Up." Airman, May 1997, 10.

Jensen, Owen E. "Information Warfare: Principles of Third Wave Warfare." Airpower Journal, Winter 1994, VIII, No. 4, 35-43.

Kim, Bonn-Oh. "Business Process Reengineering: Building a Cross-Functional Information Architecture." Journal of Systems Management, December 1994, 30-35.

Kim, Pan Suk and Lance W. Wolff. "Improving Government Performance: Public Management Reform and the National Performance Review." Public Productivity and Management Review, 18, No. 1, Fall 1994, 73-87.

Krepinevich, Andrew F. "The Air Force of 2016." Center for Strategic and Budgetary Assessments, October 1996, 1-37.

Lepkowski, Wil. "Dual-use Program in Science, Technology to be Run by Five-Agency Group." Chemical & Engineering News, March 29, 1993, 21-22.

Leth, Steven A. "Critical Success Factors for Reengineering Business Processes." National Productivity Review, Autumn 1994, 557-568.

Linden, Russ. "Business Process Reengineering: Newest Fad, or Revolution in Government?" Public Management, November 1993, 8-12.

Manganelli, Raymond L. and Mark M. Klein. "Should you Start from Scratch?" Management Review, July 1994, 45-47.

"Marine Corps Information Warfare Combines Services' Needs, Defines Their Differences." Signal, July 1996, 61-62.

McKenna, James T. "Rome Lab Targets Info Warfare Defenses." Aviation Week and Space Technology, August 12, 1996, 65-67.

Mechling, Jerry. "Reengineering Government: Is there a 'There' There?" Public Productivity and Management Review, 18, No. 2, Winter 1994, 189-197.

Memorandum of Agreement between the Advanced Research Projects Agency, Defense Information Systems Agency, and National Security Agency Concerning the Information Systems Security Research Joint Technology Office, March 1995.

Moad, Jeff. "Does Reengineering Really Work?" Datamation, August 1, 1993, 22-28.

Molander, Roger C., Andrew S. Riddile, and Peter A. Wilson. "Strategic Information Warfare: A New Face of War." Parameters, Autumn 1996, 81-92.

Munro, Neil. "Sketching a National Warfare Defense Plan." Communications of the ACM, November 1996, 99, No, 11, 15-17.

O'Malley, Chris. "Information Warriors of the 609th." Popular Science, July 1997, 71-74.

President's Commission on Critical Infrastructure Protection. "PCCIP Report: Section One: Report Summary," November 5, 1997, 1-9. WWWeb, http://www.pccip.gov/report_index.html.

"Rapid Technology Growth Spawns Land Information Warfare Activity." Signal, July 1996, 51-54.

Robinson, Jr., Clarence A. "Army Information Operations Protect Command and Control." Signal, July 1996, 47-50.

Robinson, Clarence A., Jr. "Defense Organization Safeguards War Fighters' Information Flow." Signal, October 1995, 15-18.

Robinson, Clarence A., Jr. "Information Warfare Demands Battlespace Visualization Grasp." Signal, February 1997, 17-20.

Scott, William B. "Information Warfare Demands New Approach." Aviation Week and Space Technology, March 13, 1995, 85-88.

Scott, William B. "Information Warfare Policies Called Critical to National Security." Aviation Week and Space Technology, October 28, 1996, 60-64.

Seffers, George I. and Mark Walsh. "Data-security Center Sought." Air Force Times, December 1, 1997, 27.

Spina, James P. "Business Process Reengineering in the Nuclear Power Industry: Harnessing the Power." Nuclear News, December 1994, 26-28.

Stein, George J. "Information Warfare." Airpower Journal, Spring 1995, pp. 30-39.

Szafranski, Richard. "A Theory of Information Warfare: Preparing for 2020." Airpower Journal, Spring 1995, IX, No. 1, 56-65.

Taylor, Susan. "The U.S. Patent and Trademark Office: A Case Study in Business Process Reengineering." National Productivity Review, Winter 1994/1995, 85-96.

"The Future of Warfare: Select Enemy. Delete." The Economist, March 8, 1997, 21-24.

"The New Dimension." Survey of Defense Technology, The Economist, June 10, 1995, 8-10.

Thomas, Timothy L. "Deterring Information Warfare: A New Strategic Challenge." Parameters, Winter 1996-1997, 81-91.

Wells, Daniel W. "Information Warfare in a Joint and National Context." U.S. Air War College, April 1996, 1-27.

Whisenhunt, Robert H. "Information Warfare and the Lack of a U.S. National Policy." U.S. Army War College, April 1996, 1-27.

Vita

Captain Christina M. Anderson was born on 22 January 1966 in Silver Spring, Maryland. She graduated with honors from Georgetown Visitation Preparatory School in Washington, D.C. She received a Bachelor of Arts in both Political Science and Economics at Dickinson College in Carlisle, PA, graduating cum laude in 1988. While there, she spent her junior year in Bologna, Italy. After graduating, she was a paralegal for the Department of Justice until she entered Officer Training School in March 1989.

After receiving both her commission and training in information resource management, her initial assignment was at Dover AFB, Delaware. She held a variety of jobs from August 1989 to April 1992; 436th Civil Engineering Executive Officer, Wing Protocol Officer, and Assistant Wing Executive Officer. From April 1992 to May 1994, she was assigned to RAF Lakenheath, United Kingdom, as 48th Supply Section Commander, Wing Protocol and Assistant Executive Officer, and 48th Operations Group Executive Officer. While there, she completed both a Master of Public Administration degree from Troy State University and Squadron Officer School in residence. From June 1994 to May 1996, she served as Section Commander of the 510th Fighter Squadron "Buzzards" at Aviano Air Base, Italy. The "Buzzards" were directly involved in DENY FLIGHT, the patrolling of the no-fly zone over Bosnia-Herzegovina, and DELIBERATE FORCE, the bombing campaign that led to the Dayton Peace Accords for the troubled former Yugoslavia. In May 1996, she entered the in-residence Master of Science in Information Resource Management program, Air Force Institute of Technology. Having completed the program, her follow-on assignment is to Air Combat Command, Langley Air Force Base, Virginia.

Captain Anderson has been awarded the Meritorious Service Medal, the Air Force Commendation Medal with one oak leaf cluster, an Outstanding Unit Award, and the NATO Medal.

Permanent Address: 9006 Gettysburg Lane
College Park, MD 20740

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	December 1997	Master's Thesis

4. TITLE AND SUBTITLE
DEVELOPMENT OF A NATIONAL INFORMATION WARFARE STRATEGY: A REENGINEERING APPROACH

5. FUNDING NUMBERS

6. AUTHOR(S)
Captain Christina M. Anderson

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
2950 P Street
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER
AFIT/GIR/LAS/97D-1

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Lt Col Gary C. West, Director, Information Warfare Education,
CADRE/Aerospace Research Institute, Maxwell Air Force Base, AL

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (*Maximum 200 Words*)

This thesis analyzes the United States' national strategy for defense against information warfare (IW). Vast improvements in technology have created new problem areas regarding national security. The need for defense against potential attacks on our national infrastructure continues to grow as a problem. There is currently no national direction in this critical area, which "could put the U.S. and the U.S. military into the situation of being on the receiving end of an 'Electronic Pearl Harbor'." (Stein, 39) The following questions are investigated: 1) How is the U.S. ensuring reliability and security of its information?, 2) Are current organizations adequately defending against IW?, 3) Is there a need for a national strategy to defend against IW?, 4) What recommendations are made to address national IW strategic objectives?, and 5) How might business process reengineering be applied to accomplishing a national IW strategy? To answer these, this study discusses roles and responsibilities of organizations currently involved in IW. It evaluates problems areas associated with these efforts and experts' recommended solutions. The thesis recommends business process reengineering as an effective methodology for developing and implementing the national policy. Specifically, a step-by-step process based predominantly on Hyde's (1995) process management model is used.

14. Subject Terms
information warfare, business process reengineering, military government, corporate information management, military planning, warfare

15. NUMBER OF PAGES
94

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

AFIT Control Number AFIT/GIR/LAS/97D-1

AFIT RESEARCH ASSESSMENT

The purpose of this questionnaire is to determine the potential for current and future applications of AFIT thesis research. **Please return completed questionnaire** to: AIR FORCE INSTITUTE OF TECHNOLOGY/LAC, 2950 P STREET, WRIGHT-PATTERSON AFB OH 45433-7765. Your response is **important.** Thank you.

1. Did this research contribute to a current research project? a. Yes b. No

2. Do you believe this research topic is significant enough that it would have been researched (or contracted) by your organization or another agency if AFIT had not researched it?
a. Yes b. No

3. **Please estimate** what this research would have cost in terms of manpower and dollars if it had been accomplished under contract or if it had been done in-house.

Man Years_____ $_____

4. Whether or not you were able to establish an equivalent value for this research (in Question 3), what is your estimate of its significance?

a. Highly Significant b. Significant c. Slightly Significant d. Of No Significance

5. Comments (Please feel free to use a separate sheet for more detailed answers and include it with this form):

_____ _____
Name and Grade Organization

_____ _____
Position or Title Address