



**STRATEGY  
RESEARCH  
PROJECT**

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

**INFORMATION OPERATIONS – HARNESSING THE POWER**

BY

**20020530 108**

**LIEUTENANT COLONEL CURTIS P. CHEESEMAN  
United States Army**

**DISTRIBUTION STATEMENT A:  
Approved for Public Release.  
Distribution is Unlimited.**

**USAWC CLASS OF 2002**



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

USAWC STRATEGY RESEARCH PROJECT

**INFORMATION OPERATIONS – HARNESSING THE POWER**

by

Lieutenant Colonel Curtis P. Cheeseman  
United States Army

Colonel David R. Brooks, USA  
Project Advisor

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

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

**DISTRIBUTION STATEMENT A:**  
Approved for public release.  
Distribution is unlimited.

## ABSTRACT

AUTHOR: Curtis P. Cheeseman

TITLE: Information Operations – Harnessing the Power

FORMAT: Strategy Research Project

DATE: 08 April 2002

PAGES: 29

CLASSIFICATION: Unclassified

Information Operations (IO) have become more than an enabler in reaching the goals set forth in Joint Vision 2020 of “full spectrum dominance and information superiority.” As a result of the September 11, 2001, attack on the United States IO has been identified as one of the six critical operational goals for focusing DoD’s transformation efforts. The September 30, 2001, Quadrennial Defense Review highlights both the imperative for the United States to maintain an unsurpassed capability to conduct information operations, as well as the need to strengthen United States capabilities in these areas. However, as IO takes on greater importance in achieving information superiority, it has become more complex for commanders at all levels, tactical, operational, and strategic, to identify, synchronize, and conduct information operations across the full spectrum of operations against “nontraditional” adversaries who engage in “nontraditional” conflict in the information domain. This study examines potential shortfalls and incongruities in practice and doctrine and identifies areas within the domain that can be improved to facilitate the transformation.

## TABLE OF CONTENTS

ABSTRACT .....	iii
INFORMATION OPERATIONS: HARNESSING THE POWER.....	1
BACKGROUND .....	2
INFORMATION THREAT .....	5
INFORMATION PROCESS .....	6
PHYSICAL DOMAIN .....	7
COGNITIVE DOMAIN.....	9
COMMAND PROCESS .....	11
ALTERNATIVE APPROACH TO INFORMATION OPERATIONS .....	12
RECOMMENDATIONS FOR CHANGE.....	15
CONCLUSIONS .....	16
ENDNOTES .....	17
BIBLIOGRAPHY.....	21

## INFORMATION OPERATIONS: HARNESSING THE POWER

“Information operations are essential to achieving full spectrum dominance. The joint force must be capable of conducting information operations, the purpose of which is to facilitate and protect US decision-making processes, and in a conflict, degrade those of an adversary. While activities and capabilities employed to conduct information operations are traditional functions of military forces, the pace of change in the information environment dictates that we explore broader information operations strategies and concepts.”

—Joint Vision 2020

On 11 September, 2001, the people of the United States were shocked to see, on live television, the horrific terrorist attacks being committed within the sanctuary of their borders. These actions were the first time since Pearl Harbor that overt attacks were directed against and lodged on our soil. The people and the government were caught off guard and not prepared to react fast enough to counter the surprise attack perpetrated within our borders. As a result of successful US military operations since the end of the Cold War it has become apparent that our near term adversaries will not confront the US with traditional forces or tactics, but will more than likely challenge us asymmetrically at a time and place of their choosing. Therefore, non-traditional methods of war such as cyberattack and information operations (IO) may become the norm. To counter these threats and challenges of the 21st century, defense planning has shifted from a threat-based model to a capabilities-based model of the future. The ongoing revolution in military affairs and reliance on relevant information has significantly changed the battlespace in which we must be prepared to operate. Even though our mission to deter, preempt, and defend against aggression targeted against US sovereignty or vital interests abroad with conventional means has not changed, our ability to influence the outcome of these operations with the advance of information technology has.

The ability of commanders to gather information and use information in war is not a new concept. Sun Tzu believed that all warfare is based on deception and the ability to attack the mind of the enemy is a necessary precursor for battle.<sup>1</sup> As we transform our forces to meet the challenges ahead, our defense strategy and doctrine has become increasingly dependent upon information and decision superiority. If we continue to rely on the unprecedented growth of information as an enabler at the strategic, operational, and tactical levels of warfare the US must also transition its ability to fight offensively and defensively in the information realm. Network-centric warfare and technical overmatch are required to achieve the desired effects. However, as IO concepts and doctrine are developed to support the military transformation as

outlined in the 2001 Quadrennial Defense Review and Joint Vision 2020 it is apparent there are significant shortcomings in the U.S. ability to effectively orchestrate a coordinated IO campaign across the levels of war. This project examines the current information environment and the complex problems facing commanders. It then examines the IO tools and concepts that are being developed to support the changes brought about by the transformation and events of September 11. After a basic understanding of the concepts and tools are discussed, new IO concepts and tools are introduced to integrate the capabilities required to ensure information superiority in future military operations. Lastly, the author makes recommendations to facilitate IO operations across the full spectrum of conflict and range of military operations.

## **BACKGROUND**

It started out like a scene from a movie. After the first airplane crashed into the World Trade Center (WTC), all eyes were focused on CNN and other network broadcasts. When the second airplane hit WTC tower two doubts were cleared away that something was remiss and an attack was underway. Only minutes later our fears were confirmed when newscasts reported a plane had crashed into the Pentagon, the heart of our military might. In total, approximately 3000 people were casualties of this tragic event. As a result, according to President Bush, the United States was at "war" against those who perpetrated the September 11 attack on the U.S. and those that harbor them.<sup>2</sup> While this was an overt attack on our infrastructure, many experts believe the next strike may not be as obvious as it materializes. Their belief resides in the premise that we are already at war with terrorist groups in the media and over the internet. In fact, as early as 1999, Deputy Secretary of Defense John J. Hamre was quoted by the *London Sunday Times* as saying: "We're in the middle of a cyber war."<sup>3</sup> While the internet scored high marks for reliability during the hours following the September 11 attacks, security experts warn the network might not fare as well if it were the prime target of an assault. "The internet is extremely vulnerable, especially from network-based attacks," says Richard Stiennon, research director of network security at Gartner. "It would be very easy for terrorists to infiltrate sites in the United States and do damage from them. We are advising that after any United States retaliation, there will be significant increase in cyberterrorism."<sup>4</sup> Computer network defense has always been a serious concern; however since the attacks, increased measures have been taken by DoD and U.S. Central Command (CENTCOM). CENTCOM is the supported headquarters conducting the campaign to find Osama bin Laden and his supporters. Brigadier General Dennis C. Moran, USA, director of command, control, communications and information systems (J6) reports that CENTCOM has seen "no significant

increase in any kind of probes since the operation began,” and that “no significant computer network defense incident has taken place since the onset of operation Enduring Freedom.”<sup>5</sup> While there does not appear to have been any successful attempts to bring down or disrupt military systems, opponents and supporters of the September 11 terrorist attacks were successful in defacing each other’s web sites. According to information security expert Dorothy E. Denning, these defacements are attractive to hackers because of their potentially wide visibility and low risk of arrest or physical harm.<sup>6</sup>

Similar to the conflicts in Somalia, Bosnia, and Kosovo, the operations against Osama bin Laden and al Qaeda have been dominated by the use of information operations to formulate public opinion and perception. The information campaigns started immediately after the attacks took place and have been pursued aggressively by both sides since. Contrary to the perceived desires of Osama bin Laden, the destruction and terror presented by the sight of the fallen WTC towers and the burning Pentagon unified the American public and established a basis for United States policy towards terrorism. Through the use of the media and the internet the United States reached out to the hearts and minds of the people around the world to forge a coalition of forces to wage a war on terrorism. The initial results of the campaign were successful, and after a couple weeks of criminal investigation the President waged war on al Qaeda and the Taliban government of Afghanistan for providing safe havens and bases for al Qaeda terrorist operations.

From a military perspective the war on terrorism in Afghanistan has been very successful. Satellite communications, the use of unmanned aerial vehicles (UAVs), imagery, and web communications have allowed commanders at all levels to gather and disseminate information without precedent. Operation Enduring Freedom, for the first time, has truly demonstrated the capabilities of network-centric warfare. Information superiority, an Army supporting core competency, has proven to be essential to these operations.<sup>7</sup> High speed communications and the rapid dissemination of gathered intelligence has been a key factor in enabling commanders to visualize the battlespace and make rapid decisions. Special Forces operators working with Northern Alliance warriors have been able to locate, pinpoint, and use reachback technologies to bring massed effects of precision guided munitions upon al Qaeda and Taliban forces using new tools developed since the Gulf War. In the battle for Mazar, the first cavalry charge of the 21<sup>st</sup> century, the precision guided munitions delivered by the U.S. Navy, Air Force, and Marines softened up the hardened adversaries to the point where Afghan fighters were able to defeat them.<sup>8</sup> The United States’ reliance and use of advanced technology throughout the full spectrum of operations in this war has been without parallel. For example a distinguished guest

lecturer, during the Commandant's Lecture Series, pointed out that ten percent of the munitions used during the Gulf War were precision guided. The number increased to thirty percent in the Bosnia and Kosovo campaigns. However, in Afghanistan the use of precision guided munitions has risen to seventy to eighty percent.<sup>9</sup> The military's dependence on precision guided munitions and the global command and control systems used to bring them into play put special emphasis on the ability to achieve information superiority. Leaders and decision makers count on the uninterrupted free flow of information to conduct operations through the global information grid (GIG). In noncontiguous areas it demands that defensive information operations be implemented across the full range of military operations.

The events of September 11 only served to reinforce DoD's commitment and urgency to transform the forces from a threat-based to a capability based fighting force. One that is built around the capability to deter and defend against our perceived vulnerabilities and weaknesses rather than against an enemy who we believe is a threat. We must be able to project forces rapidly around the world to conduct operations other than war and to engage conventional forces. Additionally, it has become clear that we must have the capability to confront asymmetric terrorism at home and abroad. General Shinseki sums up the Army's motivation for change best in his comments, "it's no longer a matter of complaining that we are moving too fast or spending too much money on the development of new technologies. It's not a debate. The Army must change because the nation cannot afford to have an Army that is irrelevant."<sup>10</sup> Of the six critical operational goals for transformation identified in the 2001 Quadrennial Defense Review (QDR), four of them are directly dependent on or effected by information operations (IO). They are (1) Assure information systems in the face of attack and conduct effective information operations, (2) Deny enemies sanctuary by providing persistent surveillance, tracking, and rapid engagement, (3) Enhance the capability and survivability of space systems and supporting infrastructure, (4) Leverage information technology and innovative concepts to develop interoperable Joint C4ISR.<sup>11</sup> The increasing dependence on information systems and networks makes our civilian society and military extremely vulnerable to asymmetric and non-kinetic attack. The ongoing revolution in military affairs can be both an advantage and a disadvantage in future operations. As technologies improve, our capabilities to obtain better situational understanding of the battlespace through the use of sensors and UAVs will significantly increase. The ability to process information and use precision guided munitions will be enhanced. The combination of these capabilities and the use of IO may make the use of conventional forces by adversaries unrealistic. Therefore, the only perceived alternative available to potential adversaries may be to use chemical, biological, radiological, nuclear, and

enhanced high explosive (CBRNE) weapons or ballistic missiles. The proliferation of advanced off-the-shelf technology may also make it advantageous for adversaries to attack our infrastructure. The use of information warfare, cyberattack, and other forms of terrorism are highly likely. The QDR highlights both the imperative for the United States to maintain an unsurpassed capability to conduct information operations, as well as the need to strengthen U.S. capabilities in these areas. The ability to conduct IO has become a core competency of the DoD.<sup>12</sup> Therefore; it is time to reconsider the elements of IO and redefine what constitutes IO and how it is to be implemented by our forces and government.

### **INFORMATION THREAT**

“Much like the airline industry before September 11, high-tech companies, customers and government agencies are well aware of security vulnerabilities but are reluctant to pay to fix them ... Its just a matter of time before terrorists use those flaws to launch a cyberspace equivalent of the September 11 attacks on the critical national infrastructure such as the electricity grid.”

—Richard Clarke, White House Cyber-Security Czar<sup>13</sup>

The vision for transformation of our future forces is Joint Vision 2020. The overarching focus of the vision is full spectrum dominance, achieved through the interdependent application of dominant maneuver, precision engagement, focused logistics, and full dimensional protection.<sup>14</sup> A key enabler to realizing the vision is information superiority. Information superiority implies that decision makers will have the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.<sup>15</sup> Even though there does not appear to be any near competitor or rival coalition capable of challenging us with conventional means to deny us this goal, we have to remain vigilant in our pursuit of advanced technology. Over the last few years technology has become more diffuse and as a result the capability to obtain CBRNE and other weapons of mass destruction (WMD) has become obtainable by rouge states and non-state actors. Additionally, these potential adversaries have also gained advantages through dual use systems and indigenous weapons programs. Furthermore, the dual use nature of many information systems and infrastructures may blur the distinction between military and civilian targets. The relative inexpensiveness of new computers with increased processing power has also given them the means to develop nonlethal weapons and conduct effective information operations through the media. Because of U.S. conventional force dominance, it is more likely that information or U.S. information resources will be the targets of attack. The fact that there are more tools to make more information available suggests that information has become more

important. This also implies that deception, disinformation, and use of mass media are also of increasing value as military tools. Criminal and terrorist organizations are already exploiting these tools to their advantage. These groups use encryption techniques to form cellular dispersed networks from which to launch operations. In addition to using perception management and propaganda to influence public opinion, networked terrorists are also using the media and internet to raise funds, conduct operations, and recruit new members. There is consensus that information is increasing in importance as information technology increases in reach and capacity. But at the same time the growing dependence on precise information for combat operations also creates greater opportunities for deception.<sup>16</sup> The resulting factor is that for the U.S. to achieve full spectrum dominance it must be able to obtain information superiority which can only be achieved by the successful conduct of information operations.

## **INFORMATION PROCESS**

Information operations, as defined in Joint Publication 3-13, Joint Doctrine for Information Operations, are those actions taken to affect and adversary's information and information systems while defending one's own information and information systems.<sup>17</sup> Information operations are variable in nature and are dependent on the situation and meaning of "information." Some of the factors that influence IO are the level of action, (tactical, operational, strategic) and the desired effect and nature of the situation. Information operations can be divided into two major subdivisions, offensive IO and defensive IO. Actions that can fall under the heading of offensive information operations "include, but are not limited to, operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW), physical attack/destruction, and special information operations (SIO), and could include computer network attack (CNA)."<sup>18</sup> Defensive information operations include "information assurance (IA), information security, OPSEC, physical security, counterdeception, counterpropaganda, counterintelligence (CI), EW, and SIO."<sup>19</sup> Herein lays one of the major problems of IO as it is currently defined in doctrine. There is no scope or boundary for what we label as information operations. In essence, every type of operation conducted by U.S. forces can be identified as an information operation. In addition to the two major subdivisions, IO can be broken down further into two logical subsets or domains. One domain contains the physical elements of IO, such as CNA or computer network defense (CND) and the other domain contains the cognitive elements such as perception management or influence operations. The physical domain allows us to gather information and share it with others. It also provides us with our greatest security risk in IO because it not only can be manipulated by outside actors it can

be manipulated by insiders as well. The elements of the cognitive domain allow us to develop situational awareness or manipulate an adversary's understanding of the battlespace. The effects in the cognitive domain are hard to measure and are very difficult to assess. However, they must be understood to achieve the ultimate target of IO, the human decision making processes or decision maker.<sup>20</sup>

## **PHYSICAL DOMAIN**

The United States has recognized that its military and civilian dependence on information technology makes it more vulnerable to attack than any other nation. Reliance on the GIG and its supporting infrastructure, the national information infrastructure and the defense information infrastructure make it difficult to defend. With a renewed emphasis on the importance of global and homeland security, it is clear that protection of information has become critical, safeguarding the nation's fundamental financial, energy, defense and civil government bases. The nation's vital infrastructure, both civilian and military, is an attractive target for malicious cyber terrorists and state and non-state sponsored adversaries. The foundation for today's security structure for homeland defense is built around Presidential Decision Directive 63 (PDD-63) which was released in May 1998. PDD-63 builds on the 1997 President's Commission on Critical Infrastructure Protection and sets a goal of a reliable, interconnected, secure information system infrastructure by the year 2003. This policy also established a national coordinator as well as a number of other organizations. These included: a National Infrastructure Protection Center (NIPC) at the Federal Bureau of Investigation, a National Infrastructure Assurance Council, and a Critical Infrastructure Assurance Office in the Department of Commerce. Importantly, the directive requires each department and agency to work to reduce its own exposure to new threats. PDD-63 also solicits voluntary participation of private industry to meet common goals in protecting critical systems and encourages the establishment of Information Sharing and Analysis Centers to be set up in cooperation with the Federal government based on the Centers for Disease Control and Prevention as a model.<sup>21</sup> Until the recent release of the 2001 Quadrennial Defense Review (QDR), neither the National Security Strategy nor the National Military Strategy clearly defined homeland security as a critical, separate mission consisting of specific task areas or place it in the context of the previous defense planning framework of two nearly simultaneous major theater wars.<sup>22</sup>

Even though PDD-63 establishes a framework for critical infrastructure protection (CIP), it does not provide adequate guidance and responsibility to effectively accomplish its objectives in lieu of the increasing threat of cyberattack. A recent audit of PDD-63 conducted by the

President's Council on Integrity and Efficiency and Executive Council on Integrity and Efficiency questions the government's ability to achieve the required full operating capability by 22 May 2003. Of the five deficiencies noted in the council's evaluation, two stand out as critical; the lack of coordinated management of PDD-63 requirements, and untimely identification of critical infrastructures.<sup>23</sup> Questions abound at this time as to how the new Cabinet-level Office of Homeland Security, headed by Governor Tom Ridge, will be organized to coordinate and resolve these issues. However, we do know Ridge's primary mission is to develop and coordinate a comprehensive national strategy to secure the U.S. from terrorist threats and attacks.<sup>24</sup> Since the 2001 QDR lists homeland defense as the highest priority of the U.S. military, it indicates that DoD has a greater role in the organization and responsibility for the defense of cyberattack.<sup>25</sup> Currently, NIPC is the government's lead agency for responding to cyberattacks. The NIPC is responsible for coordinating responses to the investigations of cyberattacks and other security incidents across federal, state, local, and private-sector groups. However, a recent report released by the Defense Science Board (DSB) found this to be a serious point of contention. The DSB noted difficulties in sharing data between the national security community and the NIPC. The DSB concluded that the NIPC's practice of restricting information-sharing on incidents and investigations is inimical to DoD's interests.<sup>26</sup> Another recent study conducted by the Government Accounting Office echoed the same concerns and faulted the NIPC even further when it reported that a national plan had yet to be developed in compliance with PDD-63. The same report also concluded that DoD was unable to accurately determine the status of information security across the department, the progress of its improvement efforts, or the effectiveness of its information security initiatives.<sup>27</sup> However, as DoD strives to achieve full spectrum dominance and information superiority in the next conflict, its reliance on information technology becomes critical. DoD therefore has to take greater responsibility for the nation's critical infrastructure to ensure it will be able to accomplish its missions. As the GIG becomes more robust, DoD must be given the resources and tools to oversee its protection. No one will challenge the assertion that cyberattacks will continue to increase in frequency and severity and that information warfare will become more prevalent in the next eight to ten years. For example, the number of documented computer intrusion events has increased from 1334 in 1993 to 8800 in the first half of 2000. The Computer Security Institute estimates that computer crime in the U.S. doubled in 1999 and accounted for nearly \$10 billion in financial losses.<sup>28</sup> Because sectors of the critical infrastructure – information, communications, physical distribution networks, and finance – are becoming increasingly tied together electronically, cyberattacks can have a devastating effect on them as well. The

Director of the Central Intelligence Agency (CIA) testified before Congress in February 2000 that more than one dozen countries, including Russia and the People's Republic of China, have developed or are developing the means to launch strategic-level cyberattacks.<sup>29</sup> However, strict prohibitions exist on the latitude of the military and CIA to collect intelligence on U.S. citizens and anyone within U.S. borders. Yet our increasingly global existence, where travel is relatively easy and communications are instantaneous and without boundaries, puts a real strain on the ability of the intelligence community to quickly develop and disseminate the intelligence it might need to stop a terrorist or cyberattack. Any change to these policies raises significant privacy concerns, but where do you draw the line if the nation is at risk. Another consideration involves the role of the military. The Posse Comitatus Act was passed during the Civil War as a congressional compromise to get the military out of the business of performing civil government functions. Is this act still relevant when it pertains to cyberattacks or terrorism? The military possesses significant capabilities and brings to bear important IO resources, for example the Joint Task Force for Computer Network Operations (JTF-CNO), for monitoring, tracking, locating and potentially retaliating against attackers.<sup>30</sup> However, JTF-CNO (formally called Joint Task Force – Computer Network Defense (JTF-CND)) is underfunded and understaffed for the task of managing an actual strategic information attack.<sup>31</sup> To augment JTF-CNO and the Defense Information Systems Agency (DISA), DoD has begun implementing joint reserve virtual information organizations (JRVIOS) in an attempt to backfill critical personnel shortages. The projected completion date for JRVIOS implementation is fiscal year 2007.<sup>32</sup> It may be difficult to fill these positions because of the shortage of qualified expertise in the information-technology sector. As competition for this expertise increases between the private sector and government, the comparative rate of U.S. citizens obtaining degrees in science and engineering is on the decline. The American educational system needs to produce significantly more scientists and engineers, including four times the current number of computer scientists, to meet anticipated demand.<sup>33</sup> The objectives are obvious; however, the resources, tools, and expertise to the tasks are limited.

## **COGNITIVE DOMAIN**

The effects of IO in the cognitive domain are the hardest to measure; however, they may have the most impact on future operations. The integration of PSYOP, PA, and deception operations can be used to produce a synergistic effect against targeted information systems across the range of military operations at all levels of war. With the advent of information age warfare and the speed at which information can be shared it is possible that wars may be

avoided or ended non-kinetically. With inexpensive access to the internet available to millions of people around the world the ability to influence others and manage perceptions has become quite simple. Even though Kosovo ended as a kinetic war, many people characterize the conflict as the first war on the internet. Government, nongovernment actors, and individuals used the internet to disseminate information, spread propaganda, demonize opponents, and solicit support for their positions within their country and to an international audience.<sup>34</sup> Without the use of kinetic force the activists in this conflict were able to influence operations in the battlespace. As a result decisions were altered both politically and military. The use of the media and internet was so effective that General Wesley Clark stated, "The weight of public opinion was doing to us what the Serb air defense system failed to do: limit our air strikes."<sup>35</sup> Because adversaries were able to react faster to the changing situation and disseminate information faster, they were able to disrupt the U.S. decision making process. To counter the problems identified in Kosovo and other campaigns, International Public Information Presidential Decision Directive 68 (PDD-68) was created. PDD-68 is designed to "influence foreign audiences" in support of US foreign policy and to counteract propaganda by enemies of the U.S. and to control "international military information" with the intent "to influence the emotions, motives, objective reasoning and ultimately the behavior of foreign governments, organizations, groups and individuals."<sup>36</sup> Lessons learned in Kosovo and the mechanisms established in PDD-68 were implemented in countering allegations and misinformation broadcasted by sympathetic al Qaeda supporters in Afghanistan. Although not a perfect solution initial efforts to provide a coordinated IO campaign proved to be effective. U.S. elements located in Pakistan and Afghanistan have been able to counter media and IO events as they occur.<sup>37</sup> This effort is not to be confused with the ill fated first attempt to create a consolidated information operations campaign from the Pentagon's Office of Strategic Influence. The office was shut down under allegations that it proposed to give false information to foreign journalist to further U.S. interests in the war against terrorism.<sup>38</sup> The Pentagon must continue to develop means to coordinate military perception management and deception operations with other government agencies and civilian media to formulate a synergistic balance. If IO is not coordinated across all levels of the cognitive domain by the partners involved the full effects of the efforts to win the hearts and minds of the targeted groups or people will not be realized. As the U.S. has experienced in the most recent conflicts, IO in the cognitive domain will continue to be a key contributor to any operations that are conducted by U.S. military forces. However, the use of IO must be effectively managed and coordinated. Used successfully IO can be a significant enabler in the cognitive domain to effectively alter and influence the decision making process.

## COMMAND PROCESS

As stated earlier the ultimate goal of IO is to affect adversary or potential adversary decision makers and their decision making processes. The most common model used today in the military to affect the decision making process of an adversary is the "OODA" loop: observe, orient, decide, and act. The notion of mastering the process, spinning or getting inside the adversary's decision loop is at the heart of the digital Army and the information warfare concept. DoD has spent enormous amounts of resources focusing on the "observe" and other processes so that commanders will have the ability to process the observation into data, the data into information, and the information into orders to disrupt the flow of action. But as the speed of military conflict emerges in the future, automation will outpace the ability of the human dimension to process the information. Adversaries will take advantage of the speed of the next battlespace to operate faster than a defender can observe the activity, orient himself, decide how to respond, and act on the decision.<sup>39</sup> Moreover, the OODA loop oversimplifies the command and control process and treats military organizations as stove piped entities that have a single mind which produces a single coordinated decision across echelon and function. Additionally, the OODA loop greatly oversimplifies the joint hierarchal model underlying current military doctrine and operations. If you try to follow decision cycles required in this process across the joint command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) realm, it is evident that command and control activities at the lower echelons is massive. The complexity of this process and the time cycles that differentiate the echelons of command contribute to the problems coordinating the efforts in a fast paced engagement. It is this difference that leads to fog and friction of war.<sup>40</sup> Therefore, to ensure information superiority, a new model must be considered to keep pace with the requirements characterized by the fully integrated, fused battlespace of the future. A model that appears to be more flexible to the changing environment is the adaptive control system proposed by the Center for Advanced Concepts and Technology. The adaptive control system is made up of various information systems that when connected in the C4ISR process of network-centric warfare allow decision makers to make decisions that are better understood in all echelons of the process. The C4ISR process of the adaptive control system is made up of the following parts; battlespace monitoring, awareness, understanding, sensemaking, command intent, battlespace management, and synchronization.<sup>41</sup> When these interacting parts are fully integrated the decision cycle becomes less complex and many decisions become automatic to decision makers. In many cases the sensor to shooter relationship will be fully automated and humans will only have to enter the process to make simple decisions that require cognitive

human intervention.<sup>42</sup> Even though many of the capabilities for this model have not been integrated or developed the potential of the system has been demonstrated in Kosovo and Afghanistan where UAVs and other sensors are filtering and correlating data in common relevant operational pictures to reduce uncertainty and enable synchronization with less effort and greater efficiency. Other command and control process models have been considered, however, the adaptive control model seems to be the most powerful model integrating the cognitive and physical domains of the future.

## **ALTERNATIVE APPROACH TO INFORMATION OPERATIONS**

To effectively operate in the dynamic information rich battlespace of the future the U.S. will have to redefine what constitutes information operations and how IO is conducted. The IO definition as identified earlier in JP 3-13 does not limit the scope of IO to well defined operational areas that are clearly understood by war fighters and system support personnel. As it stands now any action taken to affect an adversary's information, physical or cognitive, or action to defend one's own information is considered an information operation. Therefore, with a little imagination, IO can be a kinetic attack on an information grid or at the opposite end of the spectrum a PSYOP operation aimed at the people of a fractured country. To structure IO, the scope of the definition must be limited to actions that are non-kinetic in nature and that truly fall within a unique operational construct. The basic functions of IO that are not unique to the construct should be omitted and be placed in other areas such as Force Protection and Information Support. Lieutenant Colonel Randal Dragon explores this concept further and breaks the current construct into five potential categories; Information Operations – Perception and Network or Cyber; Information Support Functions; Intelligence Support Functions; and Supporting Operations.<sup>43</sup> The proposed construct removes physical destruction, physical security, operations security, and information assurance from IO and places them in one of the aforementioned functional categories. This proposal narrows the focus of IO and allows the IO planner to concentrate efforts on IO unique functions.

Furthermore, to meet the complex challenges of information netwar exercised asymmetrically by groups such as al Qaeda, Hamas, and Hizbollah, computer network policy and law must be addressed. Because of the seamless communication infrastructure between military and civilian networks it is nearly impossible to distinguish the source of an information attack. Sovereignty may no longer be suited to an increasingly networked world. International laws have to be explored to facilitate countermeasures to information warfare attacks and hacking attempts. Unlike conventional warfare of the twentieth century, information warfare

attacks may be difficult to define as "peace" or "war," and it may be hard to define targets as military or civilian. Additionally, the collateral damage affiliated with an attack may affect noncombatants as well as military targets.<sup>44</sup> Who responds to these attacks? Normally any clearly defined attack would be met with a military response. But in the case of computer espionage or intrusion, incidents are normally handled by law enforcement. Responsibilities need to be identified and planning must take place to prepare for the unexpected until new laws can be passed.

IO needs to be considered a battlefield operating system (BOS) with the GIG as its dominant weapons platform. The GIG provides the global backbone for network-centric operations and is the foundation for providing situational understanding and relevant information to the common operational picture. Situational understanding and awareness are key factors that allow commanders to shape the environment across the entire spectrum of conflict. IO, through the GIG, also gives commanders the ability to strike opposing adversaries non-kinetically to disrupt communications, destroy critical infrastructures, and to conduct influence operations. Comparable to other BOS's such as maneuver, fire support, air defense and intelligence, IO provides the commander and his staff an additional means to dominate the battlespace.<sup>45</sup> There are strong similarities between the cyberbattlefield and the physical world. Centers of gravity, choke points, avenues of approach, and key terrain can be major communication hubs, routers, networks and firewalls.<sup>46</sup> Synchronized with other BOS, IO formulates a formidable capability that extends over the entire spectrum of conflict. Because of the extent of these capabilities and the importance of information as an instrument of national power it is imperative that military IO efforts be coordinated from the strategic to the tactical level. If treated as a BOS, the responsibilities and capabilities would be better understood and implemented.

With the current command structure in the military there is no effective process in place to ensure that IO is synchronized across DoD and interagency lines. The formation of JTF-CNO under U.S. Space Command (USCINCSpace) is a step in the right direction; however, decentralized control of IO still pervades current operations. If IO was treated as a BOS, IO could be a more synchronized and integrated effort. As it stands today network operation responsibilities are shared between USCINCSpace and DISA. Even though this partnership has worked without a significant glitch it makes sense to have a unified commander responsible for the entire IO operation. The cell based staff structure that is established under current doctrine will not suffice in the fast pace of future operations. There needs to be more than an ad-hoc information cell established to deconflict IO efforts across the full range of military

operations in peace through war. The fragmented control of IO at the JTF and unified command level is not an option in the future environment. A standing organization needs to be established in the command chain or a CINC-IO needs to be created as a supported or supporting CINC. It is possible that these functions could be positioned under the soon to be created Northern Command, which will be responsible for homeland security for the U.S. The latter may be the optimum choice because it allows IO plans, policy, and procedure to be created and integrated by a centralized entity, but executed decentralized by an operational CINC. The creation of a single IO DoD entity would also facilitate coordination between interagency and nongovernmental organizations in the process. It is essential that tools in both the physical and cognitive domains be coordinated at the highest levels of government. There remains much debate in this area and current IO publications addressing these issues are under revision. To achieve information dominance and mass the effects of IO, the Army proposes to place IO at corps and division under a new coordinating staff officer, the ACofS, G7 (Information Operations).<sup>47</sup> While this unity of effort has merits there still exists an element of risk. At corps and below there will be two operational planning elements, the ACofS, G3 and the ACofS, G7. If IO were designated a BOS, there may be no requirement for the ACofS, G7, because the ACofS, G3 would be responsible for synchronizing IO with the other BOS as he does today in the planning process.

To support IO in network-centric operations a new set of tools and principles need to be established. Tools are required that allow network engineers and administrators to see the entire grid. Analogous to the common operational picture for tactical commanders the IO operators need to be able to visualize the battlespace to determine where potential vulnerabilities exist. Similar to conventional warfare, IO has to follow principles that will ensure its survivability and dominance in the battlespace. IO involves a constant effort to deny adversaries the ability to disrupt and influence friendly operations while maintaining the ability to conduct freedom of movement and the sharing of information. Maybe the current principles of war as we know them are not applicable. As Robert R. Leonard postulates there is compelling reasons to revise the principles of war because they are no longer appropriate for modern warfare where information dominance and precision attack are crucial. To Leonard, for information warfare to be meaningful, it must not be just about destroying enemy information or defending one's own information, it must impact all aspects of warfare.<sup>48</sup> For IO to be successful four new principles come to mind; reliability, robustness, redundancy, and interoperability. Reliability ensures that information is available when a commander needs it. Robustness establishes a presence for information anywhere in the world or where the

commander deems it appropriate. Redundancy provides the security to conduct operations in times of crises or threat without worry. Interoperability allows the commander to share information at all echelons of operations across both civil and military networks. Other possible principles to be explored are divergence and swarming. Divergence, closely related to redundancy, implies the opposite of mass. In information age warfare dispersed forces or information nodes have a better chance for survival. Swarming is a popular technique used by rouge actors such as al Qaeda and should become a principle of war or the basis for U.S. IO doctrine. The swarm-like doctrine features a campaign of episodic, pulsing attacks by nodes of the network, at locations sprawled across global time and space where the initiator has advantages for seizing the initiative, stealthily.<sup>49</sup>

## **RECOMMENDATIONS FOR CHANGE**

Protecting the U.S. homeland is the foremost responsibility of the Armed Forces of the U.S. The current policies and command structures are not responsive to the challenges confronting the critical infrastructure of the U.S. To achieve information superiority a transformation in the way IO is conducted must take place at all levels. PDD-63 should be superceded by a new directive and responsibility for CIP be coordinated by the new Office of Homeland Security and additional responsibilities be delegated to DoD for CIP. DoD needs to commit additional resources to develop network intrusion detection tools and devices that can reconstitute networks that are compromised. As the GIG becomes the foundation for DoD information activity its security is critical to the success of JV2020. To protect the networks and infrastructure that support the GIG, DoD needs greater latitude in its ability to collect, monitor, and disseminate information from the private sector and within the borders of the U.S. Even though this raises significant privacy concerns the future risks are too great to ignore. DoD needs to revamp its personnel recruitment, training, and retention policies. As demand for information-technology expertise increases DoD needs better incentives to attract and retain qualified personnel. For example, up-or-out and mandatory retirement policies need to be relaxed. DoD should provide greater educational opportunities and increased pay incentives targeted to new recruits and civilian workforce members. Trade-offs in equipment, manpower, and funding will have to be made to facilitate change, but the risk to the nation is too great to leave our information infrastructure vulnerable to cyberattack and information warfare. Not all information attacks are expected to be physical in nature. The U.S. must also develop coordinated campaigns to influence the hearts and minds of potential adversaries before they have the courage to act. Active media campaigns and coordinated IO efforts must permeate

the area of operation prior to and during conflict. All elements of national power must be brought to the table for IO to be effective. The ability to leverage information through processes like PDD-68 must be expanded. There is a lot work that needs to be done in this emerging discipline; however, the foundation has been set. The QDR elevates IO to a core DoD competency and numerous other studies conducted by government and nongovernmental agencies have recommended change. To facilitate the required changes, the requirements must be captured and integrated into the doctrine, training, leader development, organization, material, and soldiers process.

## **CONCLUSIONS**

The battlespace of the Information Age requires that we be prepared to conduct IO both offensively and defensively to affect an adversary's decision making process. IO combined with advanced automated information systems will continue to shorten the time required for staff processes. Therefore, in the future it is vital that the U.S. military forces maintain information superiority and dominance throughout the conflict. New tools have to be built to stay ahead of terrorists, bad actors, and state sponsored adversaries who want to destroy our way of life. To counter these threats the military must become more agile and robust at sharing information across hierarchical levels of command and bureaucratic boundaries. Command structures need to be flattened to facilitate the speed required to keep pace with information demands and personnel need to be trained and prepared for the unexpected. Information and knowledge will be the key to victory; thus, he who harnesses the power to control information has the upper hand.

WORD COUNT = 6898

## ENDNOTES

<sup>1</sup> Sun Tzu, The Art of War, trans. Samuel B. Griffith (New York: Oxford University Press, 1963), 41.

<sup>2</sup> Alvin Z. Rubinstein, "America's War Against Terrorism," 1 October 2001; available from <<http://www.the-idler.com/IDLER-01/10-3a.html>>; Internet; accessed 4 October 2001.

<sup>3</sup> Eric V. Larson and John E. Peters, Preparing the U.S. Army for Homeland Security, Concepts, Issues, and Options (Santa Monica: RAND, 2001), 112.

<sup>4</sup> Meg McGinity, "A Sense of Internet Security," The Net Economy, 1 October 2001, 24.

<sup>5</sup> Robert K. Ackerman, "Technology Empowers Information Operations in Afghanistan," Signal (March 2002): 19-20.

<sup>6</sup> Patricia Daukantas, "Professors Hash Out Cyberterrorism Strategies," Government Computer News, 14 December 2001; available from <[http://www.infowar.com/class\\_3/01/class3\\_121701a\\_j.shtml](http://www.infowar.com/class_3/01/class3_121701a_j.shtml)>; Internet; accessed 2 February 2002.

<sup>7</sup> Department of the Army, The Army, Field Manual 1 (Washington, D.C.: U.S. Department of the Army, 14 June 2001), 23.

<sup>8</sup> Donald Rumsfeld, "21<sup>st</sup> Century Transformation of U.S. Armed Forces (transcript of remarks and question and answer period, National Defense University, Fort McNair)." 31 January 2002; available from <<http://www.defenselink.mil/speeches/2002/s20020131-secdef.html>>; Internet; accessed 9 March 2002.

<sup>9</sup> The comments concerning the use of precision guided munitions in this paragraph are based on remarks made by a speaker participating in the Commandant's Lecture Series.

<sup>10</sup> Michael Shinseki, "CSA Remarks (as prepared) AUSA Seminar Washington D.C." 8 November 2001; available from <<http://www.army.mil/leaders/CSA/speeches/20011108CSAREMARKSAUSA.doc>>. Internet. Accessed 9 March 2002.

<sup>11</sup> Secretary of Defense, "Quadrennial Defense Review Report," 30 September 2001; available from <<http://www.defenselink.mil/pubs/qdr2001.pdf>>; Internet; accessed 9 March 2002, pp 30-31.

<sup>12</sup> Ibid., 43.

<sup>13</sup> "US High-Tech Security Czar Warns Against Cyber Complacency," New York Wall Street Journal Online, 19 February 2002; available from <[http://online.wsj.com/article\\_email/0,,DI\\_CO\\_20020219\\_007351,00.html](http://online.wsj.com/article_email/0,,DI_CO_20020219_007351,00.html)>; Internet; accessed 26 March 2002.

<sup>14</sup> Joint Chiefs of Staff, Joint Vision 2020 (Washington: Joint Staff, June 2000), 3.

<sup>15</sup> Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Pub 3-13 (Washington: Joint Staff, 9 October 1998), I-10.

<sup>16</sup> Sam J. Tangredi, "The Future Security Environment, 2001-2025: Toward a Consensus View," in QDR 2001 Strategy-Driven Choices for America's Security, ed. Michele A. Flournoy (Washington, DC: National Defense University Press, 2001), 28-43.

<sup>17</sup> Joint Chiefs of Staff, Joint Doctrine for Information Operations, I-9.

<sup>18</sup> *Ibid.*, I-10.

<sup>19</sup> *Ibid.*

<sup>20</sup> *Ibid.*, II-1.

<sup>21</sup> Office of the Press Secretary, The White House, "Fact Sheet, Protecting America's Critical Infrastructures: PDD-63," 22 May 1998; available from <<http://www.fas.org/irp/offdocs/pdd-63.htm>>; Internet; accessed 6 September 2001.

<sup>22</sup> Larson and Peters, 11.

<sup>23</sup> President's Council on Integrity & Efficiency and Executive Council on Integrity and Efficiency, "Phase 1 review Federal agencies' implementation of PDD-63," 21 March 2001; available from <<http://www.ignet.gov/pande/audit/dcover.pdf>>; Internet; accessed 10 October 2001.

<sup>24</sup> Office of the Press Secretary, The White House, "President Established Office of Homeland Security," 8 October 2001; available from <<http://www.whitehouse.gov/news/releases/2001/10/2001108.html>>; Internet; accessed 10 October 2001.

<sup>25</sup> Secretary of Defense, Quadrennial Defense Review Report, 69.

<sup>26</sup> Defense Science Board, Protecting the Homeland: 2000 Summer Study Executive Summary Volume 1 (Washington, D.C.: Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics, February 2001), 12-13.

<sup>27</sup> General Accounting Office, Critical Infrastructure Protection: Significant Challenges in Safeguarding Government and Privately Controlled Systems from Computer-Based Attacks (Washington, D.C.: U.S. General Accounting Office, 26 September 2001), 2-8.

<sup>28</sup> Antulio J. Echevarria II, LTC, The Army and Homeland Security: A Strategic Perspective (Carlisle: Strategic Studies Institute, 2001), 5.

<sup>29</sup> *Ibid.*

<sup>30</sup> Terrance Kelly, "An Organizational Framework for Homeland Defense," Parameters 31, no. 3 (Autumn 2001): 114.

<sup>31</sup> Secretary of Defense, Road Map for National Security: Imperative for Change (Washington, D.C.:U.S. Commission on National Security/21<sup>st</sup> Century, 15 March 2001), 24.

<sup>32</sup> Maryann Lawlor, "Cyberspace Forces Gear Up: Virtual Organizations Offer Technology Professionals Opportunity to Re-serve in a New Way," Signal (August 2001): 25.

<sup>33</sup> Secretary of Defense, Road Map for National Security, 37.

<sup>34</sup> Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," in Networks and Netwars, ed. John Arquilla and David Ronfelt (Santa Monica; RAND, 2001), 239.

<sup>35</sup> Wesley K. Clark, Waging Modern War (New York: PublicAffairs, 2001), 444.

<sup>36</sup> Office of the President, "International Public Information (IPI) Presidential Decision Directive PDD 68," 30 April 1999; available from <<http://www.fas.org/irp/offdocs/pdd/pdd-68.htm>>; Internet; accessed 18 December 2001.

<sup>37</sup> Judy Keen, "Information 'War Room' Deploys Its Own Troops," 19 December 2001; available from <<http://www.usatoday.com/news/attack/2001/12/19/war-room-usat.htm>>; Internet; accessed 31 March 2002.

<sup>38</sup> "Pentagon buttons propaganda office's lips," 26 February 2002; available from <<http://www.usatoday.com/news/washdc/2002/02/26/propaganda-office-closing.htm>>; Internet; accessed 31 March 2002.

<sup>39</sup> Thomas K. Adams, "Future Warfare and the Decline of Human Decision-making," Parameters 31 (Winter 2001-2002):61-62.

<sup>40</sup> David S. Alberts et al., Understanding Information Age Warfare (Washington, D.C.: CCRP Publications Series, August 2001), 133-136.

<sup>41</sup> *Ibid.*, 136.

<sup>42</sup> *Ibid.*, 137-158.

<sup>43</sup> Randal A. Dragon, Wielding the Cyber Sword: Exploiting the Power of Information Operations, Strategy Research Project (Carlisle Barracks: U.S. Army War College, 13 March 2001), 17.

<sup>44</sup> Lawrence T. Greenberg, Symoure E. Goodman, and Kevin J. Soo Hoo, Information Warfare and International Law (Washington, D.C.: CCRP, 1997), 9-11.

<sup>45</sup> Department of the Army, Operations, Field Manual 3-0 (Washington: U.S. Department of the Army, June 2001), 5-15 – 5-17.

<sup>46</sup> Robert K. Ackerman, "Army Cyberwarriors Prepare for Broader Future," Signal (March 2002): 25.

<sup>47</sup> Department of the Army, Information Operations: Doctrine, Tactics, Techniques and Procedures, Field Manual 3-13 (DRAG Draft) (Washington: U.S. Department of the Army, 9 November 2001), 1-1.

<sup>48</sup> Robert R. Leonhard, The Principles of War for the Information Age (Novato: Presidio, 1998), 232-233.

<sup>49</sup> John Arquilla and David Ronfeldt, Networks and Netwars (Santa Monica: RAND, 2001), 367.

## BIBLIOGRAPHY

- Ackerman, Robert K. "Army Cyberwarriors Prepare for Broader Future." Signal (March 2002): 23-26.
- Ackerman, Robert K. "Technology Empowers Information Operations in Afghanistan." Signal (March 2002): 17-20.
- Adams, Thomas K. "Future Warfare and the Decline of Human Decision-making." Parameters 31 (Winter 2001-2002): 57-71.
- Alberts, David S., John J. Garstka, Richard E. Hayes, and David A. Signori. Understanding Information Age Warfare. Washington, D.C.: CCRP Publications Series, August 2001.
- Arquilla, John, and David Ronfeldt. Networks and Netwars. Santa Monica: RAND, 2001.
- Clark, Wesley K. Waging Modern War. New York: PublicAffairs, 2001.
- Daukantas, Patricia. "Professors Hash Out Cyberterrorism Strategies." Government Computer News, 14 December 2001. Available from [http://www.infowar.com/class\\_3/01/class3\\_121701a\\_j.shtml](http://www.infowar.com/class_3/01/class3_121701a_j.shtml). Internet. Accessed 2 February 2002.
- Defense Science Board, Protecting the Homeland: 2000 Summer Study Executive Summary Volume 1. Washington, D.C.: Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics, February 2001.
- Denning, Dorothy E. "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy." In Networks and Netwars, ed. John Arquilla and David Ronfeldt, 239-288. Santa Monica: RAND, 2001.
- Dragon, Randal A. Wielding the Cyber Sword: Exploiting the Power of Information Operations. Strategy Research Project. Carlisle Barracks: U.S. Army War College, 13 March 2001.
- Echevarria, Antulio J., II. The Army and Homeland Security: A Strategic Perspective. Carlisle: Strategic Studies Institute, 2001.
- Greenberg, Lawrence T., Symoure E. Goodman, and Kevin J. Soo Hoo. Information Warfare and International Law. Washington, D.C.: CCRP, 1997.
- Keen, Judy. "Information 'War Room' Deploys Its Own Troops." 19 December 2001. Available from <http://www.usatoday.com/news/attack/2001/12/19/war-room-usat.htm>. Internet. Accessed 31 March 2002.
- Kelly, Terrance. "An Organizational Framework for Homeland Defense." Parameters 31, no. 3 (Autumn 2001): 105-116.
- Larson, Eric V., and John E. Peters. Preparing the U.S. Army for Homeland Security, Concepts, Issues, and Options. Santa Monica: RAND, 2001.

- Lawlor, Maryann. "Cyberspace Forces Gear Up: Virtual Organizations Offer Technology Professionals Opportunity to Re-serve in a New Way." Signal (August 2001): 25-27.
- Leonhard, Robert R. The Principles of War for the Information Age. Novato: Presidio, 1998.
- McGinity, Meg. "A Sense of Internet Security." The Net Economy, 1 October 2001, 24.
- Office of the President. "International Public Information (IPI) Presidential Decision Directive PDD 68." 30 April 1999. Available from <<http://www.fas.org/irp/offdocs/pdd/pdd-68.htm>>. Internet. Accessed 18 December 2001.
- Office of the Press Secretary, The White House. "President Established Office of Homeland Security." 8 October 2001. Available from <<http://www.whitehouse.gov/news/releases/2001/10/2001108.html>>. Internet. Accessed 10 October 2001.
- "Pentagon buttons propaganda office's lips." 26 February 2002. Available from <<http://www.usatoday.com/news/washdc/2002/02/26/propaganda-office-closing.htm>>. Internet. Accessed 31 March 2002.
- Rubinstein, Alvin Z. "America's War Against Terrorism." 1 October 2001. Available from <<http://www.the-idler.com/IDLER-01/10-3a.html>>. Internet. Accessed 4 October 2001.
- Rumsfeld, Donald. "21<sup>st</sup> Century Transformation of U.S. Armed Forces (transcript of remarks and question and answer period, National Defense University, Fort McNair)." 31 January 2002. Available from <<http://www.defenselink.mil/speeches/2002/s20020131-secdef.html>>. Internet. Accessed 9 March 2002.
- Secretary of Defense. "Quadrennial Defense Review Report." 30 September 2001. Available from <<http://www.defenselink.mil/pubs/qdr2001.pdf>>. Internet. Accessed 9 March 2002.
- Secretary of Defense. Road Map for National Security: Imperative for Change. Washington, D.C.: U.S. Commission on National Security/21<sup>st</sup> Century, 15 March 2001.
- Shinseki, Michael. "CSA Remarks (as prepared) AUSA Seminar Washington D.C." 8 November 2001. Available from <<http://www.army.mil/leaders/CSA/speeches/20011108CSAREMARKSAUSA.doc>>. Internet. Accessed 9 March 2002.
- Tangredi, Sam J. "The Future Security Environment, 2001-2025: Toward a Consensus View." In QDR 2001 Strategy-Driven Choices for America's Security, ed. Michele A. Flournoy, 25-61. Washington, D.C.: National Defense University Press, 2001.
- Tzu, Sun. The Art of War. Translated by Samuel B. Griffith. New York: Oxford University Press, 1963.
- U.S. Department of the Army. Information Operations: Doctrine, Tactics, Techniques and Procedures. Field Manual 3-13 (DRAG Draft). Washington: U.S. Department of the Army, 9 November 2001.

U.S. Department of the Army. Operations. Field Manual 3-0. Washington: U.S. Department of the Army, June 2001.

U.S. Department of the Army. The Army. Field Manual 1. Washington: U.S. Department of the Army, 14 June 2001.

U.S. General Accounting Office. Critical Infrastructure Protection: Significant Challenges in Safeguarding Government and Privately Controlled Systems from Computer-Based Attacks. Washington, D.C.: U.S. General Accounting Office, 26 September 2001.

"U.S. High-Tech Security Czar Warns Against Cyber Complacency." New York Wall Street Journal Online 19 February 2002. Available from <[http://online.wsj.com/article\\_email/0,,DI CO 20020219 007351,00.html](http://online.wsj.com/article_email/0,,DI CO 20020219 007351,00.html)>. Internet. Accessed 26 March 2002.

U.S. Joint Chiefs of Staff. Joint Doctrine for Information Operations. Joint Pub 3-13. Washington: Joint Staff, 9 October 1998.

U.S. Joint Chiefs of Staff. Joint Vision 2020. Washington: Joint Staff June 2000.