STRATEGY RESEARCH PROJECT

INFORMATION DOMINANCE: A POLICY OF SELECTIVE ENGAGEMENT

BY

LIEUTENANT COLONEL JOSEPH E. ORR
United States Army

USAWC CLASS OF 1997
U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PAPER

INFORMATION DOMINANCE: A Policy of Selective Engagement

by

LTC Joseph E. Orr

Colonel Robert Coon
Project Advisor

U.S. Army War College
Carlisle, Pennsylvania 17013

ABSTRACT

AUTHOR: Joseph E. Orr (LTC), USA

TITLE: Information Dominance: A policy of Selective Engagement.

FORMAT: Strategic Research Paper

DATE: 8 April 1997 PAGES 24 CLASSIFICATION: Unclassified

The information age revolution is changing many aspects of our everyday life. We see this in the economy, in politics, and now in the Department of Defense as it struggles to reap the full benefits of the information age technologies. As a world leader in information age technology, the United States must leverage the power of the micro-processor to best posture itself for continued growth as the world's only superpower. This information revolution, coupled with other enabling technologies, will also ensure the military continues to meet the needs of the nation in an ever changing global environment.

In order to remain the information super power, the United States must develop a strategy focused on new ways to leverage information technology to meet the political, economic, and military needs of the nation. This must include ways to protect an infrastructure vulnerable to information warfare, and new laws to govern those who travel in cyberspace. This paper will examine information as an instrument of national power; argue the need for a national information strategy; highlight the risks associated with a growing dependence on information and discuss the need for new guidelines, laws, and agreements to govern cyberspace.

TABLE OF CONTENTS

INTRODUCTION....1

INFORMATION DOMINANCE....2

INFORMATION: AN INSTRUMENT OF NATIONAL POWER?....4

SECURITY CONCERNS....9

LEGAL ISSUES....13

CONCLUSION....17

ENDNOTES....21

BIBLIOGRAPHY....23

"Our growing dependence on increasingly sophisticated and globally available information technologies creates vulnerabilities that can be exploited by any individual, group or nation in cyberspace. Unprecedented is the Herculean task of protecting all of the nation's electronic communication systems from unauthorized access, manipulation, corruption and denial of service."[1]

Emmett Paige Jr., March 1996
Assistant Secretary of Defense for Command, Control, Communications, and Intelligence

The information age revolution is changing many aspects of our everyday life. We see this in the economy, in politics, and now in the Department of Defense as it struggles to reorganize itself in order to reap the full benefits of information age technologies now available to the services. As a world leader in information age technology, the United States must leverage the power of the microprocessor to best posture itself for continued growth as the world's only superpower. This information revolution coupled with other enabling technologies will also ensure the military continues to meet the needs of the nation in an ever changing global environment.

In order to remain the information superpower, the United States must develop a strategy focused on new ways to leverage information technology to meet the political, economic and military needs of the nation. This must include ways to protect an infrastructure vulnerable to information warfare, and new laws to govern those who travel in cyberspace. This paper will examine information as an instrument of national power; argue the need for a national information strategy; highlight the risks associated with a growing dependence on information and discuss the need for new guidelines, laws, and agreements to govern cyberspace.

INFORMATION DOMINANCE

The importance of information is really nothing new. Leaders in both civilian and military organizations have always realized the significance of information. Sun Tzu appropriately addressed the power of information thousands of years before the Information Age in one of his many proverbs as, "know the enemy and know yourself; in a hundred battles you will never be in peril."[2] Information is thus the essential foundation of battlefield knowledge and as such, revered by commanders as power. The use of couriers, flags, telegraphs, radios, telephones, computers and now satellites are just a few examples of the information systems leaders used throughout history to influence operations at all levels.

We find many historical examples of offensive and defensive measures commanders have taken to maximize information. For example, the invention of the telegraph during the Civil War allowed commanders for the first time to pass information over great distances. This enabled them to conduct operations over extended distances, and command and control forces and logistics in a more accurate and timely fashion. In World War II the Allies used the Ultra information system to deceive the Germans of the actual location for the Normandy invasion. In Desert Storm, we introduced many information-based technologies to the modern battlefield. One of the most powerful technologies introduced during the campaign was the introduction of an integrated suite of information systems fused to command and control nodes, satellites, sensors, precision- guided munitions and weapon platforms. This suite is now commonly referred to as a "system of systems" in today's military literature.[3]

These information systems were used by coalition forces at the strategic, operational and tactical level with overwhelming success. They were employed in both an offensive and defensive mode, and their cumulative effects proved devastating to Iraqi forces. Strategic strikes conducted by coalition forces against Saddam Hussain's information systems rendered his command and control virtually useless in the first 24 hours of the campaign. Accurate intelligence fused to satellites, sensors, precision-guided munitions and effective information platforms enabled the coalition to rapidly and accurately strike targets with surgical precision anywhere in the area of operations.[4] The Gulf War proved to be a showcase for information age technologies and set the stage for what many now call a "Revolution in Military Affairs."

At the end of the Gulf War, the United States emerged as the sole superpower in information dominance with a clear and concise ability to overwhelm any potential enemy by leveraging the power of information-based systems. The effects will be ever-lasting. Today, information impacts much more than just military operations. In fact, we have entered an age where information systems now influence everything we do from our personal lives to diplomatic affairs in a global context.

INFORMATION: AN INSTRUMENT OF NATIONAL POWER?

Information systems are now recognized as a strategic national resource. In fact, information is identified as an instrument of national power in the Presidents' February 1996 National Security Strategy.[5] This change is a direct result of the contributions information made in support of coalition operations during Desert Storm, rapid advances in new information technologies and our effort to establish a global information super-highway. Therefore, it is certain information will continue to influence the political, economic, and military decisions of our senior leaders well into the 21st century.

Now that the information genie is out of the bottle, information has overwhelmed our strategic thinking at all levels. Articles can be found on information dominance written by leaders in Congress, the Department of Defense, the military and civilian scholars alike. As the sole information superpower in the world; the United States now finds itself at a juncture where vision, resources, leadership, and a well thought out strategic strategy is needed to ensure we use information to best influence the goals and objectives outlined by the President, Congress and the people of this nation.[6] The United States must take this lead and decide now how to manage and protect this powerful national asset.

Information has opened up a new world of possibilities for how the United States will conduct future political, economic, and military activities on a global scale. Secretary of Defense, William Perry, had this to say about information and how it will change the way we think about war in the future.

> "We live in an age that is driven by information...The ability to acquire and communicate huge volumes of information in real time, the computing power to analyze this information quickly, and the control systems to pass this analysis to multiple users simultaneously--these are the technological breakthroughs that are changing the face of war and how we prepare for war."[7]

The impact of information will be dramatic and senior leadership must exploit new ways to use information as a national instrument of power. They must develop new strategy, doctrine, and policies to ensure we effectively capitalize on the power of the information age of tomorrow. As these areas are developed, new or existing agencies must be tasked with the responsibility to resource and institutionalize these plans at home and abroad. Additionally, we must examine and emplace sophisticated security measures to protect these systems to ensure the United States continues to enjoy information dominance as outlined in the National Security Strategy.[8]

Information dominance is much more than just winning wars. The nation who leads in this new information world will reap the political, economic, and military benefits brought about by the effective use of information. In the future, as individuals and nations become more interdependent on information systems, information will be realized globally as a source of real power and be the preferred political and economical commodity for global interaction.[9] It is this phenomena that will force us to develop an effective information strategy and resource the most promising infrastructure to ensure the United States remains the sole information superpower.

One approach is to develop an information strategy built around our ability to use or deny information - not intelligence, to promote our political, economical, military, and

democratic ideas and values throughout the world. As a source of power, information can be used to build on coalitions where once there were none. It can be used to deter potential adversaries of the United States and its allies. Our ability to accurately and quickly gather, process, and transmit information anywhere in the world enables the United States to effectively deal instantly with complex issues affecting world order.[10] This philosophy supports the President's policy of Engagement and Enlargement through the effective yet less expensive exchange of information between nations.

Information can be shared with other nations without the expense or need to place large assemblies of forces and resources in a specific region of the world. It is an effective forum for diplomatic dialogue between hostile states because information knows no boundaries. There is no such thing as sovereignty. Information can be transmitted between nations without the need for established policies or treaties. Information can be used to deter nations from becoming hostile to border nations by exchanging timely and accurate information between nations, as needed, to establish trust and reduce the potential of conflicts before they start. This was clearly demonstrated in Bosnia where information systems were used to obtain the political and military goals established by NATO.[11]

The effective use of information systems such as the Predator UAV system used in Bosnia, leveraged our diplomatic will over a nation of warring states but more importantly, continues to strengthen peace and cooperation between allies and would-be adversaries through the effective exchange of real time information. Sharing information with allies and potential enemies to obtain our desired political, economical, and military

objectives will become the norm in the future. As we become more and more engaged in operations such as peace keeping, peace enforcement and military operations other than war, information will become a more important factor than military brute force.[12] This exchange of accurate and timely information can assist world leaders in a time of global uncertainty and help to ensure future political, economic, and military cooperation between nations.

The United States can provide information to help allies and potential adversaries make these decisions by using existing satellite, sensors, and surveillance systems. The baseline systems required to support such a strategy are now in place. To get there though, we must break the paradigm of refusing to share information with other nations because of outdated intelligence concerns. Remember, we are talking about sharing information, not intelligence. Maximizing the potential of these systems is in our best interest to ensure our continued influence in future world order. A collective sharing agreement will encourage other nations to work with the United States in support of our national goals and objectives. Selective sharing of information from our network of information systems should instill cooperation among world leaders who share a common and clearer picture of the world around them. Information can reduce the uncertainty of current events, enable leaders to make better decisions, and when to use various instruments of national power. This selectively shared information strategy offers the United States a greater potential to:

a. influence foreign policy

b. increase our global economic influence

c. reduce the proliferation of weapons of mass destruction

d. counter terrorism, organized crime and drug trafficking

e. promote our democratic values and ideas

f. deter aggression

g. win America's wars

h. enhance future coalition building in a more cost-effective manner.[13]

In fact, as a deterrent measure, information may someday influence world order and discipline in much the same way as nuclear weapons do today. If we do not pursue such a strategy then we will only encourage others to pursue such a capability against us.

These systems are expensive and the nations which the United States is most likely to find itself in a regional conflict with do not have the desire nor the money to finance such an effort. The luxury of information dominance enjoyed by the United States will change if nations feel threatened by our unwillingness to share information. The selective sharing of information will help to guarantee we do not encourage other nations to unnecessarily compete with the United States. Along these same lines, the United States must aggressively pursue and resource a strategy which encourages the selective sharing of information. In doing so, we must also proceed with caution and thoroughly investigate the challenges and risks associated with an information-dominated society.

SECURITY CONCERNS

The United States is the most information-dependent nation in the world and is quickly becoming the most vulnerable to information warfare. Mr. Barry Horton, the Defense Department's Assistant Secretary for C3I warns, "the society and the economy is at risk...and in order to protect the well being and indeed the security of the nation, one has to protect not only the forces and their information support and the intelligence support, but also society and the economy at large."[14] The information explosion occurring in the United States is estimated to continue to double in size every 5 to 6 years and by the year 2000, information is expected to double in size every 11 hours. These figures will only increase as we find more ways to use the power of computers. Computer systems today now operate everything from electricity and water to international banking and commerce. In fact, they operate almost all of the services we depend on each day. This growing dependence on information raises many new concerns about the security of information and the systems we now depend on in the information age.

Mr. Emmett Paige, the Assistant Secretary of Defense for Command, Control, Communications and Intelligence is just one of many senior officials concerned about information security. In a speech to the Personnel Security Research Center Security Conference in June 1996, he addressed the information security liability of the nation.

> "One of the greatest challenges to creating a new information system, whether to support the warfighter or to manage communications, is how to maintain the security of information. Now with the administration's national information infrastructure initiative we have even greater challenges in this area. The vulnerability of government networks is increasing as data flow simplifies. The ability of individuals to penetrate information networks has been demonstrated on many occasions."[15]

Mr. Rich Wilhem, a senior member of Vice President Al Gore's information highway office, concurs. He believes the vast majority of critical information infrastructure is privately owned which raises the question of who has the responsibility for our nation's information security.[16] This places the burden for protecting these systems in private ownership but at some point the Federal Government will have to participate because of the magnitude of the problem surrounding information security. Mr. Bruce McConnell, chief of information policy in the White House Office of Management and Budget, believes "commercial information infrastructure is ripe for hostile government, criminal organizations and terrorist groups seeking to wreak havoc on the U.S. economy,"[17] Because of the complexity of information security, he is leading an effort to get the Federal Government to form partnerships with industry. This will help to ensure proper and coordinated responsibilities are established for securing infrastructure between Government and non-governmental agencies. Senator Robert Kerrey (D-NE), addresses this problem as a "lack of a coordinated effort to protect these systems that are critical to U.S. national security," which he believes has made "America a target rich environment for Information Warfare."[18]

As a nation, we are just now beginning to realize the vulnerabilities of information systems, as witnessed in the daily compromise of national systems throughout the Department of Defense, the Pentagon, and the information industry. In his book Information Warfare: Chaos on the Electronic Superhighway, Mr. Winn Schwartau highlights the danger of our growing dependence on information.

> "With over 100 million computers inextricably tying us all together through the most complex array of land and satellite based communications systems...government and commercial systems are so poorly protected today that they can be essentially considered defenseless. An electronic Pearl Harbor is waiting to happen."[19]

This problem will only grow worse as the information industry finds new and better ways for information systems to influence personal, commercial, military, and international diplomacy over the next 10 years.

A recent Joint Security Commission characterized America's vulnerability to information warfare as "the major security challenge of this decade and possibly the next century." [20] The growing concern over information security and the catastrophic effect it would have on the American people and the world, if compromised, will also continue to grow proportionately if ways are not found to protect information and supporting infrastructure. The Director of the Central Intelligence Agency, John M. Deutch, recently told a Senate panel that " the electron is the ultimate precision guided weapon...that sorties were inevitable and it is not whether these attacks will happen, but rather when and where they will be focused."[21] Imagine the implications of a successful hacker attack on the computer systems operating the air traffic control tower at the Chicago O'Hare International airport at Christmas. The possibility of such an event is real and has raised considerable concern throughout Capitol Hill and corporate America.[22] Realizing the potential of such a threat, the Department of Defense deliberately tried to break into selected information systems to determine the exact vulnerability of our national, military, and civilian computer systems.[23] This study provided some sobering results.

Today it is estimated that "over 95 percent of the worldwide telecommunications needs of the Department of Defense is satisfied by commercial communication systems."[24] Investigations conducted in June 1994 by the General Accounting Office and the Defense Information System Agency (DISA) on these systems found they were not secure against even modest attacks. Even more alarming, the investigation found over 250,000 computers had been broken into by unknown sources between 1992 and 1996. To verify this data, DISA deliberately broke into 8,932 DOD computers using basic computer skills and hardware. They successfully gained access to 88% of the computers. Later investigations revealed 96% were undetected and worse yet, only 1% was reported.[25] These tests proved DOD computer systems could be easily entered using basic computer skills and equipment. In fact, in most cases it only took a person with a 386 computer, a CD-ROM, a modem, and a little bit of patience. Although disheartening, this report stimulated many throughout the Executive branch of government to establish new agencies to investigate the effects of information warfare.

President Clinton recently established a center to investigate information warfare. This center is charged to determine the effects of information warfare attacks and to develop appropriate countermeasures.[26] This will be a colossal effort. It will require an extensive examination of the social, political, economic, military and legal issues surrounding information and appropriate practices to protect such information. The legal ramifications alone will be enormous.

LEGAL ISSUES

The information explosion presents many new legal and moral issues to investigate in ways we have yet to imagine. General Ronald R. Fogelman, Chief of Staff, U.S. Air Force addressed the area of Information Warfare in a 1995 article in *Computer World* with the following precaution, " Because exploiting [information systems] will readily cross international borders, we must be cognizant of what the law allows and will not allow. We must have good legal advice as we get into this."[27]

Restricting the rights of individuals and corporate America using the information superhighway raises much debate and uncertainty over what constitutes information crime. There are many areas that lack clear and agreed upon legal definitions. For example, what constitutes an information attack? What is an appropriate response and rules of engagement for such attacks. What are appropriate offensive and defensive countermeasures?[28] Is it a crime when a teenage hacker steals software on the Internet, or when a terrorist modifies bank transactions between countries or only when a nation tries to destroy the information infrastructure of another nation? These are hard questions which do not have finite answers in this new world of cyberspace.

Cyberspace is a whole new world which lacks well-defined rules to govern how we prosecute those who violate this space. "International laws are neither consistent nor tailored to meet the needs of Cyberspace."[29] John Arquilla and David Ronfeld authors of the book, Cyberwar is Coming!, discuss the reality and dangers of what they call "net wars" between nations in cyberspace to monopolize information power. "Net war is Information Warfare without the need of military forces, extensive resources or physical

battles."[30] It is a bloodless battlefield where individuals destroy information systems without leaving a trace of evidence for others to prosecute the crimes of the cyberspace criminal. There are no laws to govern the information which travels in cyberspace It is a world where there are no borders, no policemen or soldiers to rule and protect the information traveling across cyberspace. In this world, where all of our information power travels, there are no established rules, laws or treaties.[31]

Senator Newt Gingrich (R-GA) raised the issue of cyberspace when he recently addressed the Armed Forces Communications and Electronics Association on Information Warfare, "Cyberspace is a free flowing zone to which anyone has access, if they have a minimal level of capital...and we had better be prepared for zones of creativity in our opponents we've never dreamed of."[32] As the power of information becomes greater, many countries will develop new ways to use it against other nations to obtain greater political and economical gains. Mr. Deutch recently reported on Capitol Hill "he is concerned that the threat to our information systems will grow as the enabling technologies to attack these systems proliferate and more countries develop new strategies that incorporate such attacks."[33] He also reported that cyberspace attack is one of the top threats to United States national security and the United States is not well organized as a government to address the cyberspace threat." [34] More alarming is the growing number of countries around the world who are developing the doctrine, strategies, and tools to conduct information strikes. How then is the United States going to prosecute the lawless in cyberspace without internationally agreed-upon laws or treaties in place?

Current laws will not work against Information Warfare. For example, today the law requires a search warrant to investigate a would-be criminal. Although this law makes sense, it is ineffective against cyberspace hackers. Hackers destroy information in a matter of split seconds. They can attack computer systems undetected at any time from anywhere in the world leaving a virus to destroy information in a matter of seconds, days, or even years later. "Hackers loop and weave from system to system often crisscrossing national borders...We often can't tell if an attack is from the United States or from some foreign state," warns Senator Sam Nunn (D.-GA).[35] In fact, by the time most individuals usually detect their information or systems have been penetrated the damage has already been done. A hacker conducting crime in cyberspace leaves no fingerprints or evidence to later prosecute in a court of law. This makes it almost impossible to catch a hacker in the act. If current laws are not amended, cyberspace crime will continue to increase internationally.

New laws must be developed to prosecute criminals in cyberspace, yet also protect the individual, political, and economic rights of nations operating in cyberspace.[36] The development of such policies will raise many issues over measures taken to protect information. Dr. Michael R. Nelson, special assistant for information technology, White House Office of Science and Technology Policy, said during a National Information Conference in February, "... show stoppers for the Internet are "privacy, security, intellectual property," and that problems in establishing effective security must be solved if the United States is ever to make efficient use of the information highway."[37] Our

inability to enforce laws designed to protect information and those who create, rely upon, or own information is now a paramount concern as we zoom into the Information Age.

The need for new laws, treaties, and agreements to govern information and the infrastructure will have a profound impact on our ability to remain the sole information super power in the world. We must develop new laws which clearly spell out what constitutes the right to attack, defend against, or prosecute those who violate our information data or the systems where the information resides. Senator Jon Kyl (R-AZ), attached an amendment to last year's defense authorization bill directing the administration to produce such a report addressing the security of the United States Information Infrastructure against Information Warfare and laws designed to protect these systems. This effort will take the leadership of the United States, international cooperation, and a clear understanding of the legal issues associated with this new power we derive from information. Once fully understood, we must integrate these new laws, treaties, and agreements into a comprehensive strategy to ensure this instrument of power meets the political, economical, and military needs of the nation.

CONCLUSION

The information revolution is here today and with it are many assumptions of a better tomorrow. But, as this paper has tried to identify, in order to leverage this new technology, we must proceed with caution. Although information can enhance the political, economic, and military might of the nation; at the same time, there are many risks and vulnerabilities associated with information. As the world becomes more interconnected through information systems, our dependence on information will surely increase and, in concert, our vulnerability to cyber war, computer crime, and information warfare. There is already sufficient warning and cause for concern. In our quest for information dominance we must be careful to ensure we do not put the nation at risk through a growing dependence on information. This will be an enormous task for senior leaders in government, industry and the military.

The United States is now at a critical juncture in the information race where foresight, leadership, and resources are required to develop the proper ways, ends, and means necessary to ensure information meets the needs of the nation well into the 21st Century. First on the agenda, the President must establish a strategic vision for the information instrument of power and then provide the means to ensure the ways are accomplished in concert with his ends. This will be a monumental effort for President Clinton's administration. New agencies must be created, adequate resources applied, and cooperation obtained among those interconnected on the global information highway. This endeavor will take trust, patience, resources, and cooperation at home and abroad.

As the Toffler's highlight in their book, War and Anti-War, information knowledge will be the sole source of great wealth and power for nations in the future.[38] Today, the United States dominates the information domain with superior hardware, software, and capability. In order to retain this position of power, steps must be taken to protect the nation's information and information infrastructure from computer crime and possible terrorist activity. In the current worldwide information race there are many nations striving for information superiority. Worse yet, systems like the INTERNET are making it surprisingly easy for them to obtain like-capabilities at a fraction of the cost because of inadequate protection, legal authority, and global regulatory measures necessary to prosecute cyberspace crime. We cannot afford to let this continue in the future. New laws, treaties, and agreements must be developed to protect this valuable resource at home and abroad. Failing to act now may jeopardize our position of power and the ability to influence future world, economic, and military activities. The President, Congress, Department of Defense, Justice Department, industry, the military, and even the American people share in this responsibility.

At the national level, many government and civilian agencies are working to resolve these issues. The core of the problem rests in the fact that 95% of all information systems in the United States are civilian-owned and operated. Leaders in industry realize the need for increased security, but are concerned about constraints government may place on these systems. There is an issue of trust and dollars. Industry does not want to bear the burden of paying for required protection systems, nor do they want to have restrictions placed on them which reduces their ability to compete on a global market.

Although both parties acknowledge the need for greater protection measures, there is still a long way to go until these issues are satisfactorily resolved. On the positive side, there are many in government who recognize the magnitude of the problem and believe it is time to weigh in with guidance and resources to ensure these systems are properly protected. Unfortunately, there is much work to do if we are going to resolve these problems in the years ahead.

The information systems we use today are rapidly increasing our political, economical, and military interdependence with other nations throughout the world. As the information superpower in the world, the United States must leverage this information to shape the events of the world to best obtain the goals and objectives outlined in the National Security Strategy. This can be best accomplished through a selective engagement strategy using our information instrument of power. Our willingness to share information with allies, and when appropriate, our enemies will help to guarantee these goals are met in the future. No other nation on earth has this capability. Selective sharing of information can sustain our position as a world superpower, bolster our economical influence, and enhance the military's ability to win the nation's wars.

Information is not the cure all for the problems the United States will face in the future. But, information does promise to provide an enormous resource if leveraged properly to ensure the United States remains the sole superpower in the 21st century. To do so will require a great deal of vision, cooperation, and resources. Understanding the limitations and risks associated with a strategy of information dominance is the key to ensuring such a future as we zip along the information highway of tomorrow.

ENDNOTES

1. Paige, Emmett Jr. "The Future of Information Security," Defense Issues, Volume 11, Number 71, 26 August 1996, p.2.

2. Griffith, Samual B. Sun Tzu The Art of War. Oxford University Press, 1971, p. 84.

3. Johnson, Stuart E. and Martin C. Libicki. Dominate Battlespace Knowledge The Winning Edge. Washington D.C.: National Defense University Press, 1995, pp. 4-5.

4. Campen, Alan D. The First Information War. AFCEA International Press, Fairfax, Virginia, 1992, p. xi.

5. Office of the President of the United States, A National Strategy of Engagement and Enlargement, Washington: The White House, February 1996, p. 1.

6. Campen, Alan D. "Assessments Necessary in Coming to Terms with Information War," Signal, June 1996, pp. 547-49.

7. Office of the Assistant Secretary of Defense for Command and Control, Communications and Intelligence, Information Warfare briefing. Washington: Department of Defense, 1994, Slide 2.

8. Office of the President of the United States, A National Strategy of Engagement and Enlargement, Washington: The White House, February 1996, p. 24.

9. Toffler, Alvin and Heidi. War and Anti-War. New York: Warner Books Inc., May 1995, pp. 16, 24.

10. Office of the President of the United States, A National Strategy of Engagement and Enlargement, Washington: The White House, February 1996, pp. 12,24.

11. Fulghum, David A. "Reinforced U.S. Reconnaissance To Monitor Global Flash Points," Aviation Week & Space Technology, 21 October 1996, p. 16.

12. Baker, Jim. "The Owens Legacy," Armed Forces Journal International," July 1996, p. 22.

13. Nye, Joseph S. and William A. Owens. "America's Information Age," Foreign Affairs, March-April 1996.

14. Interview with Barry Horton, Deputy Assistant Secretray of Defense for C3I, Jane's Defence Weekly, April 10, 1996.

15. Paige, Emmitt Jr. "From The Cold War To The Global Information Age," Defense Issues, Volume 10, Number 34, April 24, 1996, p. 3.

16. Ackerman, Robert K. "Commercial Military Information Security Requirements Meld," Signal, May 1996, p. 108.

17. Ackerman, Robert K. "Businesses Face Threat of Information Warfare," Signal, May 1996, p. 45.

18. Ackerman, Robert K. "Commercial Military Information Security Requirements Meld," Signal, May 1996, p. 108.

19. Schwartau, Winn. Information Warfare: Chaos on the Electronic Superhighway. p. 37.

20. Waller, Douglas. "Onward Cyber Soldiers," Time, August 21, 1995, p. 40.

21. Williams, Robert H. "Info Warfare Attacks Score in Military's Risk Pantheon," National Defense, September 1996, p. 16.

22. Mann, Paul. "Cyber Threat Expands with Unchecked Speed," Aviation Week & Space Technology, July 1996, p. 63.

23. Robinson, Clarence A. Jr. "Information Warfare Strings Trip Wire Warning Strategy," Signal, May 1996, p..32.

24. Robinson, Clarence A. Jr. "Crucial Network Imperatives Spawn Information War Peril," Signal, June 1996, p. 5.

25. Evers, Stacey. "Stopping the hacking of cyber information," Janes Defence Weekly, April 10, 1996, p. 23.

26. Willaims, Robert H. "Info Warfare Attacks Score in Military's Risk Pantheon," National Defense, September 1996, p. 5.

27. Anthes, Gary H. "New laws sought for information warfare," Computer World, 5 June 1995, p. 5 5.

28. Robinson, Clarence A. Jr. "Crucial Network Imperatives Spawn Information War Peril," Signal, June 1996, p. 38.

29. Robinson, Clarence A. Jr. "No Sheriffs Patrol Universal Cyberspace Frontier Towns," Signal, June 1996, p. 39

30. Arquilla, John and David Ronfeld, "Cyber War is Coming," Comparative Strategy, April-June 1993, Volume 12, pp. 141-165.

31. Robinson, Clarence A. Jr. "Crucial Network Imperitives Spawn War Peril," Signal, June 1996, p. 38.

32. Campen, Alan D. "Risk to Information-based Warfare Gambles with National Security," Signal, July 1995, p. 68.

33. Silverburg, David. "Computing Currents," Armed Forces Journal International, July 1996, p. 26..

34. Mann, Paul, "Cyber Threat Expands with Unchecked Speed," Aviation Week & Space Technology, July 1996, p. 63.

35. Ibid., p. 63.

36. Robinson, Clarence A. Jr. "No Sheriffs Patrol Universal Cyberspace Frontier Towns," Signal, June 1996, pp. 41-42.

37. Campen, Alan D. and Andrew C. Braunburg. "Information Infrastructure Key Enabler for Innovation," Signal, April 1996, 62-63.

38. Toffler, Alvin and Heidi. War and Anti-War. New York: Warner Books Inc., May 1995, p. 2.

BIBLIOGRAPHY

Ackerman, Robert K. "Businesses Face Threat of Information Warfare," Signal, May 1996, p. 45.

Ackerman, Robert K. "Commercial Military Information Security Requirements Meld," Signal, May 1996, p. 108.

Arquilla, John and David Ronfeld, "Cyber War is Coming," Comparative Strategy, April-June 1993, Volume 12, pp. 141-165.

Baker, Jim. "The Owens Legacy," Armed Forces Journal International," July 1996, p. 22.

Campen, Alan D. "Assessments Necessary in Coming to Terms with Information War," Signal, June 1996, pp. 547-49.

Campen, Alan D. The First Information War. AFCEA International Press, Fairfax, Virginia, 1992, p. xi.

Campen, Alan D. "Risk to Information-based Warfare Gambles with National Security," Signal, July 1995, p. 68.

Evers, Stacey. "Stopping the hacking of cyber information," Janes Defence Weekly, April 10, 1996, p. 23.

Fulghum, David A. "Reinforced U.S. Reconnaissance To Monitor Global Flash Points," Aviation Week & Space Technology, 21 October 1996, p. 16.

Griffith, Samual B. Sun Tzu The Art of War. Oxford University Press, 1971, p. 84.

Hardy, Stephen M. "The New Guerrilla Warfare," Journal of Electronic Defense, September 1996, p. 48.

Horton, Barry. Deputy Assistant Secretary of Defense for C3I, Interview, Jane's Defence Weekly, April 10, 1996.

Johnson, Stuart E. and Martin C. Libicki. Dominate Battlespace Knowledge The Winning Edge. Washington D.C.: National Defense University Press, 1995, pp. 4-5.

Mann, Paul. "Cyber Threat Expands with Unchecked Speed," Aviation Week & Space Technology, July 1996, p. 63.

Nye, Joseph S. and William A. Owens. "America's Information Age," Foreign Affairs, March-April 1996.

Office of the Assistant Secretary of Defense for Command and Control, Communications and Intelligence, Information Warfare briefing. Washington: Department of Defense, 1994, Slide 2.

Office of the President of the United States, A National Strategy of Engagement and Enlargement, Washington: The White House, February 1996, p. 1.

Paige, Emmitt Jr. "The Future of Information Security," Defense Issues, Volume 11, Number 71, 26 August 1996, p. 2.

Pexton, Patrick. "3000 Troops Head To Gulf," Army Times, 30 September, 1996, p. 3.

Robinson, Clarence A. Jr. "Crucial Network Imperatives Spawn Information War Peril," Signal, June 1996, p. 5.

Robinson, Clarence A. Jr. "Information Warfare Strings Trip Wire Warning Strategy," Signal, May 1996, p..32.

Robinson, Clarence A. Jr. "No Sheriffs Patrol Universal Cyberspace Frontier Towns," Signal, June 1996, p. 39.

Schwartau, Winn. Information Warfare: Chaos on the Electronic Superhighway. p. 37.

Silverburg, David. "Computing Currents," Armed Forces Journal International, July 1996, p. 26.

Tice, Jim. "Force XXI Will Need Special People," Army Times, July 17, 1995, p. 12.

Toffler, Alvin and Heidi. War and Anti-War. New York: Warner Books Inc., May 1995, p. 2.

Toffler, Alvin and Heidi. War and Anti-War. New York: Warner Books Inc., May 1995, pp. 16, 24.

Waller, Douglas. "Onward Cyber Soldiers," Time, August 21, 1995, p. 40.

Williams, Robert H. "Info Warfare Attacks Score in Military's Risk Pantheon," National Defense, September 1996, p. 16.